



Management Guide

Amazon Redshift



Amazon Redshift: Management Guide

Copyright © 2024 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

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 provisionnés	39
Utilisation des AWS SDK	40
Signature d'une requête HTTP	41
Configuration de la CLI Amazon Redshift	47
Amazon Redshift sans serveur	49
Qu'est-ce qu'Amazon Redshift sans serveur ?	49
Console Amazon Redshift sans serveur	50
Considérations relatives à l'utilisation d'Amazon Redshift sans serveur	54
Capacité de calcul pour Amazon Redshift sans serveur	57
Compréhension de la capacité Amazon Redshift sans serveur	57
Mise à l'échelle et optimisation pilotées par l'IA (version préliminaire)	58
Facturation pour Amazon Redshift sans serveur	60
Tarification	60
Facturation de la capacité de calcul	60
Facturation pour stockage	65
Utilisation de l'essai gratuit d'Amazon Redshift sans serveur	66
Notes d'utilisation de facturation	66
Connexion à Amazon Redshift sans serveur	68
Connexion à Amazon Redshift sans serveur	68
Connexion à Amazon Redshift sans serveur via des pilotes JDBC	69
Connexion à Amazon Redshift sans serveur avec l'API de données	71
Se connecter avec SSL à Amazon Redshift sans serveur	71
Connexion à Amazon Redshift sans serveur à partir d'un point de terminaison de VPC géré par Amazon Redshift	74

Connexion à Amazon Redshift sans serveur à partir d'un point de terminaison de VPC	
Redshift dans un autre compte ou une autre région	74
Configuration des paramètres de trafic réseau appropriés pour Amazon Redshift sans serveur	79
Définition des rôles de base de données à accorder aux utilisateurs fédérés dans Amazon Redshift sans serveur	79
Ressources supplémentaires	80
Définition des rôles de base de données à accorder aux utilisateurs fédérés dans Amazon Redshift sans serveur	80
Identity and Access Management dans Amazon Redshift Serverless	84
Octroi d'autorisations à Amazon Redshift Serverless	84
Mise en route avec les informations d'identification IAM pour Amazon Redshift	86
Gestion de l'accès aux objets de base de données Amazon Redshift sans serveur avec des autorisations de rôle de base de données	87
Migration à partir d'un cluster provisionné vers Amazon Redshift sans serveur	89
Création d'un instantané de votre cluster provisionné	89
Connexion à Amazon Redshift sans serveur à l'aide d'un pilote	90
Utilisation du kit SDK Amazon Redshift sans serveur	93
Présentation des groupes de travail et des espaces de noms d'Amazon Redshift sans serveur	93
Présentation des groupes de travail et des espaces de noms d'Amazon Redshift sans serveur	93
Gestion d'Amazon Redshift sans serveur à l'aide de la console	96
Configuration d'Amazon Redshift sans serveur pour la première fois	96
Utilisation de groupes de travail	96
Utilisation des espaces de noms	102
Gestion des limites d'utilisation, des limites des requêtes et d'autres tâches administratives	106
Surveillance des requêtes et des charges de travail avec Amazon Redshift sans serveur	109
Surveillance des requêtes et de la charge de travail avec Amazon Redshift sans serveur	109
Journalisation d'audit pour Amazon Redshift sans serveur	114
Exportation de journaux	114
Utilisation des instantanés et des points de récupération	124
Instantanés	125
Points de récupération	128
Planification d'instantanés	129

Copie des sauvegardes dans une autre Région AWS	132
Restauration d'une table	134
Utilisation de l'AWS Command Line Interface ou de l'API Amazon Redshift sans serveur	135
Partage de données dans Amazon Redshift sans serveur	138
Partage de données dans Amazon Redshift sans serveur	139
Aperçu des ressources de balisage	141
Clusters Amazon Redshift provisionnés	143
Présentation d'Amazon Redshift	143
Clusters et nœuds	144
Utilisez EC2-VPC lorsque vous créez votre cluster	149
EC2-VPC	150
Alarme d'espace disque par défaut	150
Statut du cluster	151
Considérations relatives à l'utilisation des clusters provisionnés Amazon Redshift	154
Considérations sur les régions et les zones de disponibilité	154
Maintenance du cluster	155
Gestion des limites d'utilisation	161
Fonctionnalités de mise en réseau prises en charge par les nœuds RA3	163
Types de nœud	164
Opérations du cluster	171
Redimensionnement des clusters	171
Suspension et reprise des clusters	189
Renommer les clusters	191
Arrêt et suppression de clusters	192
Déplacement de votre cluster	193
Instantanés et sauvegardes	198
Configuration d'un déploiement multi-AZ	228
Configuration d'un déploiement multi-AZ	229
Gestion d'un déploiement multi-AZ	232
Basculement d'un déploiement multi-AZ	240
Surveillance des requêtes pour le fonctionnement multi-AZ	242
Gestion des clusters à l'aide de la console	245
Création d'un cluster	245
Création d'un cluster de prévisualisation	249
Modification d'un cluster	250
Suppression d'un cluster	252

Redémarrage d'un cluster	253
Redimensionnement d'un cluster	253
Mise à niveau de la version d'un cluster	254
Obtention d'informations sur la configuration du cluster	255
Obtention d'une vue d'ensemble de l'état du cluster	255
Création d'un instantané de cluster	255
Création ou modification d'une alarme d'espace disque	256
Utilisation des données de performance du cluster	256
Gestion des clusters à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift ..	256
Gestion des clusters dans un VPC	257
Présentation	258
Création d'un cluster dans un VPC	260
Gestion des groupes de sécurité VPC pour un Cluster	262
Configuration des paramètres de communication des groupes de sécurité pour un cluster	
Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur	263
Comment Amazon Redshift fonctionne avec le partage VPC pour les ressources AWS	267
Groupes de sous-réseaux du cluster	268
Historique des versions de cluster	271
Utilisation des intégrations zéro ETL	272
Considérations	275
Bien démarrer avec les intégrations zéro ETL	276
Création et configuration d'un entrepôt des données Amazon Redshift cible	278
Activation de la sensibilité à la casse	280
Configuration de l'autorisation dans Amazon Redshift	282
Étapes suivantes	286
Création de bases de données de destination	286
Création d'une base de données de destination dans Amazon Redshift	287
Ajout de données à votre source	288
Interrogation et création de vues matérialisées avec les données répliquées	289
Interrogation des données répliquées dans Amazon Redshift	289
Création de vues matérialisées avec les données répliquées	290
Gestion des intégrations zéro ETL	292
Partage de vos données dans Amazon Redshift	294
Métriques pour les intégrations zéro ETL	295
Résolution des problèmes liés aux intégrations zéro ETL	297
Interrogation d'une base de données	307

Connexion à Amazon Redshift	308
Interrogation d'une base de données à l'aide de l'éditeur de requête v2 Amazon Redshift	309
Configuration de votre Compte AWS	310
Utilisation de l'éditeur de requête v2	318
Interaction avec l'assistant SQL génératif de l'éditeur de requêtes v2 (version préliminaire) .	338
Chargement de données dans une base de données	346
Création et exécution de requêtes	357
Création et exécution de blocs-notes	363
Interrogation du AWS Glue Data Catalog	367
Interrogation d'un lac de données	370
Utilisation des unités de partage des données	373
Planification d'une requête	376
Visualisation des résultats	386
Collaborer et partager en équipe	393
Interrogation d'une base de données à l'aide de l'éditeur de requête	395
Considérations	397
Activation de l'accès	397
Connexion à l'éditeur de requête	399
Utilisation de l'éditeur de requête	400
Planification d'une requête	402
Connexion à un entrepôt de données à l'aide des outils client SQL	407
Recommandations pour la connexion aux outils clients	407
Configuration des connexions dans Amazon Redshift	408
Configuration des options de sécurité des connexions	588
Connexion à partir d'outils et de codes clients	597
Connexion avec SQL Workbench/J	646
Connectez-vous à votre entrepôt de données par programmation	647
Utilisation d'un profil d'authentification pour se connecter à Amazon Redshift	647
Résolution des problèmes de connexion dans Amazon Redshift	650
Utilisation de l'API de données	659
Utilisation de l'API de données	660
Considérations relatives à l'appel à l'API de données	660
Exécution d'instructions SQL avec un jeton d'idempotence	666
Autorisation de l'accès	668
Appel à l'API de données	675
Résolution des problèmes liés à l'API de données	700

Planification des opérations d'API de données avec Amazon EventBridge	701
Surveillance de l'API de données	705
Groupes de paramètres	708
Présentation	708
A propos des groupes de paramètres	708
Valeurs des paramètres par défaut	709
Configuration des valeurs des paramètres à l'aide du AWS CLI	711
Configuration de la gestion de la charge de travail	713
Propriétés WLM dynamiques et statiques	713
Propriétés du paramètre <code>wlm_json_configuration</code>	714
Configuration du paramètre <code>wlm_json_configuration</code> à l'aide du AWS CLI	721
Gestion des groupes de paramètres à l'aide de la console	730
Création d'un groupe de paramètres	730
Modification d'un groupe de paramètres	731
Création ou modification d'une règle de surveillance de requête à l'aide de la console	734
Suppression d'un groupe de paramètres	735
Association d'un groupe de paramètres à un cluster	736
Gestion des groupes de paramètres à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift	736
Intégration avec un AWS partenaire	737
Intégration avec un AWS partenaire à l'aide de la console Amazon Redshift	737
Chargement de données auprès de AWS partenaires	739
Achat de nœuds réservés	740
Présentation	740
A propos des offres de nœuds réservés	741
Comparaison de prix entre les offres de nœuds réservés	741
Fonctionnement des nœuds réservés	743
Nœuds réservés et facturation consolidée	744
Exemples de nœuds réservés	744
Achat d'une offre de nœuds réservés avec la console	746
Mise à niveau des nœuds réservés avec le AWS CLI	747
Achat d'une offre de nœud réservé à l'aide de l'AWS CLI et de l'API Amazon Redshift	748
Sécurité	750
Protection des données	752
Chiffrement des données	753
Création de jetons de données	772

Confidentialité du trafic inter-réseau	773
Gestion des identités et des accès	774
Authentification par des identités	774
Contrôle d'accès	778
Présentation de la gestion des accès	778
Utilisation des politiques basées sur une identité (politiques IAM)	785
Fédération de fournisseurs d'identité natifs pour Amazon Redshift	844
Connexion de Redshift à IAM Identity Center pour offrir aux utilisateurs une expérience d'authentification unique	848
Utilisation des rôles liés à un service	867
Utilisation de l'authentification IAM pour générer des informations d'identification de l'utilisateur de base de données	873
Autoriser Amazon Redshift à accéder aux services AWS	933
Gestion des mots de passe d'administration Amazon Redshift à l'aide de AWS Secrets Manager	969
Autorisations requises pour AWS Secrets Manager l'intégration	970
Rotation du secret de mot de passe d'administrateur	971
Récupération de l'Amazon Resource Name (ARN) du secret dans Amazon Redshift	971
Création d'un secret pour les informations de connexion à la base de données	972
Considérations relatives à l'utilisation AWS Secrets Manager avec Amazon Redshift	976
Journalisation et surveillance	976
Journalisation des audits de base de données	977
Se connecter avec CloudTrail	991
Validation de la conformité	1003
Résilience	1004
Sécurité de l'infrastructure	1005
Isolement de réseau	773
Groupes de sécurité	1007
Connexion à l'aide d'un point de terminaison de VPC d'interface	1007
Analyse de la configuration et des vulnérabilités	1013
Tâches de réseau	1015
Utilisation d'un nom de domaine personnalisé pour les connexions client	1015
Sécurité pour un nom de domaine personnalisé	1016
Configuration d'un nom de domaine personnalisé	1016
Utilisation des points de terminaison de VPC gérés par RedShift	1025
Considérations	1026

Gestion des terminaux à l'aide de la console Redshift	1027
Gestion à l'aide du AWS CLI	1029
Gestion via des opérations d'API Amazon Redshift	1029
Gestion de l'utilisation AWS CloudFormation	1030
Routage VPC amélioré	1030
Utilisation des points de terminaison d'un VPC	1032
Routage VPC amélioré	1033
Redshift Spectrum et le routage VPC amélioré	1035
Surveillance des performances de cluster	1040
Présentation	1040
Données de performance	1041
Métriques Amazon Redshift	1042
Dimensions des métriques Amazon Redshift	1053
Données de performances de charge et de requête Amazon Redshift	1056
Utilisation des données de performance	1058
Affichage des données de performances de cluster	1059
Affichage de l'historique des requêtes	1067
Affichage des données de performances de base de données	1071
Affichage de la simultanéité des charges de travail et données de mise à l'échelle de la simultanéité	1074
Affichage des requêtes et des charges	1077
Affichage des métriques du cluster pendant les opérations de chargement	1081
Analyse des performances de la charge de travail	1082
Gérer les alarmes	1084
Utilisation des indicateurs de performance dans la CloudWatch console	1085
Événements	1087
Présentation des événements du cluster	1087
Utilisation d'Amazon Simple Notification Service	1088
Abonnement aux notifications d'événements d'un cluster Amazon Redshift	1089
Affichage des événements du cluster à l'aide de la console	1091
Affichage des événements du cluster à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift	1091
Gestion des notifications d'événement d'un cluster	1092
Gestion des notifications d'événement d'un cluster à l'aide de la console Amazon Redshift	1092
Gestion des notifications d'événements du cluster à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift	1093

Notifications d'événement Amazon Redshift	1093
Catégories d'événements et messages d'événements Amazon Redshift	1093
Notifications d'événements Amazon Redshift sans serveur avec Amazon EventBridge	1117
Notifications d'événements d'intégration sans ETL avec Amazon EventBridge	1126
Quotas et limites	1138
Quotas pour les objets Amazon Redshift	1138
Quotas pour les objets Amazon Redshift sans serveur	1147
Quotas pour l'API de données Amazon Redshift	1149
Quotas pour les objets de l'éditeur de requêtes v2	1152
Quotas et limites pour les objets Amazon Redshift Spectrum	1154
Contraintes d'affectation de noms	1155
Identification	1159
Présentation du balisage	1159
Balisage des exigences	1160
Gestion des balises des ressources à l'aide de la console	1161
Gestion des étiquettes à l'aide de l'API Amazon Redshift	1161
Versions de cluster	1163
Patch 181	1163
Nouvelles fonctionnalités	1164
Correctif 180	1165
Nouvelles fonctionnalités	1166
Correctif 179	1167
Nouvelles fonctionnalités	1168
Correctif 178	1169
Nouvelles fonctionnalités	1170
Correctif 177	1172
Nouvelles fonctionnalités	1173
Correctif 176	1174
Nouvelles fonctionnalités	1175
Correctif 175	1176
Nouvelles fonctionnalités	1177
Correctif 174	1177
Nouvelles fonctions pour cette version	1177
Nouvelles fonctions pour cette version	1177
Nouvelles fonctions pour cette version	1177
Nouvelles fonctions pour cette version	1177

Nouvelles fonctions pour cette version	1177
Nouvelles fonctions pour cette version	1177
Nouvelles fonctions pour cette version	1177
Correctif 173	1179
Nouvelles fonctions pour cette version	1179
Nouvelles fonctions pour cette version	1179
Nouvelles fonctions pour cette version	1179
Nouvelles fonctions pour cette version	1179
Nouvelles fonctions pour cette version	1179
Nouvelles fonctions pour cette version	1179
Nouvelles fonctions pour cette version	1179
Nouvelles fonctions pour cette version	1179
Nouvelles fonctions pour cette version	1179
Nouvelles fonctions pour cette version	1179
Correctif 172	1180
Nouvelles fonctionnalités	1181
Correctif 171	1181
Nouvelles fonctionnalités	1182
Correctif 170	1182
Nouvelles fonctionnalités	1182
Correctif 169	1182
Nouvelles fonctionnalités	1183
Correctif 168	1183
Nouvelles fonctionnalités	1183
Exemples de code	1184
Actions	1187
CreateCluster	1188
CreateTable	1194
DeleteCluster	1198
DescribeClusters	1202
DescribeStatement	1209
GetStatementResult	1212
Insert	1214
ModifyCluster	1216
Query	1221
Scénarios	1223

Commencez à utiliser Amazon Redshift	1223
Exemples de services croisés	1250
Créer une application web pour suivre les données Amazon Redshift	1250
Historique du document	1252
.....	mcclxxxvi

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 du meilleur rapport prix/performance et de fonctionnalités SQL familières dans un easy-to-use environnement sans administration.

Quelle que soit la taille du jeu de données, Amazon Redshift offre des performances de requêtes rapides grâce aux outils SQL et aux applications de business intelligence que vous utilisez déjà.

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 Amazon Redshift sans serveur](#) : cette rubrique vous guide dans le processus de configuration d'un entrepôt des 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 demande HTTP ou HTTPS envoyée à l'API en la signant. 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 Utilisation des instantanés et des 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 Utilisation des instantanés et des 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 varient en Région AWS téraoctets et sont mesurés en téraoctets. 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.
fonctions définies par l'utilisateur (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 au cluster de bases de données Aurora et aux bases de données Amazon RDS depuis Amazon Redshift Serverless. 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.
HyperLogJournal	Vous pouvez exécuter HyperLogLog des 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.
Interrogation de données semi-structurées	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 AWS CLI ou l'API Amazon Redshift Serverless pour baliser les ressources à l'aide de 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.
CloudFormation ressources	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 dans Amazon Redshift Serverless, consultez la référence des types de ressources Amazon Redshift Serverless .
CloudTrail ressources	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 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 [Achat de nœuds réservés pour Amazon Redshift](#).

Création d'instantanés de cluster

Les snapshots sont point-in-time des sauvegardes d'un cluster. 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 qu'au 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 AWS Identity and Access Management (IAM) pour créer des comptes utilisateurs et gérer les autorisations associées à ces comptes afin de contrôler les opérations du cluster. Pour plus d'informations, consultez [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 ressources liées à l'API Amazon Redshift : la console Amazon Redshift, l'interface de ligne de commande (CLI), l'API et le kit 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 plateforme EC2-VPC pour votre cluster Amazon Redshift, vous devez utiliser les groupes de sécurité VPC. Nous vous recommandons de lancer votre cluster dans une plateforme EC2-VPC.

Vous ne pouvez pas déplacer un cluster vers un VPC après qu'il a été lancé avec EC2-Classique. Cependant, vous pouvez restaurer un instantané EC2-Classique vers un cluster EC2-VPC à l'aide de la console Amazon Redshift. Pour plus d'informations, consultez [Restauration d'un cluster à partir d'un instantané](#).

- Si vous utilisez la plateforme EC2-Classique 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 l'accès entrant explicite à une plage d'adresses CIDR/IP 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 plus d'informations, consultez [Groupes de sécurité du cluster 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 télécharger 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 de vos 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 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. 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 des données de base afin de choisir le bon équilibre prix/performance 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
		<p>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 Compréhension de la capacité Amazon Redshift sans serveur.</p>	

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 simultanéité .

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 connexion.

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 Compréhen	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
		sion de la capacité Amazon Redshift sans serveur.	
Suspension et reprise	<p>Vous pouvez suspendre un cluster provisionné lorsque vous n'avez pas de charges de travail à exécuter, afin de réduire les coûts.</p>	<p>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.</p>	<p>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.</p>

Fonctionnalité	Description	Sans serveur	Alloué
Interroger des données externes avec des requêtes Spectrum	Vous pouvez interroger des données dans des compartiments Amazon S3, dans différents formats, tels que JSON.	La facturation s'accumule lorsque les ressources de calcul traitent les charges. De plus, la facturation s'accumule au fur et à mesure que les données Redshift Spectrum sont interrogées, comme toute autre transaction. Pour plus d'informations, consultez Facturation de la capacité de calcul .	Avec un cluster entrepôt des données mis en service, la capacité Amazon Redshift Spectrum existe sur des serveurs distincts interrogés depuis le cluster Amazon Redshift. Pour plus d'informations, consultez Interroger les données externes à l'aide d'Amazon Redshift Spectrum .

Fonctionnalité	Description	Sans serveur	Alloué
Facturation des ressources informatiques	Comment s'accumule la facturation entre Amazon Redshift et Amazon Redshift sans serveur.	Avec Amazon Redshift sans serveur, vous payez pour les charges de travail que vous exécutez, en RPU/ heures sur une base par seconde, avec un forfait minimum de 60 secondes. Cela inclut les requêtes qui accèdent aux données dans des formats de fichiers ouverts dans	Avec un cluster provisionné, la facturation s'effectue à la seconde lorsque le cluster n'est pas suspendu.

Fonctionnalité	Description	Sans serveur	Alloué
		Amazon S3. Pour plus d'informations, consultez Facturation de la capacité de calcul.	

Fonctionnalité	Description	Sans serveur	Alloué
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 avec AWS KMS (avec des clés AWS gérées ou gérées par le client) ou non chiffrées. Veuillez consulter 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. Veuillez consulter Facturation de la capacité de calcul .	Le stockage est facturé séparément des ressources informatiques pour un cluster mis en service avec des nœuds RA3, et pour Amazon Redshift sans serveur.

Fonctionnalité	Description	Sans serveur	Alloué
Gestion des utilisateurs	La façon dont les utilisateurs sont gérés.	<p>Pour Amazon Redshift Serverless, les utilisateurs sont des utilisateurs IAM ou Redshift. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift Serverless.</p> <p>Pour plus d'informations sur la gestion des identités IAM, y compris les bonnes pratiques pour les rôles IAM,</p>	<p>Pour un entrepôt de données provisionné, les utilisateurs sont des utilisateurs IAM ou Redshift. Pour plus d'informations, consultez la section Gestion de la sécurité des bases de données dans le manuel Amazon Redshift Database Developer Guide.</p> <p>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.</p>

Fonctionnalité	Description	Sans serveur	Alloué
		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 Serverless est compatible avec n'importe quel outil ou application client 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	Amazon Redshift provisionné est compatible avec n'importe quel outil ou application client 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
		Serverless, consultez Connexion à Redshift Serverless .	
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 <code>workgroup-name</code> à la place du paramètre <code>cluster-identity</code> lorsque vous exécutez une commande. Pour plus d'informations sur	Amazon Redshift provisionné prend en charge l'API Amazon Redshift Data. Avec les clusters Amazon Redshift, vous utilisez le <code>cluster-identity</code> paramètre au lieu du <code>workgroup-name</code> paramètre. 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 le point-in-time rétablissement.	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 Utilisation des instantanés et des 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 le partage de données entre bases de données, comptes et régions ainsi que 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 Utilisation des instantanés et des 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 Vues de surveillance . Pour plus d'informations sur la façon de migrer vos requêtes depuis les anciennes tables et vues système provisionnées vers 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
		<p>nouvelles vues, consultez Migration vers les vues de surveillance SYS.</p>	
Groupes de paramètres	<p>Groupe de paramètres qui s'applique 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.</p>	<p>Amazon Redshift sans serveur n'utilise pas le concept de groupes de paramètres.</p>	<p>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.</p>

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
		<p>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.</p>	

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 idéale 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	Pour un cluster approvisionné, la mise en service du journal d'audit basé sur Amazon S3 a constitué la norme. Désormais, la livraison des journaux d'audit CloudWatch est étendue aux entrepôts de données provisionnés.

Fonctionnalité	Description	Sans serveur	Alloué
		Redshift 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 aux données d'événements provenant de diverses sources.	Amazon Redshift Serverless utilise Amazon EventBridge pour gérer les notifications d'événements afin de vous tenir au courant des modifications apportées up-to-date à votre entrepôt de données. Pour plus d'informations, consultez Notifications d'événements Amazon Redshift sans	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, voir Gestion des notifications d'événement d'un cluster .

Fonctionnalité	Description	Sans serveur	Alloué
		serveur avec Amazon EventBridge ge .	

Utilisation des interfaces de gestion Amazon Redshift pour les clusters provisionnés

Note

Cette rubrique se concentre sur les interfaces de gestion Amazon Redshift pour les clusters provisionnés. Il existe des interfaces de gestion similaires pour Amazon Redshift Serverless et Amazon Redshift Data API.

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, consultez [Exemples de code pour Amazon Redshift à l'aide de kits de développement logiciel AWS](#).

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 .

Utilisation de ce service avec un AWS SDK

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation populaires. Chaque 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 for C++	AWS SDK for C++ exemples de code
AWS CLI	AWS CLI exemples de code

Documentation SDK	Exemples de code
AWS SDK for Go	AWS SDK for Go exemples de code
AWS SDK for Java	AWS SDK for Java exemples de code
AWS SDK for JavaScript	AWS SDK for JavaScript exemples de code
Kit AWS SDK pour Kotlin	Kit AWS SDK pour Kotlin exemples de code
AWS SDK for .NET	AWS SDK for .NET exemples de code
AWS SDK for PHP	AWS SDK for PHP exemples de code
AWS Tools for PowerShell	Outils pour des exemples PowerShell de code
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) exemples de code
AWS SDK for Ruby	AWS SDK for Ruby exemples de code
Kit AWS SDK pour Rust	Kit AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
Kit AWS SDK pour Swift	Kit 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 SDK, consultez [Utilisation des interfaces de gestion Amazon Redshift pour les clusters provisionnés](#). 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 AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
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. <ul style="list-style-type: none"> • Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur. • Pour les AWS SDK, les outils et les AWS API, consultez la section

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
		Authentification IAM Identity Center dans le Guide de référence AWS des SDK 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 d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer les AWS CLI demandes programmatisées adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. <ul style="list-style-type: none">• Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur.• Pour les AWS SDK et les outils, voir Authentifier à l'aide d'informations d'identification à long terme dans le Guide de AWS référence des SDK 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'informations d'identification pour créer un ensemble de codes d'authentification de message 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 `wJa1rXUtnFEMI/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 commande AWS CLI 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 à son tour utilise Python (<https://www.python.org/>). Il AWS CLI peut être exécuté sur n'importe quel système d'exploitation supportant Python.

Instructions d'installation

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 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 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 informations de référence sur les commandes de la CLI Amazon Redshift, rendez-vous sur [Amazon Redshift](#) dans le manuel de référence. 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 des entrepôts des données. 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 celui-ci. 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.

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 analysez-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.
- Free trial (Essai gratuit) : cette section indique les crédits d'essai gratuit restant dans votre compte AWS . 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 Network and security (Réseau et sécurité)** : vous pouvez afficher les valeurs liées au VPC, les valeurs de chiffrement AWS KMS et les valeurs de journalisation d'audit. Vous pouvez uniquement mettre à jour la journalisation de l'audit. Pour plus d'informations sur la définition des paramètres de réseau et de sécurité à l'aide de la console, consultez [Gestion des limites d'utilisation, des limites des requêtes et d'autres tâches administratives](#).
- **AWS KMS key— AWS KMS key** Utilisé pour chiffrer les ressources dans Amazon Redshift Serverless.
- **Permissions (Autorisations)** : vous pouvez gérer les rôles IAM qu'Amazon Redshift sans serveur peut assumer pour utiliser des ressources en votre nom. Pour plus d'informations, consultez [Identity and Access Management dans Amazon Redshift Serverless](#).
- **Redshift-managed VPC endpoints (Points de terminaison VPC gérés par RedShift)** : vous pouvez accéder à votre instance Amazon Redshift sans serveur à partir d'un autre VPC ou sous-réseau. Pour plus d'informations, consultez [Connexion à Amazon Redshift sans serveur depuis d'autres points de terminaison d'un VPC](#).

Limites

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 plus d'informations, consultez [Compréhension de la capacité 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.
- Partage de données provenant d'autres espaces de noms et Comptes AWS— Vous pouvez créer une base de données à partir d'un partage de données provenant d'autres espaces de noms et 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.

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](#).

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 plus d'informations, consultez [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](#).

Maintenance window (Fenêtre de maintenance) : Amazon Redshift sans serveur n'a pas de fenêtre de maintenance. Les mises à jour de version logicielle sont automatiquement appliquées. Il n'y a pas d'interruption de la connexion existante ou de l'exécution des requêtes lorsque Amazon Redshift change de version. Les nouvelles connexions se feront toujours et fonctionneront instantanément avec Amazon Redshift sans serveur.

Availability Zone IDs (ID de la zone de disponibilité) : lorsque vous configurez votre instance Amazon Redshift sans serveur, ouvrez **Additional considerations (Considérations supplémentaires)** et assurez-vous que les ID de sous-réseau fournis dans le champ **Subnet (Sous-réseau)** contiennent au moins trois des ID de zone de disponibilité pris en charge. 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.

Three subnets (Trois sous-réseaux) : vous devez avoir trois sous-réseaux minimum et ils doivent être répartis sur trois zones de disponibilité. Par exemple, vous pouvez utiliser trois sous-réseaux qui correspondent aux zones de disponibilité us-east-1a, us-east-1b et us-east-1c. La région USA Ouest (Californie du Nord) fait exception à cette règle. Même si, de la même manière que les autres régions, elle requiert trois sous-réseaux, ceux-ci doivent se limiter à deux zones de disponibilité. La condition est que l'une de ces zones de disponibilité doit contenir deux sous-réseaux.

Exigences relatives aux adresses IP gratuites — Vous devez disposer d'adresses IP gratuites lorsque vous créez un groupe de travail Amazon Redshift Serverless. Le nombre minimum d'adresses IP augmente à mesure que le nombre d'unités de traitement Redshift (RPU) pour le groupe de travail augmente. Plus précisément, chaque sous-réseau du VPC de votre groupe de travail nécessite un nombre minimum d'adresses IP. Pour plus d'informations sur l'allocation d'adresses IP, consultez [Adressage IP](#) dans le Guide de l'utilisateur Amazon VPC.

Le nombre minimum d'adresses IP libres requis lors de la création d'un groupe de travail est le suivant :

Nombre d'adresses IP gratuites requises pour chaque sous-réseau

Unités de traitement Redshift (RPU)	Adresses IP libres requises	Taille minimum du CIDR
8	9	/27
16	15	/27
32	13	/27
64	21	/27
128	37	/26
256	69	/25
512	133	/24

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 d'adresses IP libres requises lors de la mise à jour des sous-réseaux d'un groupe de travail est le suivant :

Nombre d'adresses IP libres requises lors de la mise à jour d'un sous-réseau

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

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.

Capacité de calcul pour Amazon Redshift sans serveur

Compréhension de la capacité Amazon Redshift sans serveur

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.

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). Une RPU fournit 16 Go de mémoire. La définition d'une capacité de base plus élevée améliore les performances des requêtes, notamment pour les tâches de traitement des données qui consomment beaucoup de ressources. La capacité de base par défaut pour Amazon Redshift sans serveur est de 128 RPU. Vous pouvez régler le paramètre de capacité de base de 8 RPU à 512 RPU par unités de 8 (8, 16, 24... 512), à l'aide de la AWS console, de l'opération `UpdateWorkgroup` API ou de l'opération dans le `update-workgroup` AWS CLI

Avec une capacité minimale de 8 RPU, vous disposez désormais d'une plus grande flexibilité pour exécuter des charges de travail plus simples ou plus complexes en fonction des exigences de performance. 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. 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 ou plus.

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.

- Les configurations de 8 ou 16 RPU 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.
- La modification de la capacité de base de votre groupe de travail peut annuler certaines requêtes exécutées sur votre groupe de travail.

Mise à l'échelle et optimisation pilotées par l'IA (version préliminaire)

Ceci est la documentation préliminaire relative à la mise à l'échelle et aux optimisations pilotées par l'IA dans Amazon Redshift sans serveur, qui est en version préliminaire. La documentation et la fonction sont toutes deux sujettes à modification. Nous vous recommandons d'utiliser cette fonction uniquement dans des environnements de test et non dans des environnements de production. Pour voir les conditions générales, consultez [Beta and Previews \(Bêtas et aperçus\)](#) dans les [Conditions de service AWS](#).

Cet aperçu est disponible dans les versions suivantes Régions AWS :

- USA Est (Ohio) (us-east-2)
- USA Est (Virginie du Nord) (us-east-1)
- USA Ouest (Oregon) (us-west-2)
- Asie-Pacifique (Tokyo) (ap-northeast-1)
- Europe (Irlande) (eu-west-1)
- Europe (Stockholm) (eu-north-1)

Vous pouvez créer un groupe de travail en version préliminaire pour tester les nouvelles fonctionnalités d'Amazon Redshift sans serveur. Vous ne pouvez pas utiliser ces fonctionnalités en

production ni déplacer votre groupe de travail vers un autre groupe de travail. Pour connaître les conditions générales de la version préliminaire, consultez [Versions Bêta et préliminaires dans les Conditions générales du service AWS](#). Pour obtenir des instructions sur la création d'un groupe de travail en version préliminaire, consultez [Création d'un groupe de travail de prévisualisation](#).

Vous pouvez également définir un rapport prix/performance cible pour votre groupe de travail, afin que Redshift puisse apporter automatiquement à vos ressources des optimisations pilotées par l'IA. De cette façon, vous pouvez atteindre votre rapport prix/performance cible tout en optimisant les coûts. Cette optimisation automatique du rapport prix/performance 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.

Par 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 le niveau de capacité de base approprié. La définition d'une capacité de base plus élevée permet d'obtenir un meilleur rapport prix/performance, mais elle entraîne également des coûts plus élevés, de sorte que le coût risque de ne pas correspondre à vos attentes. Grâce à l'optimisation des ressources et à la mise à l'échelle pilotées par l'IA, Amazon Redshift sans serveur ajuste automatiquement les RPU pour atteindre vos rapports prix/performance cible tout en optimisant les coûts pour votre organisation. 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/performance cible de votre organisation en cas de requêtes complexes.

Les rapports prix-performance cible sont un paramètre spécifique à chaque groupe de travail. Les différents groupes de travail peuvent avoir des rapports prix/performance cible différents.

Pour que les coûts restent prévisibles, définissez une limite de capacité maximale qu'Amazon Redshift sans serveur est autorisé à allouer à vos charges de travail.

Pour configurer les objectifs de performance et de prix, utilisez la AWS console. Par défaut, le rapport prix/performance cible est activé lorsque vous créez un nouveau groupe de travail et il est défini sur Équilibré. Pour définir un rapport prix/performance différent ou spécifier une capacité de base pour votre groupe de travail, utilisez des paramètres personnalisés lors de la création d'un groupe de travail. Pour plus d'informations sur la création d'un groupe de travail, consultez [Création d'un groupe de travail avec un espace de noms](#).

Pour modifier le rapport prix/performance cible pour votre groupe de travail :

1. Sur 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 Rapport prix/performances cible et ajustez le curseur en fonction du rapport que vous souhaitez définir pour votre groupe de travail.
4. Sélectionnez Enregistrer les modifications.

Pour mettre à jour le nombre maximal de RPU qu'Amazon Redshift sans serveur peut allouer à votre charge de travail, accédez à l'onglet Limites de la configuration du groupe de travail.

Pour en savoir plus sur les optimisations pilotées par l'IA et la mise à l'échelle des ressources, regardez la vidéo suivante.

Facturation pour Amazon Redshift sans serveur

Tarifification

Pour obtenir des informations sur la tarification, consultez [Tarification Amazon Redshift](#).

Facturation de la capacité de calcul

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 exigences de prix/performance de votre charge de travail au niveau du 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](#).

Une autre façon de maintenir prévisible le coût d'Amazon Redshift sans serveur est d'utiliser la fonctionnalité AWS [Cost Anomaly Detection](#) pour réduire les surprises liées à la facturation et offrir plus de 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 ?

L'objectif des limites maximales d'heures de RPU et du paramètre de capacité maximale est de contrôler les coûts. Mais ils y parviennent par différents moyens. Les points suivants expliquent la différence :

- **Capacité maximale** : ce paramètre définit le nombre le plus élevé de RPU qu'Amazon Redshift sans serveur utilise à des fins de mise à l'échelle. Lorsque la mise à l'échelle automatique du calcul est requise, le fait d'avoir une capacité maximale élevée peut améliorer le débit des requêtes. Lorsque la limite de capacité maximale est atteinte, le groupe de travail n'augmente plus les ressources.
- **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 la capacité maximale de façon exclusive ou vous pouvez la compléter par des actions liées aux limites d'utilisation maximales 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.
- La configuration du paramètre de capacité maximale n'interfère pas avec l'exécution des requêtes, même en période d'utilisation élevée de RPU. Cela ne fonctionne pas comme une limite d'utilisation, qui peut empêcher l'exécution des requêtes. Cela limite uniquement les ressources de calcul disponibles pour le groupe de travail. 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](#).
- 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 pour les charges de travail que vous exécutez, en RPU/heures sur une base par seconde, avec un forfait minimum 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'agrégier 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 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 d'utilisateurs est facturé au taux standard des sauvegardes, en fonction de votre niveau d'utilisation.

Les coûts de transfert de données et de machine learning (ML) s'appliquent séparément, de la même manière que les clusters alloués. Les répliqués d'instantanés et le partage de données entre régions AWS sont facturés selon les 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 `SnapshotStorage`, 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](#).

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](#).

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 actuellement à l'environnement sans serveur de votre Compte AWS ordinateur. 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'avec l'opération d'API UpdateWorkgroup et l' AWS CLI opérationupdate-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 sans serveur avec votre client SQL préféré en utilisant le pilote JDBC version 2 fourni par Amazon Redshift.

Pour se connecter avec des informations d'identification pour l'authentification de la base de données en utilisant le pilote JDBC version 2.1.x ou ultérieure, 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 et l'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 se connecter à IAM en utilisant le pilote JDBC version 2.1.x ou ultérieure, 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'API AWS CLI et 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 indique la valeur par défaut du groupe de travail et 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
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 le groupe de travail s'exécute. 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 au lieu du `cluster-identifiant` paramètre dans vos AWS CLI appels.

Pour plus d'informations sur l'API de données, consultez [Utilisation de l'API de données Amazon Redshift](#). Par exemple, le code appelant l'API de données en Python et d'autres exemples, consultez [Getting Started with Redshift Data API](#) et consultez les use-cases dossiers `quick-start` et dans 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 Serverless crée et installe un certificat SSL émis [AWS Certificate Manager \(ACM\)](#) pour chaque groupe de travail. Les certificats ACM sont publiquement approuvés par la plupart des systèmes d'exploitation, des navigateurs web et des clients. Vous devrez peut-être télécharger un bundle de certificats si vos clients ou applications SQL se connectent à Redshift Serverless à l'aide du protocole SSL avec l'option de `sslmode` connexion définie `require`, `verify-ca` ou `verify-full`. Si votre client a besoin d'un certificat, Redshift Serverless fournit un certificat groupé 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 `418dea9b6d5d5de7a8f1ac42e164cdf`.
 - 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 `418dea9b6d5d5de7a8f1ac42e164cdf`.

- Le numéro de total de contrôle sha256 est
36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

N'utilisez pas les solutions groupées de certificats antérieures qui se trouvent 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 Serverless a changé la façon dont les certificats SSL sont gérés. Vous devrez peut-être mettre à jour vos certificats CA racine actuels pour continuer à vous connecter à vos groupes de travail à l'aide du protocole SSL. Pour plus d'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 des groupes de travail acceptent les connexions, qu'elles utilisent le protocole SSL ou non.

Pour créer un nouveau groupe de travail qui accepte uniquement les connexions SSL, utilisez la `create-workgroup` commande et définissez le `require_ssl` paramètre sur `true`. Pour utiliser l'exemple suivant, remplacez *yourNamespaceName* par le nom de votre espace de noms et remplacez par *yourWorkgroupName* 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 `update-workgroup` commande et définissez le `require_ssl` paramètre sur `true`. Notez que Redshift Serverless redémarrera votre groupe de travail lorsque vous mettrez à jour le paramètre. `require_ssl` Pour utiliser l'exemple suivant, remplacez-le *yourWorkgroupName* par le nom de votre groupe de travail.

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

```
--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 SSL conforme à la norme FIPS à Amazon Redshift Serverless

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

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

Pour mettre à jour un groupe de travail existant afin d'utiliser une connexion SSL conforme à la norme FIPS, utilisez la `update-workgroup` commande et définissez le paramètre `use_fips_ssl true`. Notez que Redshift Serverless redémarrera votre groupe de travail lorsque vous mettrez à jour le paramètre `use_fips_ssl`. Pour utiliser l'exemple suivant, remplacez-le *yourWorkgroupName* par le nom de votre groupe de travail.

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

[Pour plus d'informations sur la configuration de Redshift Serverless pour utiliser des connexions conformes à la norme FIPS, 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 l'installation 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 gérés par Redshift.](#)

Connexion à Amazon Redshift sans serveur à partir d'un point de terminaison de VPC Redshift dans un autre compte ou une autre région

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-serverless : PutResourcePolicy
- redshift-serverless : GetResourcePolicy

- redshift-serverless : DeleteResourcePolicy
- EC2 : CreateVpcEndpoint
- EC2 : ModifyVpcEndpoint

Il se peut que vous ayez 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-serverless : ListWorkgroups
- redshift-serverless : CreateEndpointAccess
- redshift-serverless : UpdateEndpointAccess
- redshift-serverless : GetEndpointAccess
- redshift-serverless : ListEndpointAccess
- redshift-serverless : 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 :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CrossAccountCrossVPCAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "123456789012",
          "234567890123"
        ]
      },
      "Action": [
        "redshift-serverless:CreateEndpointAccess",
        "redshift-serverless:UpdateEndpointAccess",

```


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 réseau Redshift supplémentaires. Il n'est pas non plus obligatoire 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, 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](#).

Configuration des paramètres de trafic réseau appropriés pour Amazon Redshift sans serveur

Se connecter à Amazon Redshift sans serveur lorsqu'il est publiquement accessible

Les instructions pour définir les paramètres de trafic réseau sont disponibles dans [Accessibilité publique avec configuration de groupe de sécurité par défaut ou personnalisée](#). Cela inclut un cas d'utilisation où le cluster est accessible au public.

Se connecter à Amazon Redshift sans serveur lorsqu'il n'est pas publiquement accessible

Les instructions pour définir les paramètres de trafic réseau sont disponibles dans [Accessibilité privée avec configuration de groupe de sécurité par défaut ou personnalisée](#). Cela inclut un cas d'utilisation où le cluster n'est pas disponible sur Internet.

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

Vous pouvez définir des rôles dans votre organisation qui déterminent les rôles de base de données à accorder dans Amazon Redshift sans serveur. Pour plus d'informations, consultez [Définition des rôles de base de données à accorder aux utilisateurs fédérés dans Amazon Redshift sans serveur](#).

Ressources supplémentaires

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 [Contrôle d'accès basé sur les rôles \(RBAC\)](#).

Configuration des rôles de la 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 ou Okta, ou sur site, tel que 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. Tel est le cas des 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 l'éditeur de requêtes Amazon Redshift v2 avec Active Directory](#)

[Federation Services \(AD FS\)](#) ou [Fédérer l'accès à authentification unique à l'éditeur de requêtes Amazon Redshift 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 une banque 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, consultez la section [Transmission de balises de session à l'aide de AssumeRoleWith SAML](#).

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. Dans ce cas d'utilisation, configurez les valeurs des balises pour vos rôles dans AWS Identity and Access Management. 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 AWS Identity and Access Management (IAM) et Amazon Redshift pour sécuriser vos ressources en contrôlant qui peut y accéder. Pour plus d'informations, consultez [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.

Autoriser Amazon Redshift Serverless à accéder AWS à d'autres services pour vous

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 AWS Identity and Access Management (IAM). Vous pouvez également créer un rôle IAM via la console Amazon Redshift et le définir comme rôle par défaut. Pour plus d'informations, consultez [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 [site `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, consultez [Autoriser Amazon Redshift à accéder à d' AWS autres 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, télécharger, 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 AWS Management Console le, choisissez la console Amazon Redshift, puis choisissez Redshift Serverless dans le menu. Depuis le tableau de bord Serverless, 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.

Lorsque vous disposez d'un groupe de travail Amazon Redshift Serverless existant et que vous souhaitez configurer des rôles IAM pour celui-ci, ouvrez le. AWS Management Console Choisissez la console Amazon Redshift, puis choisissez Redshift Serverless. Sur la console Amazon Redshift Serverless, choisissez la configuration de l'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, AWS Management Console vous pouvez gérer les politiques d'autorisation pour les rôles dans AWS Identity and Access Management. 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 [Présentation des groupes de travail et des espaces de noms d'Amazon Redshift sans serveur](#).

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.

Gestion de l'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 AWS Identity and Access Management 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

Pour migrer à partir d'un cluster provisionné vers Amazon Redshift sans serveur, consultez les étapes suivantes.

Création d'un instantané de votre cluster provisionné

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. 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.

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 sans serveur.

Pour créer un instantané de votre cluster provisionné

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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).
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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
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 fourni par Amazon Redshift. Nous vous recommandons de vous connecter en utilisant le pilote JDBC version 2.1.x ou ultérieure. 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 et l'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 se connecter en utilisant une authentification par mot de passe, utilisez la syntaxe suivante.

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

Pour vous connecter à l'aide du pilote Amazon Redshift Python, 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='enter a user',
    password='enter a password'
    # port value of 5439 is specified by default
) as conn:
    pass
```

Connexion à l'aide d'IAM

Si vous préférez vous connecter avec IAM, utilisez le point de terminaison de pilote suivant. Ce point de terminaison de pilote vous permet de vous connecter à une base de données spécifique et utilise l'opération d'API [GetCredentials](#) d'Amazon Redshift sans serveur.

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

Ce point de terminaison de pilote ne prend pas en charge la personnalisation de `dbUser`, `dbGroup` et `auto-create`. Par défaut, le pilote crée automatiquement des utilisateurs de base de données lors de la connexion et les affecte aux groupes en fonction des groupes que vous avez définis dans IAM. Remarque : les noms de groupes que vous spécifiez dans IAM ne peuvent contenir que des lettres minuscules, des chiffres, des tirets bas (« _ »), le signe plus (« + »), des points (« . »), des arobases (@) ou des tirets (« - »). Sinon, le pilote risque de ne pas se connecter à `dbGroup`.

Assurez-vous que votre AWS identité dispose de la politique IAM appropriée pour l'`RedshiftServerlessGetCredentials` action. Voici un exemple de politique IAM qui accorde les autorisations appropriées à une AWS identité pour se connecter à Amazon Redshift Serverless. Pour plus d'informations sur les autorisations IAM, consultez [Ajouter des autorisations IAM Identity](#).

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



```

        "Resource": "*"
    }
]
}

```

Connexion à l'aide d'IAM avec dbUser et dbGroups

Si vous souhaitez utiliser des options de connexion dbUser et dbGroup personnalisées, utilisez le point de terminaison de pilote suivant. Comme pour l'autre point de terminaison de pilote Amazon Redshift sans serveur, cette syntaxe crée automatiquement des utilisateurs de base de données lors de la connexion. Ce point de terminaison de pilote utilise l'opération d'API [GetCredentials](#) d'Amazon Redshift sans serveur. dbUser doit commencer par une lettre et ne contenir que des caractères alphanumériques, des tirets bas (« _ »), le signe plus (« + »), des points (« . »), des arobases (@) ou des tirets (« - ») et doit contenir moins de 128 caractères. dbGroups ne doit contenir que des lettres minuscules, des chiffres, des tirets bas (« _ »), le signe plus (« + »), des points (« . »), des arobases (@) ou des tirets.

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

Pour vous connecter à l'aide du pilote Amazon Redshift Python, utilisez 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>',
    db_user='enter a user',
    password='enter a password',
    db_groups='<db-groups>'
    # port value of 5439 is specified by default
) as conn:
    pass

```

Connexion à l'aide d'ODBC

Pour se connecter à l'aide d'ODBC, utilisez la syntaxe suivante.

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

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](#).

Présentation des groupes de travail et des espaces de noms d'Amazon Redshift sans serveur

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.

Présentation des groupes de travail et des espaces de noms d'Amazon Redshift sans serveur

L'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 le chiffrement des 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 AWS Command Line Interface, ou des API Amazon Redshift Serverless pour la ressource spécifique.

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 AWS Command Line Interface, ou des API Amazon Redshift Serverless.

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.

Commencer avec Amazon Redshift sans serveur 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 de 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.

Gestion des groupes de travail et des espaces de noms à l'aide de l'API AWS Command Line Interface Serverless et d'Amazon Redshift

Outre l'utilisation de la AWS console, vous pouvez également utiliser l'API Amazon Redshift Serverless AWS CLI ou l'API Amazon Redshift 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 restaurant un instantané. Pour plus d'informations, consultez

Opération API	Commande de la CLI	Description
		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.
ListNamespaces	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-réseaux, 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.

Gestion d'Amazon Redshift sans serveur à l'aide de la console

Pour créer, modifier et supprimer votre entrepôt des données Amazon Redshift sans serveur, utilisez Serverless dashboard (Tableau de bord sans serveur) dans la console Amazon Redshift. L'accès aux paramètres individuels de la console dépend de votre rôle IAM et de vos autorisations.

Pour plus d'informations sur la configuration d'Amazon Redshift sans serveur, consultez [Configuration d'Amazon Redshift sans serveur pour la première fois](#). Pour plus d'informations sur la création et la configuration de groupes de travail, consultez [Utilisation de groupes de travail](#). Pour plus d'informations sur la configuration d'espaces de noms, consultez [Utilisation des espaces de noms](#).

Configuration d'Amazon Redshift sans serveur pour la première fois

La première fois que vous sélectionnez Serverless dashboard (Tableau de bord sans serveur), il vous guide à travers les étapes de la configuration d'Amazon Redshift sans serveur. Sous Get started with the serverless experience (Démarrer avec l'expérience sans serveur), vous pouvez créer votre entrepôt des données Amazon Redshift sans serveur en utilisant un exemple de jeu de données. Amazon Redshift sans serveur charge automatiquement l'exemple de jeu de données pendant le processus de création. Vous pouvez effectuer des requêtes immédiatement sur les données après la création de l'entrepôt des données. [Pour plus d'informations sur la façon de configurer Amazon Redshift Serverless pour la première fois, consultez Redshift Serverless.](#)

Utilisation de groupes de travail

Pour isoler les charges de travail et gérer des ressources dans Amazon Redshift sans serveur, vous pouvez créer des groupes de travail et des espaces de noms. Le groupe de travail lié à l'informatique regroupe des ressources informatiques comme les RPU et les groupes de sous-réseau VPC. 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](#).

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

Vous devez terminer la configuration initiale d'Amazon Redshift sans serveur avant de passer à ces étapes. 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](#).

Suivez ces étapes pour créer 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 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. Pour plus d'informations sur les VPC, consultez [Vue d'ensemble des VPC et des sous-réseaux](#).
4. 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](#).
5. Sous Subnet (Sous-réseau), spécifiez un ou plusieurs sous-réseaux à associer à votre base de données. Ces sous-réseaux font partie du VPC 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](#).
6. 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).

Création d'un groupe de travail de prévisualisation

Pour tester les nouvelles fonctions d'Amazon Redshift sans serveur, vous pouvez créer un groupe de travail Amazon Redshift sans serveur dans Aperçu. Vous ne pouvez pas utiliser ces fonctions dans la production ni déplacer votre groupe de travail Preview (Aperçu) vers un groupe de travail de production. Pour connaître les conditions générales de la version préliminaire, consultez Versions Bêta et préliminaires dans les [Conditions générales du service AWS](#).

Les fonctions suivantes ne sont actuellement pas disponibles dans des groupes de travail en version préliminaire :

- [Utilisation des intégrations zéro ETL](#)

Pour créer un groupe de travail dans Preview (Aperçu)

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dans le menu de navigation, choisissez Tableau de bord sans serveur, puis Configuration de groupe de travail. Les groupes de travail actuellement associés à votre compte Région AWS sont répertoriés. Un sous-ensemble des propriétés de chaque groupe de travail s'affiche dans les colonnes de la liste.
3. Une bannière sur la page Configuration de groupe de travail présente un aperçu des groupes de travail. Cliquez sur le bouton Create preview workgroup (Créer un groupe de travail en version préliminaire) pour ouvrir la page de création d'un groupe de travail.
4. Saisissez les propriétés de votre groupe de travail. Nous vous recommandons de saisir un nom pour le groupe de travail qui indique qu'il est en version préliminaire. Choisissez les options pour votre groupe de travail, y compris les options étiquetées -preview, pour les fonctions que vous souhaitez tester. Continuez à parcourir les pages pour saisir les options pour votre groupe de

travail et votre espace de noms. Pour des informations générales sur la création de groupes de travail, consultez [the section called “Création d’un groupe de travail avec un espace de noms”](#).

5. Choisissez Créer pour créer un groupe de travail en version préliminaire.
6. Lorsque votre groupe de travail en version préliminaire est disponible, utilisez votre client SQL pour charger et interroger des données.

Pour plus d’informations sur la version préliminaire dans des clusters provisionnés, consultez [Création d’un cluster de prévisualisation](#).

Affichage des propriétés d’un groupe de travail

Dans Amazon Redshift sans serveur, un groupe de travail est une collection de ressources prêtes à être utilisées. Lorsque vous choisissez Amazon Redshift Serverless, dans la AWS console, vous pouvez sélectionner 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.
- Creation date (Date de création) : la date à laquelle le groupe de travail a été créé.
- Balises : balises associées au groupe de travail.

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 2.1 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](#).

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

- **Network and security (Réseau et sécurité)** : vous pouvez voir les propriétés du réseau, telles que l'identifiant Virtual private cloud (VPC) [Cloud privé virtuel (VPC)], la liste VPC security group (Groupes de sécurité VPC), les paramètres Enhanced VPC routing (Routage VPC amélioré) et Publicly accessible (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.

- 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 [Compréhension de la capacité 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 [Aperçu des ressources de balisage](#).

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](#).

Utilisation des 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](#).

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. Tel est le cas des 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.

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 created (Date de création) : la date 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. Tel est le cas des 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](#).

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)**.

Modification de la AWS KMS clé d'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 entreprise.

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

Modification d'une AWS KMS clé à l'aide de la console

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 Amazon Redshift Serverless 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 entreprise.

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

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
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.

Modification des clés AWS KMS de chiffrement à l'aide du AWS CLI

update-namespace À utiliser pour 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.

Limites

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.

Gestion des limites d'utilisation, des limites des requêtes et d'autres tâches administratives

Vous pouvez configurer les paramètres de la console pour contrôler l'utilisation et limiter les coûts.

Gestion 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 :
 - Connectez-vous à la table système : ajoutez un enregistrement à la vue système [SYS_QUERY_HISTORY](#). Vous pouvez interroger la `usage_limit` colonne 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 Cross-Region data sharing usage limit (Limite d'utilisation du partage de données entre régions), qui limite la quantité de données transférées de la région productrice à 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](#).

Gestion 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.

Filtrage de requêtes

Vous pouvez utiliser les filtres disponibles sur le tableau de bord sans serveur. Pour filtrer des requêtes, effectuez les opérations suivantes :

1. Sur la gauche du volet Query summary (Récapitulatif des requêtes), sélectionnez la liste déroulante pour filtrer en fonction des requêtes terminées, des requêtes ayant échoué ou des deux.
2. À droite du volet Query summary (Récapitulatif des requêtes), sélectionnez la liste déroulante pour filtrer en fonction des requêtes en cours d'exécution, des requêtes en file d'attente ou des deux.

Modification de votre mot de passe administrateur

1. Choisissez Namespace configuration (Configuration d'espace de noms). Choisissez ensuite Change admin password (Changer le mot de passe administrateur). Une boîte de dialogue s'affiche.
2. Vous pouvez spécifier une valeur pour New admin username (Nouveau nom d'utilisateur administrateur) et New admin user password (Nouveau mot de passe d'utilisateur administrateur).
3. Choisissez Enregistrer.

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

Le tableau de bord Amazon Redshift Serverless contient un ensemble de panneaux qui présentent des at-a-glance métriques et des informations sur votre groupe de travail et votre espace de noms. 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.
- **Unités de partage des données** : affiche le nombre d'unités de partage des données utilisés pour partager des données entre, par exemple, des comptes 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.

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

Surveillance des requêtes et de la charge 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.

Octroi d'un accès pour surveiller les 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. Choisissez <https://console.aws.amazon.com/iam/>.
2. Sous Access Management (Gestion des accès), choisissez Politiques (politiques).
3. Choisissez Create Policy (Créer une politique).
4. Choisissez JSON, puis collez la définition de politique suivante.

```
{
  "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 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. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du 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](#) du 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.

Pour accorder une autorisation 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.

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";
```

Pour accorder une autorisation 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.

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 "IAM: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 "IAM:role-name";
```

Vues de surveillance

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 les commandes COPY et UNLOAD pour charger ou décharger des

données, et vous devez surveiller de près la progression en termes d'octets / lignes transférés et de fichiers terminés pour suivre le respect des accords de niveau de service métier. Cela se fait normalement en exécutant fréquemment des requêtes de table système (c'est-à-dire toutes les minutes) pour suivre la progression et générer des alertes donnant lieu à des enquêtes/mesures correctives 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](#).

Journalisation d'audit pour Amazon Redshift sans serveur

Exportation de journaux

Vous pouvez configurer Amazon Redshift Serverless pour exporter les données 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 consulter les métriques. Vous pouvez utiliser CloudWatch les journaux pour stocker vos enregistrements de journal 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 respectifs 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.

Surveillance des événements du journal dans 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 métriques et un accès client prédéfinis, vous pouvez utiliser une configuration automatisée, 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 journaux dans Amazon CloudWatch 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 AWS CLI, ou l'API Amazon CloudWatch Logs. Pour plus d'informations sur la modification des périodes de conservation des CloudWatch journaux dans les journaux, consultez la section Conservation des données des journaux des modifications 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, 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](#).

Métriques Amazon Redshift sans serveur

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 [Présentation des groupes de travail et des espaces de noms d'Amazon Redshift sans serveur](#).

CloudWatch les métriques de calcul sont les suivantes :

CloudWatch calculer des métriques

Nom de la métrique	Unités	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}

Nom de la métrique	Unités	Description	Jeux de dimensions
QueryDuration	Microsecondes	Durée moyenne pour exécuter une requête.	{Base de données LatencyRange, groupe de travail}, {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}

Nom de la métrique	Unités	Description	Jeux de dimensions
ComputeCapacity	RPU	Nombre moyen d'unités de calcul allouées au cours des 30 dernières minutes, arrondi à l'entier le plus proche.	{Workgroup}
ComputeSeconds	secondes de RPU	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	Unités	Description	Jeux de dimensions
UsageLimitAvailable	Heures RPU ou To	<p>En fonction de UsageType , UsageLimitAvailable renvoie ce qui suit :</p> <ul style="list-style-type: none"> • Si la valeur UsageType est SERVERLESS_COMPUTE , UsageLimitAvailable renvoie le nombre d'heures de RPU restantes que le groupe de travail peut interroger dans la limite donnée. • S'il s'agit de CROSS_REGION_DATASHARING, UsageLimitAvailable renvoie le nombre de To restants 	{UsageLimitId, UsageType, Groupe de travail}

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

Nom de la métrique	Unités	Description	Jeux de dimensions
UsageLimitConsumed	Heures RPU ou To	<p>En fonction de UsageType , UsageLimitConsumed renvoie ce qui suit :</p> <ul style="list-style-type: none"> • Si la valeur UsageType est SERVERLESS_COMPUTE , UsageLimitConsumed renvoie le nombre d'heures de RPU que le groupe de travail a déjà demandées dans la limite spécifiée. • S'il s'agit de CROSS_REGION_DATASHARING, UsageLimitConsumed renvoie le nombre de To que le client a déjà utilisés 	{UsageLimitId, UsageType, Groupe de travail}

Nom de la métrique	Unités	Description	Jeux de dimensions
		pour scanner dans la limite spécifiée.	

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

CloudWatch métriques relatives aux données et au stockage

Nom de la métrique	Unités	Description	Jeux de dimensions
TotalTableCount	Nombre de tables	Le nombre de tables d'utilisateurs existant à un moment donné. Ce total n'inclut pas les tables Amazon Redshift Spectrum.	{Database, Namespace}
DataStorage	Mégaoctets	Le nombre de mégaoctets utilisés, en disque ou en espace de stockage, pour les données Redshift.	{Namespace}

La SnapshotStorage métrique est indépendante de l'espace de nommage et du groupe de travail.

CloudWatchLa SnapshotStorage métrique est la suivante :

CloudWatch SnapshotStorage métrique

Nom de la métrique	Unités	Description	Jeux de dimensions
SnapshotStorage	Mégaoctets	Le nombre de mégaoctets utilisés, en disque ou en espace de stockage, pour les instantanés.	{}

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 :

CloudWatch dimensions et valeurs de dimension

Dimension	Description et valeurs
DatabaseName	Nom de la base de données. Une valeur personnalisée.
Latency	Les valeurs possibles sont les suivantes : <ul style="list-style-type: none"> 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 :

Dimension	Description et valeurs
	<ul style="list-style-type: none">• 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 de la 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.
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.

Dimension	Description et valeurs
UsageType	La fonctionnalité Amazon Redshift sans serveur est limitée. Les valeurs possibles sont les suivantes : <ul style="list-style-type: none">• SERVERLESS_COMPUTE• CROSS_REGION_DATASHARING

Utilisation des instantanés et des points de récupération

Une sauvegarde dans Amazon Redshift Serverless est une point-in-time représentation des objets et des données de 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. Les points de récupération sont créés toutes les 30 minutes et conservés pendant 24 heures.

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 dans un cluster provisionné, vous devez choisir le type de nœud à utiliser, tel que RA3, ainsi que 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 comptes AWS, ce qui leur permet d'accéder aux données contenues dans l'instantané et d'exécuter des requêtes.

Instantanés

Vous pouvez restaurer un instantané que vous avez créé sur la console Amazon Redshift sans serveur vers un espace de noms disponible associé à un groupe de travail. Un espace de noms est disponible lorsqu'il est prêt à être interrogé et/ou modifié. Vous ne pouvez pas restaurer un instantané chiffré avec une clé KMS gérée par AWS dans un espace de noms sans serveur..

Pour afficher une liste de tous vos instantanés, choisissez Data backup (Sauvegarde des données) dans la console Amazon Redshift sans serveur.

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.

Pour mettre à jour la période de conservation d'un instantané

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

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.

Pour créer un instantané final de toutes les données dans un espace de noms avant de supprimer 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 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).

Pour partager un instantané avec un autre compte AWS ou retirer l'accès d'un compte à un instantané

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.

Restauration d'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 provisionné

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](#).

Points de récupération

Les points de récupération d'Amazon Redshift sans serveur sont créés toutes les 30 minutes environ et enregistrés pendant 24 heures.

Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données) pour gérer les points de récupération. Vous pouvez effectuer les opérations suivantes :

- Restauration d'un point de récupération dans un espace de noms sans serveur.
- Convertir un point de récupération en instantané.

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).

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.

Planification d'instantanés

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	, - * /
Heures	0 – 23	, - * /
Day-of-month	1–31	, - * ? / L W
Mois	1–12 ou JAN–DEC	, - * /
Day-of-week	1–7 ou dim.–sam.	, - * ? 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 ? dans le ay-of-week champ D.
- 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 D 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 day-of-week champ. Par exemple, « 3#1,6#3 » n'est pas valide, car il est interprété comme deux expressions.

Limites

- 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.			

Minutes	Heures	Jour de la semaine	Signification			
30	0/6	SAT-SUN	Le samedi et le dimanche, toutes les 6 heures, 30 minutes 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 *)
```

Actuellement, vous pouvez uniquement utiliser l'API Amazon Redshift sans serveur ou AWS CLI pour créer une planification d'instantané. Pour plus d'informations sur ces opérations, consultez [Utilisation d'AWS CLI et de l'API Amazon Redshift sans serveur](#).

Copie des sauvegardes dans une autre Région AWS

Vous pouvez configurer Amazon Redshift sans serveur pour copier automatiquement les instantanés et les points de récupération dans une autre Région AWS. Lorsque vous créez un instantané dans la Région AWS source, il est copié dans une région de destination. Vous pouvez configurer votre espace de noms de manière à ce qu'il copie les instantanés et les points de récupération dans une seule Région AWS de destination à la fois. Pour obtenir la liste des Régions AWS où Amazon

Redshift sans serveur est disponible, consultez les points de terminaison répertoriés pour l'[API Redshift sans serveur](#) 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 chiffrées à l'aide d'une clé qu'AWS gère pour vous. Pour utiliser une autre clé, choisissez la clé que vous souhaitez utiliser lorsque vous configurez la copie des sauvegardes dans la Région AWS source, et Amazon Redshift sans serveur crée automatiquement un octroi, qui active le chiffrement des instantanés dans la Région AWS de destination.

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 Région AWS de destination dans laquelle copier l'instantané.
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 clé AWS KMS à utiliser pour le chiffrement 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.

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.

Utilisation de l'AWS Command Line Interface ou de l'API Amazon Redshift sans serveur

Outre la console AWS, vous pouvez également utiliser AWS CLI ou l'API Amazon Redshift sans serveur pour interagir avec les instantanés et les points de récupération. 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
CreateSnapshot	create-snapshot	Crée un instantané. Les instantanés doivent être associés à un espace de noms, vous devez donc

Opération API	Commande de la CLI	Description
		inclure le nom d'un espace de noms dans votre requête. Par défaut, Amazon Redshift sans serveur conserve les instantanés pendant une période indéfinie, mais vous pouvez spécifier une période de conservation.
RestoreFromSnapshot	restore-from-snapshot	Restaure les bases de données dans un instantané, dans votre espace de noms. Si vous effectuez une restauration d'un instantané à partir d'Amazon Redshift sans serveur sur un cluster provisionné, vous devez spécifier le paramètre <code>snapshotArn</code> de l'instantané que vous restaurez. Sinon, si vous effectuez une restauration sans serveur vers une restauration sans serveur, vous pouvez spécifier <code>snapshotArn</code> ou <code>snapshotName</code> , mais pas les deux.

Opération API	Commande de la CLI	Description
RestoreTableFromSnapshot	restore-table-from-snapshot	Restaure une table à partir d'un instantané dans votre espace de noms Amazon Redshift sans serveur. Vous ne pouvez pas utiliser cette opération pour restaurer des tables avec des clés de tri entrelacées.
GetSnapshot	get-snapshot	Extrait des informations sur un instantané.
ListSnapshots	list-snapshots	Extrait des informations sur plusieurs instantanés.
DeleteSnapshot	delete-snapshot	Supprime un instantané.
RestoreFromRecoveryPoint	restore-from-recovery-point	Restaure les données dans un point de récupération, dans votre espace de noms.
RestoreTableFromRecoveryPoint	restore-table-from-recovery-point	Restaure une table depuis un point de récupération dans votre espace de noms Amazon Redshift sans serveur. Vous ne pouvez pas utiliser cette opération pour restaurer des tables avec des clés de tri entrelacées.
ConvertRecoveryPointToSnapshot	convert-recovery-point-to-instantané	Convertit un point de récupération en instantané.
GetRecoveryPoint	get-recovery-point	Extrait des informations sur un point de récupération.

Opération API	Commande de la CLI	Description
ListRecoveryPoints	list-recovery-points	Extrait des informations sur plusieurs points de récupération.

Pour planifier la création d'instantané, utilisez les opérations d'API suivantes.

Opération API	Commande de la CLI	Description
CreateScheduledAction	create-scheduled-action	Crée une action planifiée, qui contient un calendrier et une action Amazon Redshift sans serveur. Par exemple, vous pouvez créer un calendrier indiquant le moment d'exécuter l'opération d'API <code>CreateSnapshot</code> .
DeleteScheduledAction	delete-scheduled-action	Supprime une action planifiée.
GetScheduledAction	get-scheduled-action	Extrait des informations sur une action planifiée.
ListScheduledActions	list-scheduled-actions	Extrait des informations sur une liste d'actions planifiées.
UpdateScheduledAction	update-scheduled-action	Met à jour une action planifiée.

Partage de données dans Amazon Redshift sans serveur

Utilisez le partage de données pour partager un maximum d'informations cohérentes au fur up-to-date et à mesure de leur mise à jour dans Amazon Redshift Serverless.

Partage de données dans Amazon Redshift sans serveur

Grâce au partage de données, vous avez un accès direct aux données afin que vos utilisateurs puissent consulter le plus grand nombre d'informations cohérentes au fur et à mesure de leur mise à jour dans Amazon Redshift Serverless.

Mise en route du partage de données dans Amazon Redshift Serverless

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 [Mise en route du partage de données à l'aide de l'interface SQL](#) ou [Mise en route du partage de données à l'aide de la console](#) dans le Guide du développeur de base de données 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 entre ou entre elles. Compte AWS Comptes AWS 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 la console Amazon Redshift AWS Management Console, puis choisissez la console Amazon Redshift. Choisissez Configuration de l'espace de noms, puis Unités de partage des données. Suivez la procédure dans [Mise en route du partage de données à l'aide de la console](#) dans le Guide du développeur de base de données Amazon Redshift.

Pour commencer à partager des données Comptes AWS, ouvrez la console Amazon Redshift AWS Management Console, puis choisissez la console Amazon Redshift. Choisissez Unités de partage des données. Suivez la procédure dans [Mise en route du partage de données à l'aide de la console](#) dans le Guide du développeur de base de données Amazon Redshift.

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. Suivez les procédures détaillées dans la section [Création de bases de données à partir d'unités de partage des données](#).

Octroi d'un accès pour afficher des unités de partage des données à l'aide de la console

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](#).

Considérations relatives au partage de données dans Amazon Redshift sans serveur

Voici des considérations relatives à l'utilisation du partage de données dans Amazon Redshift sans serveur :

- Amazon Redshift prend uniquement en charge les clusters provisionnés des types d'instance `ra3.16xlarge`, `ra3.4xlarge` et `ra3.xlplus`, et le point de terminaison sans serveur comme producteurs ou consommateurs du partage de données.
- 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.

Aperçu des ressources de balisage

Dans AWS, les balises sont des étiquettes définies par l'utilisateur qui se composent de paires clé-valeur. Amazon Redshift sans serveur 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 souhaitez 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 services AWS ou avez des catégories standard pour votre entreprise, nous vous recommandons de créer les mêmes paires clé-valeur pour les ressources à des fins de cohérence.

Si vous supprimez une ressource, les balises associées sont supprimées. Vous pouvez utiliser à la fois la console Amazon Redshift Serverless AWS CLI et la console 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

Dans les sections suivantes, vous pouvez apprendre les bases de la création d'un entrepôt des données en lançant un ensemble de nœuds de calcul, appelé cluster Amazon Redshift.

Rubriques

- [Présentation d'Amazon Redshift](#)
- [Utilisez EC2-VPC lorsque vous créez votre cluster](#)
- [Alarme d'espace disque par défaut](#)
- [Statut du cluster](#)
- [Considérations relatives à l'utilisation des clusters provisionnés Amazon Redshift](#)
- [Opérations du cluster](#)
- [Configuration d'un déploiement multi-AZ](#)
- [Gestion des clusters à l'aide de la console](#)
- [Gestion des clusters à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift](#)
- [Gestion des clusters dans un VPC](#)
- [Historique des versions de cluster](#)

Présentation d'Amazon Redshift

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 des 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 RA3. Pour plus d'informations, consultez [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 RA3 ou DC2 en fonction des performances requises, de la taille des données et de la croissance prévue des données.

Les nœuds RA3 avec stockage géré vous permettent d'optimiser votre entrepôt des données en dimensionnant et en payant le calcul et le stockage géré indépendamment. Avec 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 RA3 en fonction de la quantité de données que vous traitez quotidiennement. Les clusters utilisant les types de nœuds RA3 sont lancés dans un cloud privé virtuel (VPC). Vous ne pouvez pas lancer de clusters RA3 en mode EC2 Classic. Pour plus d'informations, consultez [Création d'un cluster dans un VPC](#).

Le stockage géré par Amazon Redshift utilise de grands disques SSD haute performance dans chaque nœud RA3 pour un stockage local rapide et Amazon S3 pour un stockage durable à plus 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 en constante augmentation, le stockage géré vous permet d'adapter automatiquement la capacité de stockage de votre entrepôt de données indépendamment des nœuds de calcul.

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). Vous ne pouvez pas lancer de clusters DC2 dans EC2-Classic. Pour plus d'informations, consultez [Création d'un cluster 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 un seul nœud, le nœud est partagé pour les fonctionnalités « principal » et « calcul ». Les clusters à nœud unique ne sont pas recommandés pour l'exécution de 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 aux 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, comme les nœuds ou les instantanés, au sein d'une AWS région. Pour plus d'informations sur les quotas par défaut qui s'appliquent aux ressources Amazon Redshift, consultez

[Limites d'Amazon Redshift](#) dans Référence générale d'Amazon Web Services. Pour demander une augmentation, soumettez-nous un [Formulaire d'augmentation de limite Amazon Redshift](#).

Le coût de votre cluster dépend de la AWS région, du type de nœud, du nombre de nœuds et du fait que les nœuds sont réservés à l'avance ou non. 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 entêtes 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 de nœuds inférieur en fonction du quota appliqué à votre AWS compte dans la AWS région sélectionnée. Pour demander une augmentation, soumettez-nous un [Formulaire d'augmentation de limite 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.

Types de 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.xlplu s (nœud unique)	4	32	2	4 To	1	4 To ³
ra3.xlplus (multi-nœ uds)	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
ra3.16xla rge	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.

Types de nœud de calcul dense

Type de nœud	vCPU	RAM (Go)	Tranche par défaut par nœud	Stockage par nœud	Plage de nœuds	Capacité totale
dc2.large	2	15	2	SSD NVMe de 160 Go	1–32	5.12 To
dc2.8xlarge	32	244	16	SSD NVMe de 2,56 To	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 anciens noms 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
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 métriques Amazon CloudWatch . 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 effectué des tests et proof-of-concepts pour valider votre configuration de production. Pour plus d'informations, consultez [Achat de nœuds réservés pour Amazon Redshift](#).

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](#).

Utilisez EC2-VPC lorsque vous créez 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. Créez votre cluster à l'aide d'EC2-VPC. Si vous utilisez toujours EC2-Classique, nous vous recommandons d'utiliser EC2-VPC pour améliorer les performances et la sécurité. Pour plus d'informations sur ces plateformes réseau, consultez la section [Plateformes prises en charge](#) dans le guide de l'utilisateur Amazon EC2. Les paramètres de votre AWS compte déterminent si EC2-VPC ou EC2-Classique sont disponibles pour vous.

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 jumbo TCP/IP 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](#).

EC2-VPC

Lorsque vous utilisez EC2-VPC, votre cluster s'exécute dans un cloud privé virtuel (VPC) qui est logiquement isolé de votre compte. AWS Si vous allouez votre cluster dans EC2-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 [Groupes de sous-réseaux du cluster Amazon 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'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 depuis la fenêtre État du cluster sous CloudWatch Alarmes. Le nom est `percentage-disk-space-used-default-chaîne`. 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 s'appelle `< clustername >-default-alarm (< recipient >)` ; par exemple, `(notify@example.com). examplecluster-default-alarms`

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 ou modification 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.

État	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 Suppression d'un cluster .
final-snapshot	Amazon Redshift prend un instantané final du cluster avant de le supprimer. Pour plus d'informations, consultez 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 pour Amazon Redshift à l'aide de modules de sécurité matérielle .

État	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 Gestion des clusters 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 des clusters .
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 les clusters .
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 dans Amazon Redshift .
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 .

État	Description
updating-hsm	Amazon Redshift met à jour la configuration HSM. .

Considérations relatives à l'utilisation des clusters provisionnés 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.

Rubriques

- [Considérations sur les régions et les zones de disponibilité](#)
- [Maintenance du cluster](#)
- [Gestion des limites d'utilisation d'Amazon Redshift](#)
- [Fonctionnalités de mise en réseau prises en charge par les nœuds RA3](#)
- [Types de nœud](#)

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 dans 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.

Rubriques

- [Fenêtres de maintenance](#)
- [Report de la maintenance](#)
- [Sélection du suivi de maintenance des clusters](#)
- [Gestion des versions de cluster](#)
- [Restauration de la version de cluster](#)
- [Détermination de la version de maintenance du cluster](#)

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 (Melbourne) : 12:00 – 20:00 UTC
- Région Asie-Pacifique (Mumbai) : 16:30 – 03:00 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 (Tokyo) : 13:00 – 02:00 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 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. 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 à laquelle 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 de 45 jours au plus. 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 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 [Abonnement aux notifications d'événements d'un 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](#)
- [Gestion des clusters à l'aide de la console](#)
- [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 approuvée ou à la précédente.

Le suivi de maintenance 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 (Actuelle) et la version précédente est assignée au suivi Trailing (Précédente). Pour définir le suivi de maintenance du cluster, choisissez l'une des valeurs suivantes :

- Current (Actuelle) – Pour utiliser la version approuvée la plus récente du cluster.
- Trailing (Précédente) – Pour utiliser la version du cluster avant la version actuelle.
- Version préliminaire – Utilisez la version de cluster qui contient les nouvelles fonctionnalités disponibles pour la version préliminaire.

Par exemple, supposons que votre cluster exécute actuellement la version 1.0.2762 et que la version actuelle d'Amazon Redshift est 1.0.3072. Si vous définissez la valeur de suivi de maintenance sur Current (Actuelle), votre cluster sera mis à jour vers la version 1.0.3072 (la version approuvée suivante) au cours de la prochaine période de maintenance. Si vous définissez la valeur du suivi de maintenance sur Trailing (Précédente), votre cluster ne sera mis à jour que lorsqu'il y aura une version postérieure à la version 1.0.3072.

Pistes de la version préliminaire

Une piste de version préliminaire n'est pas toujours disponible pour la sélection. Lorsque vous choisissez une piste Version préliminaire, le nom de la piste doit également être sélectionné.

Les pistes de version préliminaire et les ressources connexes sont temporaires, ont des limites fonctionnelles et peuvent ne pas contenir toutes les fonctionnalités actuelles d'Amazon Redshift disponibles dans d'autres piste. Lorsque vous utilisez des pistes de version préliminaire :

- Utilisez la nouvelle console Amazon Redshift lorsque vous utilisez des pistes de version préliminaire. Par exemple, lorsque vous créez un cluster à utiliser avec des fonctions de version préliminaire.
- Vous ne pouvez pas faire passer un cluster d'une piste de version préliminaire à une autre piste.
- Vous ne pouvez pas faire passer un cluster d'une piste de version préliminaire actuelle à une piste de fin.
- Vous ne pouvez pas faire passer un cluster d'une piste de version préliminaire actuelle ou à une piste de fin.
- Vous ne pouvez pas restaurer depuis un instantané créé à partir d'une piste de version préliminaire différente.
- Vous pouvez uniquement utiliser la piste de version préliminaire lors de la création d'un nouveau cluster ou de la restauration à partir d'un instantané.
- Vous ne pouvez pas restaurer à partir d'un instantané créé depuis une piste de version préliminaire différente ou avec une version de maintenance de cluster ultérieure à la version de cluster de la piste de version préliminaire. Par exemple, lorsque vous restaurez un cluster sur une piste de version préliminaire, vous pouvez uniquement utiliser un instantané créé à partir d'une version de maintenance de cluster antérieure à celle de la piste de version préliminaire.

Changement de suivi de maintenance

Modifier le suivi d'un cluster est généralement une décision unique. Vous devez faire preuve de prudence lorsque vous procédez à cette modification. Si vous passez du suivi de maintenance Trailing (Précédente) à Current (Actuelle), nous mettrons à jour le cluster vers la version de suivi Current (Actuelle) pendant la prochaine fenêtre de maintenance. Cependant, si vous modifiez le suivi de maintenance sur Trailing (Précédente), nous ne mettrons à jour votre cluster que lorsqu'il y existera une version postérieure à la version de suivi Current (Actuelle).

Suivis de maintenance et Restauration

Un instantané hérite du suivi de maintenance du cluster source. Si vous modifiez le suivi de maintenance du cluster source après avoir pris un instantané, l'instantané et le cluster source disposeront donc de suivis de maintenance différents. Lorsque vous effectuez une restauration à partir de l'instantané, le nouveau cluster héritera donc du suivi de maintenance du cluster

source. Vous pourrez modifier le suivi de maintenance une fois la restauration terminée. Le redimensionnement d'un cluster n'affecte pas le suivi de maintenance du cluster.

Gestion des versions de cluster

Un suivi de maintenance est composé d'une série de versions. Vous pouvez configurer votre cluster sur le suivi Current (Actuelle) ou sur le suivi Trailing (Précédente). Si vous configurez votre cluster sur le suivi Current (Actuelle), il sera toujours mis à jour vers la version la plus récente du cluster au cours de sa fenêtre de maintenance. Si vous configurez votre cluster sur le suivi Trailing (Précédente), il sera toujours exécuté sur la version de cluster publiée juste avant la version la plus récente.

La colonne Statut de la version de la liste des clusters de la console Amazon Redshift indique si l'un de vos clusters est disponible pour une mise à jour.

Restauration de la version de cluster

Si votre cluster est à jour avec la dernière version de cluster, vous pouvez choisir d'effectuer une restauration à la version précédente.

Pour obtenir des informations détaillées sur les fonctionnalités et améliorations incluses dans chaque version de cluster, consultez [Historique des versions de cluster](#).

Pour restaurer une version de cluster précédente

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
2. Dans le menu de navigation, choisissez Clusters.
3. Choisissez le cluster à restaurer.
4. Pour Actions, choisissez Version de cluster à restaurer. La page Version de cluster à restaurer apparaît.
5. Si une version est disponible pour la restauration, suivez les instructions de la page.
6. Choisissez Restaurer maintenant.

Détermination de la version de maintenance du cluster

Vous pouvez déterminer le moteur Amazon Redshift et la version de la base de données avec la console Amazon Redshift.

Pour rechercher la version d'un cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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. Les détails du cluster sont affichés, ce qui peut inclure les onglets Cluster performance (Performance du cluster), Query monitoring (Surveillance des requêtes), Databases (Bases de données), Datashares (Unités de partage des données), Schedules (Planifications), Maintenance et Properties (Propriétés).
3. Choisissez l'onglet Maintenance pour plus de détails.
4. Dans la section Maintenance, recherchez Version de cluster actuelle.

Note

Bien que la console affiche ces informations dans un même champ, il s'agit de deux paramètres dans l'API Amazon Redshift, `ClusterVersion` et `ClusterRevisionNumber`. Pour plus d'informations, consultez [Cluster](#) dans la Référence API Amazon Redshift.

Gestion des limites d'utilisation d'Amazon Redshift

Vous pouvez définir des limites pour surveiller et contrôler votre utilisation et le coût associé de certaines fonctions Amazon Redshift. Vous pouvez créer des limites d'utilisation quotidiennes, hebdomadaires et mensuelles, et définir des actions exécutées automatiquement par Amazon Redshift si ces limites sont atteintes. Les actions incluent notamment la consignation d'un événement dans une table système pour enregistrer une utilisation dépassant vos limites définies. Parmi les autres actions possibles, mentionnons l'envoi d'alertes avec Amazon SNS et Amazon CloudWatch pour notifier un administrateur et la désactivation d'une utilisation ultérieure pour contrôler les coûts.

Vous pouvez définir des limites d'utilisation pour chaque cluster. Une fois votre cluster créé, vous pouvez définir des limites d'utilisation pour les fonctionnalités suivantes :

- Amazon Redshift Spectrum
- Mise à l'échelle de la simultanéité Amazon Redshift
- Partage de données entre régions Amazon Redshift

Les limites d'utilisation sont disponibles avec la version 1.0.14677 ou ultérieure dans les régions AWS où la mise à l'échelle de la simultanéité Amazon Redshift Spectrum et Amazon Redshift sont disponibles.

Une limite Amazon Redshift spécifie le seuil de la quantité totale de données analysées par incréments de 1 To. Une limite de mise à l'échelle de la simultanéité spécifie le seuil de la durée totale utilisée par la mise à l'échelle de la simultanéité par incréments d'1 minute. Une limite de partage de données entre régions spécifie le seuil de la quantité totale de données analysées par incréments de 1 To.

Une limite peut être spécifiée pour une période quotidienne, hebdomadaire ou mensuelle (en utilisant UTC pour déterminer le début et la fin de la période). Si vous créez une limite au milieu d'une période, la limite est mesurée à partir de ce point jusqu'à la fin de la période. Par exemple, si vous créez une limite mensuelle le 15 mars, la première période mensuelle est mesurée du 15 au 31 mars.

Vous pouvez définir plusieurs limites d'utilisation pour chaque fonction. Chaque limite peut avoir une action différente. Les actions possibles sont les suivantes :

- Se connecter à la table système : il s'agit de l'action par défaut. Les informations sont consignées dans la table `STL_USAGE_CONTROL`. La journalisation est utile pour évaluer l'utilisation passée et décider des limites d'utilisation futures. Pour plus d'informations sur les éléments journalisés, consultez [STL_USAGE_CONTROL](#) dans le manuel du développeur de base de données Amazon Redshift.
- Alerte : Amazon Redshift émet des métriques CloudWatch pour l'utilisation disponible et consommée. Vous pouvez définir jusqu'à trois limites d'utilisation pour chaque fonction. Si vous activez l'action d'alerte à l'aide de la console Amazon Redshift, une alarme CloudWatch est automatiquement créée sur ces métriques. Vous pouvez éventuellement joindre un abonnement Amazon SNS à cette alarme. Si vous utilisez l'AWS CLI ou une opération d'API, assurez-vous de créer l'alarme CloudWatch manuellement. Lorsque le seuil est atteint, les événements sont également consignés dans une table système.
- Désactiver la fonction : lorsque le seuil est atteint, Amazon Redshift désactive la fonction jusqu'à ce que le quota soit actualisé pour la prochaine période (quotidienne, hebdomadaire ou mensuelle). Une seule limite pour chaque fonction peut avoir l'action de désactivation. Les événements sont également consignés dans une table système et des alertes peuvent être émises.

Les limites d'utilisation persistent jusqu'à ce que la définition de limite d'utilisation elle-même ou que le cluster soit supprimé.

Vous pouvez définir et gérer des limites d'utilisation avec la nouvelle console Amazon Redshift, l'AWS CLI ou avec les opérations d'API Amazon Redshift. Pour définir une limite sur la console Amazon Redshift, accédez à votre cluster et choisissez Configure usage limit (Configurer la limite d'utilisation) pour Actions. Pour afficher les limites d'utilisation précédemment définies pour votre cluster, accédez à votre cluster et choisissez l'onglet Maintenance, section Usage limits (Limites d'utilisation). Pour afficher la quantité d'utilisation disponible et consommée pour votre cluster, accédez à votre cluster. Sélectionnez l'onglet Cluster performance (Performances du cluster), puis affichez les graphiques correspondant à l'utilisation consommée pour une fonction.

Vous pouvez utiliser les opérations de la CLI Amazon Redshift suivantes pour gérer les limites d'utilisation. Pour plus d'informations, consultez la Référence des commandes d'AWS CLI.

- [create-usage-limit](#)
- [describe-usage-limits](#)
- [modify-usage-limit](#)
- [delete-usage-limit](#)

Vous pouvez utiliser les opérations d'API Amazon Redshift suivantes pour gérer les limites d'utilisation. Pour plus d'informations, consultez la référence d'API Amazon Redshift.

- [CreateUsageLimit](#)
- [DescribeUsageLimits](#)
- [ModifyUsageLimit](#)
- [DeleteUsageLimit](#)

Regardez la vidéo suivante pour savoir comment créer et surveiller des limites d'utilisation à l'aide de la console Amazon Redshift : [Cost Controls for Amazon Redshift Spectrum and Concurrency Scaling](#).

Fonctionnalités de mise en réseau prises en charge par les nœuds RA3

Les nœuds 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 :

- Point de terminaison VPC de cluster provisionné : lorsque vous créez ou restaurez un cluster 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 élastique dans votre AWS compte et l'attache au point de terminaison 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 Serverless](#).

- Clusters RA3 à sous-réseau unique – Vous pouvez créer un cluster 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 du cluster lorsque le sous-réseau ne comporte pas plusieurs zones de disponibilité (AZ).
- Clusters RA3 et groupes de sous-réseaux à sous-réseaux multiples : vous pouvez créer un cluster 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 que vous avez ajoutés précédemment ou en ajouter d'autres. Pour plus d'informations, consultez la section [Groupes de sous-réseaux du cluster Amazon Redshift](#).
- Accès aux points de terminaison entre comptes ou 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 géré par Redshift. Vous pouvez le configurer comme une connexion privée entre un VPC contenant un cluster ou un groupe de travail et un VPC dans lequel vous exécutez un outil client, par exemple. Vous pouvez ainsi accéder à l'entrepôt de données sans utiliser d'adresse IP publique et sans acheminer le trafic via Internet. Pour plus d'informations, consultez la section [Utilisation des points de terminaison VPC gérés par Redshift](#).
- Délocalisation du cluster : vous pouvez déplacer un cluster vers une autre zone de disponibilité (AZ) sans perte de données en cas d'interruption de service. Vous devez l'activer dans la console. Pour plus d'informations, consultez [Déplacement de votre 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 easy-to-read DNS qui achemine les connexions SQL-client vers le point de terminaison de votre cluster. Pour plus d'informations, consultez [Utilisation d'un nom de domaine personnalisé pour les connexions client](#).

Types de nœud

Ces sections détaillent les tâches disponibles pour les différents types de nœuds.

Rubriques

- [Nœuds RA3](#)
- [Types de nœuds DC2](#)

Nœuds RA3

Ces sections détaillent les tâches disponibles pour les nœuds RA3.

Rubriques

- [Présentation](#)
- [Mise à niveau vers des types de nœuds RA3](#)

Présentation

Les nœuds RA3 offrent 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.

Envisagez de choisir des types de nœuds 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.

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 les régions AWS](#).

⚠ 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 [Détermination de la version de maintenance du cluster](#).

Assurez-vous d'utiliser la nouvelle console Amazon Redshift lorsque vous travaillez avec les types de nœuds RA3.

En outre, pour utiliser les types de nœuds RA3 avec les opérations Amazon Redshift qui utilisent la piste de maintenance, la valeur de cette dernière doit être définie sur une version de cluster qui prend en charge RA3. Pour plus d'informations sur le suivi de maintenance, 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 RA3

Pour tirer parti de la séparation du calcul du stockage, vous pouvez créer ou mettre à niveau votre cluster avec le type de nœud RA3. Pour utiliser les types de nœuds 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 RA3, effectuez l'une des opérations suivantes :

- Ajoutez ou supprimez des nœuds avec l'opération de redimensionnement élastique. Dans certaines situations, la suppression de nœuds d'un cluster 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 des clusters](#). 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 des clusters](#).

Disponibilité du type de nœud RA3 dans les régions AWS

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 (Melbourne) (ap-southeast-4)
- Région Asie-Pacifique (Mumbai) (ap-south-1)

- 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 (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 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-Est) (us-gov-east-1)
- AWS GovCloud (US-Ouest) (us-gov-west-1)

Mise à niveau vers des types de nœuds RA3

Pour mettre à niveau votre type de nœud existant vers RA3, vous disposez des options suivantes afin de 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 RA3. Dès que la création du cluster est terminée (généralement en quelques minutes), les nœuds 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, RA3 préserve les informations relatives aux hot blocks de la charge de travail DC2 et remplit son cache local avec les blocs les plus actifs. 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 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 les clusters](#) 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 RA3 grâce au redimensionnement élastique. Pour plus d'informations, consultez [Elastic resize \(Redimensionnement élastique\)](#).

Le tableau suivant présente des recommandations lors de la mise à niveau vers des types de nœuds RA3. (Ces recommandations s'appliquent également aux nœuds réservés.)

Les recommandations de ce tableau 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. Provisionnez un cluster pour votre entrepôt de données POC au lieu de Redshift Serverless. Pour plus d'informations sur la réalisation d'une preuve de concept, consultez [Réaliser une preuve de concept \(POC\) pour Amazon Redshift dans le manuel Amazon Redshift Database Developer Guide](#).

Type de nœud existant	Nombre de nœuds existants	Nouveau type de nœud recommandé	Action de mise à niveau
dc2.8xlarge	2–15	ra3.4xlarge	Créez 2 nœuds de ra3.4xlarge pour chaque

Type de nœud existant	Nombre de nœuds existants	Nouveau type de nœud recommandé	Action de mise à niveau
			nœud de dc2.8xlarge ¹ .
dc2.8xlarge	16–128	ra3.16xlarge	Créez 1 nœud de ra3.16xlarge tous les 2 nœuds de dc2.8xlarge ¹ .
dc2.large	1 – 4	none	Conservez le cluster dc2.large existant.
dc2.large	5–15	ra3.xlplus	Créez 3 nœuds de ra3.xlplus tous les 8 nœuds de dc2.large ¹ .
dc2.large	16–32	ra3.4xlarge	Créez 1 nœud de ra3.4xlarge tous les 8 nœuds de dc2.large ^{1,2} .

¹Des 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.

²Les 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.

Types de nœuds DC2

Ces sections détaillent les tâches disponibles pour les types de nœuds DC2.

Opérations du cluster

Une fois le cluster créé, vous pouvez y effectuer plusieurs opérations. Les opérations incluent le redimensionnement, la pause, la reprise, le renommage et la suppression.

Rubriques

- [Redimensionnement des clusters](#)
- [Suspension et reprise des clusters](#)
- [Renommer les clusters](#)
- [Arrêt et suppression de clusters](#)
- [Déplacement de votre cluster](#)
- [Instantanés et sauvegardes Amazon Redshift](#)

Redimensionnement des clusters

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.

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 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. Cet instantané inclut toujours des [tables sans sauvegarde](#) pour les nœuds où cela est applicable. (Certains types de nœuds, comme RA3, n'ont pas de table sans sauvegarde.) 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, le rollback 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 passer à 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 des nœuds RA3, consultez [Mise à niveau vers des types de nœuds 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`.

- **Platform restriction (Restriction de plateforme)** : le redimensionnement élastique est disponible uniquement pour les clusters qui utilisent la plateforme EC2-VPC. Pour plus d'informations, consultez [Utilisez EC2-VPC lorsque vous créez 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-clusteroption`. 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 `dc2.large` 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 `dc2` prend en charge le redimensionnement élastique jusqu'au double du nombre de nœuds. Pour illustrer cela, vous pouvez ajouter un nœud à un cluster `dc2.8xlarge` à 4 nœuds pour en faire un cluster à cinq nœuds, ou ajouter d'autres nœuds jusqu'à atteindre huit nœuds.

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 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 ra3 prennent en charge une diminution du 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
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
dc2.8xlarge	2x	Jusqu'à la moitié du nombre (de 16 à 8 nœuds, par exemple)

Type de nœud d'origine	Limite d'augmentation	Limite de réduction
dc2.large	2x	Jusqu'à la moitié du nombre

Note

Choix des types de nœuds existants lorsque vous redimensionnez un cluster RA3 : si vous tentez de redimensionner un cluster contenant des nœuds 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 RA3 peut offrir une meilleure disponibilité

Le redimensionnement classique a été amélioré lorsque le type de nœud cible est 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 des performances et des résultats optimaux lorsque vous effectuez un redimensionnement classique vers un cluster 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 les nœuds 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 RA3

Lors d'un redimensionnement classique vers RA3, les tables avec une distribution KEY qui sont migrées comme une 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 classique lorsque le cluster cible est RA3

Le redimensionnement classique comprend les étapes suivantes, lorsque le type de cluster cible est RA3 et que vous remplissez les conditions préalables 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.

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 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 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 RA3 : si vous tentez de redimensionner un cluster contenant des nœuds 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 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 classique lorsque le cluster cible n'est pas RA3

Le redimensionnement classique consiste en ce qui suit, lorsque le type de nœud cible est autre que 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 RA3 ou qu'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.

Redimensionnement élastique vs redimensionnement classique

Attitude	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Comme res				
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				

Attitude	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Comme res				
			<p>dans votre cluster source, vous pouvez continuer à accéder aux journaux dans Amazon S3 ou dans Amazon S3 CloudWatch, après un redimensionnement. Vous pouvez conserver ou supprimer ces journaux, selon ce</p>				

Attitude	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Comme res				
			que vos stratégies de données spécifient.				

Attitude	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Comme res				
Modification des types de nœuds	<p>Pour le redimensionnement élastique, lorsque le type de nœud ne change pas : le redimensionnement sur place, et la plupart des requêtes sont conservées.</p> <p>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.</p>	<p>Pour le redimensionnement classique : un nouveau cluster est créé. Les requêtes sont supprimées lors du processus de redimensionnement.</p>					

Attitude	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.		

Attitude	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				

Attitude	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Comme res				
			<p>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.</p> <p>Pour le redimensionnement classique vers</p>				

Attitude	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Comme res				
			un cluster RA3, vous ne pouvez pas l'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, consultez [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 [create-scheduled-action dans la référence de AWS CLI commande ou Action](#) dans la référence d'API Amazon [CreateScheduledRedshift](#).

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 `exemplecluster` en `exemplecluster-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 `exemplecluster`. À partir de cet instant, toutes les applications qui utilisent le point de terminaison contenant `exemplecluster` 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.

Suspension et reprise des clusters

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 :

- Clusters EC2-Classical.

- 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.
- Les tables sans sauvegarde sur le cluster ne sont pas restaurées à la reprise. Pour plus d'informations sur les tables sans sauvegarde, consultez [Exclusion des tables des instantanés](#).
- 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](#)

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.

Renommer les clusters

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](#).

Arrêt et suppression de clusters

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. Vous pouvez par la suite restaurer l'instantané si vous souhaitez reprendre l'exécution du cluster et l'interrogation des données.

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. Pour plus d'informations sur l'arrêt et la suppression des clusters, consultez [Suppression d'un cluster](#).

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.

Déplacement de votre 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 des clusters Amazon Redshift est prise en charge uniquement pour les types d'instances RA3 comme ra3.16xlarge, ra3.4xlarge et ra3.xlplus. Les types d'instances RA3 utilisent

Redshift Managed Storage (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 désactivée par défaut sur tous les clusters RA3. 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 AWS CLI Amazon Redshift ou l'API Amazon Redshift. Pour modifier le port par défaut d'un groupe de travail sans serveur, utilisez l'API sans serveur Amazon Redshift AWS CLI ou l'API Amazon Redshift.

Si vous activez la relocalisation et que vous utilisez l'adresse IP du nœud principal pour accéder à votre cluster, assurez-vous de 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-vc-Endpoints` pour obtenir l'interface Elastic Network 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 commandes Amazon Redshift, consultez la section AWS CLI Commandes [disponibles dans le manuel de référence des AWS CLI commandes](#).

Note

Pour rappel, la relocalisation du cluster n'est pas une condition préalable à la configuration de fonctionnalités réseau Redshift supplémentaires. Par exemple, vous pouvez le compléter par

une [copie d'instantanés entre régions](#), afin de renforcer la résilience de votre environnement, mais cela n'est pas obligatoire. Il n'est pas non plus 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, 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](#).

Limites

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 de produits 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.

Activation de la relocalisation des clusters

Vous pouvez activer et gérer la relocalisation de clusters à partir de la console Amazon Redshift et de l'AWS CLI API Amazon Redshift.

Pour activer la relocalisation des clusters, définissez un groupe de sous-réseaux comprenant plusieurs zones de disponibilité. Si Amazon Redshift identifie plusieurs zones de disponibilité accessibles, il en choisit automatiquement une dans la liste pour déplacer le cluster.

Une fois la relocalisation terminée, vous utilisez le même point de terminaison pour accéder au cluster. Amazon Redshift supprime les ressources de calcul du cluster d'origine et les renvoie au groupe de ressources.

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.

Activation de la relocalisation lors de la création d'un cluster

Procédez comme suit pour activer la relocalisation lors de la création d'un cluster.

Pour activer la relocalisation d'un cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
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 les [clusters provisionnés Amazon Redshift](#) dans le guide de démarrage Amazon Redshift.
4. Sous Backup (Sauvegarde), choisissez Enable (Activer) pour Cluster relocation (Relocalisation du cluster). La relocalisation est désactivée 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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. 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 Backup (Sauvegarde), choisissez Enabled (Activé). La relocalisation est désactivée 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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 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 .

Avec la AWS CLI, l'exemple de commande suivant crée un cluster Amazon Redshift nommé **mycluster** dont la relocalisation est activée.

```
aws redshift create-cluster --cluster-identifiant mycluster --number-of-nodes 2 --
master-username enter a username --master-user-password enter a password --node-type
ra3.4xlarge --port 5439 --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-identifiant mycluster --port 5439
```

L'exemple de commande suivant inclut le `availability-zone-relocation` paramètre sur le cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifiant mycluster --availability-zone-
relocation
```

L'exemple de commande suivant désactive le `availability-zone-relocation` paramètre sur le cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifiant mycluster --no-availability-zone-
relocation
```

L'exemple de commande suivant invoque la relocalisation du cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifiant mycluster --availability-zone us-
east-1b
```

Instantanés et sauvegardes Amazon Redshift

Rubriques

- [Présentation des instantanés](#)
- [Instantanés automatiques](#)
- [Planifications d'un instantané automatique](#)
- [Format de la planification d'instantané](#)
- [Instantanés manuels](#)
- [Gestion du stockage des instantanés](#)
- [Exclusion des tables des instantanés](#)
- [Copie d'instantanés sur une autre région AWS](#)
- [Restauration d'un cluster à partir d'un instantané](#)
- [Restauration d'une table à partir d'un instantané](#)
- [Partage d'un instantané](#)
- [Gestion d'instantanés à l'aide de la console](#)
- [Gestion des instantanés à l'aide de l'API Amazon Redshift AWS CLI et de l'API Amazon Redshift](#)
- [Utilisation des AWS Backup](#)

Présentation des instantanés

Les snapshots sont point-in-time des sauvegardes d'un cluster. 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 AWS Management Console `describe-cluster-snapshots` dans la CLI ou dans l'action de l'API `Snapshots.DescribeCluster`](#) 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](#).

Utilisation de snapshots et de sauvegardes dans Amazon Redshift Serverless

Amazon Redshift Serverless, comme un cluster provisionné, vous permet d'effectuer une sauvegarde en tant que point-in-time représentation des objets et des données de l'espace de noms. Il existe deux types de sauvegardes dans Amazon Redshift Serverless : les instantanés créés manuellement et les points de restauration créés automatiquement par Amazon Redshift Serverless. Pour plus d'informations sur l'utilisation des instantanés pour Amazon Redshift Serverless, consultez la page [Utilisation des instantanés et des points de restauration](#).

Vous pouvez également restaurer un instantané d'un cluster provisionné vers un espace de noms sans serveur. Pour plus d'informations, consultez [Restaurer 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.

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 automatisés pour les types de nœuds RA3. Vous pouvez définir une période de conservation automatisée de type nœud RA3 allant de 1 à 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 est conservé 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 cron de type Unix.

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 planifications utilise une syntaxe [cron](#) de type Unix 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	, - * /
Jour du mois	1–31	, - * ? / L W
Mois	1–12 ou JAN–DEC	, - * /
Jour de la semaine	1–7 ou dim.–sam.	, - * ? 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 ? dans le ay-of-week champ D.
- 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 ay-of-week champ D 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 day-of-week champ. Par exemple, « 3#1,6#3 » n'est pas valide, car il est interprété comme deux expressions.

Limites

- 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 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-identifiant "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](#).

Gestion du stockage des 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 des instantanés manuels à l'aide de la commande CLI [batch-delete-cluster-snapshots AWS Management Console](#) ou à l'aide de la commande CLI.

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.

Copie d'instantanés sur une autre région AWS

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. Que ce soit dans les régions AWS source ou de destination, les instantanés manuels sont supprimés à la fin de leur période de conservation 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 des instantanés chiffrés vers une 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.

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_START – REDSHIFT-EVENT-2008 envoyé lorsque le processus de restauration commence.
2. RESTORE_SUCESS – 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 RA3 émettent uniquement des événements RESTORE_START et RESTORE_SUCCESS. Il n'y a pas de transfert de données explicite à effectuer après la réussite d'un RESTORE, car les types de nœuds RA3 stockent les données dans le stockage géré par Amazon Redshift. Avec les nœuds RA3, les données sont transférées en continu entre les nœuds RA3 et le stockage géré par Amazon Redshift dans le cadre du traitement normal des requêtes. Les nœuds RA3 mettent en cache les données sensibles localement et conservent automatiquement les blocs moins fréquemment interrogés dans le stockage géré par Amazon Redshift.

Vous pouvez suivre la progression d'une restauration en appelant l'opération [DescribeClustersAPI](#) ou en consultant les détails du cluster dans le AWS Management Console. 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 souhaitons 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 choisissons de restaurer dans un cluster composé de trois nœuds.

```
{  
  "NodeConfigurationOptionList": [  
    {  
      "EstimatedDiskUtilizationPercent": 65.26134808858235,  
      "NodeType": "dc2.large",  
      "NumberOfNodes": 24  
    },  
    {  
      "EstimatedDiskUtilizationPercent": 32.630674044291176,  
      "NodeType": "dc2.large",  
      "NumberOfNodes": 48  
    },  
    {  
      "EstimatedDiskUtilizationPercent": 65.26134808858235,  
      "NodeType": "dc2.8xlarge",  
      "NumberOfNodes": 3  
    },  
    {  
      "EstimatedDiskUtilizationPercent": 48.94601106643677,  
      "NodeType": "dc2.8xlarge",  
      "NumberOfNodes": 4  
    },  
    {  
      "EstimatedDiskUtilizationPercent": 39.156808853149414,  
      "NodeType": "dc2.8xlarge",  
      "NumberOfNodes": 5  
    },  
    {  
      "EstimatedDiskUtilizationPercent": 32.630674044291176,  
      "NodeType": "dc2.8xlarge",  
      "NumberOfNodes": 6  
    }  
  ]  
}
```

}

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 regroupées dans trois nœuds `dc2.8xlarge`.

```
aws redshift restore-from-cluster-snapshot --region eu-west-1 --snapshot-identifier
mycluster-snapshot --cluster-identifier mycluster-123456789012-x --node-type
dc2.8xlarge --number-of-nodes 3
```

Si vous avez des nœuds réservés, par exemple des nœuds réservés DC2, vous pouvez passer à des nœuds réservés RA3. 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 des nœuds RA3, consultez [Mise à niveau vers des types de nœuds 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.

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 AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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.

Exemple 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-identifiant mycluster-  
example  
  
--new-table-name my-new-table  
--snapshot-identifiant my-snapshot-id  
--source-database-name sample-  
database  
  
--source-table-name my-source-table
```

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 :

```
{
  "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 :

```
{
  "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 une politique telle que la suivante :

```

{
  "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.

Gestion d'instantanés à l'aide de la console

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. Cette section explique comment gérer vos instantanés dans la console Amazon Redshift. Pour plus d'informations sur les instantanés, consultez [Instantanés et sauvegardes Amazon Redshift](#).

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.

Rubriques

- [Création d'une planification d'instantané](#)
- [Création d'un instantané manuel](#)
- [Modification de la période de conservation d'un instantané manuel](#)
- [Suppression d'instantanés manuels](#)
- [Copie d'un instantané automatique](#)
- [Restauration d'un cluster à partir d'un instantané](#)
- [Restauration d'un espace de noms sans serveur à partir d'un instantané](#)
- [Partage d'un instantané de cluster](#)
- [Configuration d'une copie d'instantané entre régions pour un cluster non chiffré](#)
- [Configuration d'une copie instantanée entre régions pour un cluster AWS KMS chiffré](#)
- [Modification de la période de conservation pour la copie d'instantanés entre régions](#)

Création d'une planification d'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 AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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.

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 [Création d'un instantané de cluster](#).

Pour créer un snapshot manuel

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

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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](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).

Suppression d'instantanés manuels

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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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).

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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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.

Restauration d'un cluster à partir d'un instantané

Lorsque vous restaurez un cluster à partir d'un instantané, Amazon Redshift crée un nouveau cluster avec toutes les données de l'instantané sur le nouveau cluster.

Pour restaurer le cluster à partir d'un instantané

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

Si vous AWS Secrets Manager ne gérez pas le mot de passe administrateur de votre cluster, vous pouvez lui demander de gérer votre cluster restauré en choisissant Gérer les informations d'identification d'administrateur AWS Secrets Manager dans la section Configuration du cluster et en spécifiant une clé KSM. Dans le cas contraire, le cluster est restauré avec les informations d'identification d'administrateur qu'il possédait au moment de la prise de l'instantané. Vous pouvez mettre à jour les informations d'identification d'administrateur du cluster sur la page de détails du cluster après l'avoir restauré.

Si vous avez AWS Secrets Manager géré le mot de passe administrateur de votre cluster au moment où la capture d'écran a été prise, 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, par exemple des nœuds réservés DC2, vous pouvez passer à des nœuds réservés RA3. 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 des nœuds RA3, consultez [Mise à niveau vers des types de nœuds RA3](#).

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 [Travailler avec des instantanés et des points de récupération](#). Amazon Redshift convertit automatiquement les tables comportant des clés

entrelacées en clés composées lorsque vous restaurez un instantané de cluster provisionné dans un espace de noms Amazon Redshift Serverless. 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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](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.

Partage d'un instantané de cluster

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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](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 AWS KMS utilisée pour créer l'instantané soit partagée avec le ou les comptes effectuant 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 [DescribeKey](#) la documentation de référence de l'API Amazon Redshift.

La politique des clés gérée par le client peut être mise à jour par programme ou dans la AWS Key Management Service console.

Autoriser l'accès à la clé AWS 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 politique de clé KMS avec le nom de ressource Amazon (ARN) du AWS compte sur lequel vous partagez, comme indiqué `Principal` dans la politique 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`.

```
{
  "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 AWS Identity and Access Management (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

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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](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. Choisissez Enregistrer.

Configuration d'une copie instantanée entre régions pour un cluster AWS KMS chiffré

Lorsque vous lancez un cluster Amazon Redshift, vous pouvez choisir de le chiffrer à l'aide d'une clé racine provenant du AWS Key Management Service (AWS KMS). Les clés AWS KMS sont spécifiques à une AWS région. Si vous souhaitez activer la copie instantanée entre régions pour un cluster AWS KMS chiffré, vous devez configurer une autorisation de copie instantanée pour une clé racine dans la région de destination AWS. 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 des instantanés chiffrés vers une autre région AWS](#).

Pour configurer un instantané interrégional pour un cluster AWS KMS chiffré

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](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. Choisissez 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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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).

Gestion des instantanés à l'aide de l'API Amazon Redshift AWS CLI et de l'API Amazon Redshift

Vous pouvez utiliser les opérations d'interface de ligne de commande Amazon Redshift suivantes pour gérer les instantanés.

- [authorize-snapshot-access](#)
- [copy-cluster-snapshot](#)
- [create-cluster-snapshot](#)
- [delete-cluster-snapshot](#)
- [describe-cluster-snapshots](#)
- [disable-snapshot-copy](#)
- [enable-snapshot-copy](#)
- [modify-snapshot-copy-retention-period](#)
- [restore-from-cluster-snapshot](#)
- [revoke-snapshot-access](#)

Vous pouvez utiliser les actions d'API Amazon Redshift suivantes pour gérer les instantanés.

- [AuthorizeSnapshotAccès](#)
- [CopyClusterInstantané](#)
- [CreateClusterInstantané](#)
- [DeleteClusterInstantané](#)
- [DescribeClusterInstantanés](#)
- [DisableSnapshotCopier](#)
- [EnableSnapshotCopier](#)
- [ModifySnapshotCopyRetentionPériode](#)
- [RestoreFromClusterSnapshot](#)
- [RevokeSnapshotAccès](#)

Pour plus d'informations sur les instantanés Amazon Redshift, consultez [Instantanés et sauvegardes Amazon Redshift](#).

Utilisation des AWS Backup

AWS Backup est un service entièrement géré qui vous permet de centraliser et d'automatiser la protection des données sur les services AWS dans le cloud et sur site.

Avec AWS Backup pour 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 provisionnés Amazon Redshift. Cela vous permet d'automatiser et de consolider les tâches de sauvegarde que vous deviez effectuer séparément auparavant, sans aucun processus manuel.

Une sauvegarde, également appelée point de récupération, représente le contenu d'une ressource, comme un volume cluster Amazon Redshift, à un instant donné. Une sauvegarde fait généralement référence aux différentes sauvegardes des services AWS, tels que les instantanés Amazon Redshift. 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 sur AWS Backup, consultez [Working with backups](#) (Utilisation des sauvegardes).

Amazon Redshift est intégré en natif à AWS Backup. Cela vous permet de définir vos plans de sauvegarde et d'attribuer des ressources Amazon Redshift aux plans de sauvegarde. AWS Backup automatise la création d'instantanés manuels Amazon Redshift et stocke en toute sécurité ces instantanés dans un coffre-fort de sauvegarde chiffré que vous spécifiez dans votre plan de sauvegarde. Pour plus d'informations sur les coffres-forts, consultez [Working with backup vaults](#) (Utilisation des coffres-de sauvegarde). 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 [Managing backups using backup plans](#) (Gestion des sauvegardes à l'aide de plans de sauvegarde).

Rubriques

- [Considérations relatives à l'utilisation d'AWS Backup avec Amazon Redshift](#)
- [Gestion d'AWS Backup avec Amazon Redshift](#)

Considérations relatives à l'utilisation d'AWS Backup avec Amazon Redshift

Les sections suivantes décrivent les considérations et les limites relatives à l'utilisation d'AWS Backup avec Amazon Redshift.

Considérations relatives à l'utilisation d'AWS Backup avec Amazon Redshift

Voici des considérations relatives à l'utilisation d'AWS Backup avec Amazon Redshift :

- AWS Backup pour Amazon Redshift est disponible quand AWS Backup et Amazon Redshift sont disponibles dans la même Région AWS. Pour en savoir plus sur les zones de disponibilité d'AWS Backup, consultez [Disponibilité des fonctionnalités par Régions AWS](#).
- Pour commencer à utiliser AWS Backup, vérifiez que vous avez rempli toutes les conditions requises. Pour plus d'informations, veuillez consulter les [Prérequis](#).
- Inscrivez-vous au service AWS Backup. Les choix d'inscription s'appliquent au compte spécifique et à la Région AWS. Il se peut que vous deviez vous inscrire à plusieurs régions avec le même compte. Pour plus d'informations, consultez [Getting started 1: Service Opt-in](#) (Mise en route 1 : Inscription à l'aide d'un service).
- À partir de la console Amazon Redshift, vous pouvez créer des instantanés manuels et automatisés. AWS Backup ne prend en charge que les instantanés manuels pour le moment.
- Une fois que vous avez utilisé AWS Backup pour gérer les paramètres des instantanés, vous ne pouvez pas continuer à gérer les paramètres manuels des instantanés à l'aide d'Amazon Redshift. Vous pouvez cependant continuer à gérer les paramètres à l'aide d'un plan AWS Backup. Pour plus d'informations, consultez [Managing backups using backup plans](#) (Gestion des sauvegardes à l'aide de plans de sauvegarde).
- Pour réduire les coûts de stockage lorsque vous avez des compartiments Amazon S3 compatibles avec la gestion des versions à sauvegarder, nous vous recommandons de définir une règle d'expiration du cycle de vie. Pour plus d'informations sur la spécification d'une règle de cycle de vie, consultez [Exemple 6 : Spécification d'une règle de cycle de vie pour un compartiment activé pour la gestion des versions](#). Si vous ne définissez pas de période d'expiration du cycle de vie, vos coûts de stockage Amazon Redshift risquent d'augmenter car AWS Backup conserve toutes les versions de vos données Amazon Redshift.

Limites

Les limites suivantes s'appliquent à l'utilisation d'AWS Backup dans Amazon Redshift :

- Vous ne pouvez pas 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](#).
- AWS Backup n'est pas compatible avec Amazon Redshift sans serveur.

Gestion d'AWS Backup avec Amazon Redshift

Pour protéger les ressources de vos clusters provisionnés Amazon Redshift, vous pouvez utiliser la console AWS Backup ou utiliser par programmation l'API AWS Backup ou l'AWS Command Line Interface (AWS CLI). Lorsque vous avez besoin de récupérer une ressource, vous pouvez utiliser la console AWS Backup ou l'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 pour 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 plus d'informations, consultez la page [Amazon Redshift backups](#) (Sauvegardes Amazon Redshift).
- Automatisez la planification et la rétention des sauvegardes en configurant les plans de sauvegarde de manière centralisée.
- Restaurez un cluster vers la sauvegarde enregistrée de votre choix. Vous définissez la fréquence à laquelle vous souhaitez sauvegarder vos ressources. Pour plus d'informations, consultez [Restore an Amazon Redshift cluster](#) (Restaurer un cluster Amazon Redshift).

Configuration d'un déploiement multi-AZ

Amazon Redshift prend en charge les déploiements à plusieurs zones de disponibilité (multi-AZ) pour les clusters RA3 provisionnés. En utilisant des déploiements multi-AZ, votre entrepôt des données Amazon Redshift peut continuer à fonctionner en cas de défaillance lorsqu'un événement inattendu se produit dans une zone de disponibilité. Un déploiement multi-AZ 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 RA3 lors

de l'exécution d'un entrepôt des données multi-AZ. Les coûts de stockage restent les mêmes, car ils sont partagés entre toutes les zones de disponibilité d'une Région AWS.

Actuellement, Amazon Redshift prend en charge l'objectif de point de restauration zéro (RPO), ce qui permet aux données d'être à jour up-to-date en cas de panne. Grâce au déploiement multi-AZ, Amazon Redshift améliore encore ses capacités de récupération existantes et réduit son objectif de délai de reprise (RTO). Cela est possible, car un déploiement multi-AZ permet une reprise plus rapide en cas de défaillance ou de sinistre, portant ainsi le contrat de niveau de service (SLA) d'Amazon Redshift à 99,99 %, contre 99,9 % avec un entrepôt des données mono-AZ.

Configuration d'un déploiement multi-AZ

Pour configurer un déploiement Multi-AZ, sélectionnez l'option Multi-AZ et spécifiez le nombre de nœuds de calcul à provisionner dans chaque zone de disponibilité. Amazon Redshift déploie automatiquement des ressources de calcul égales sur 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. Cela permet à un déploiement multi-AZ d'agir comme un entrepôt des données unique avec un seul point de terminaison, éliminant ainsi le besoin de modifier les applications en cas de sinistre. Bien qu'un déploiement multi-AZ traite une requête individuelle à l'aide des ressources de calcul résidant dans une seule zone de disponibilité, il peut automatiquement répartir le traitement de plusieurs requêtes simultanées vers les deux zones de disponibilité, afin d'augmenter le débit global pour les charges de travail à simultanéité élevée.

Vous pouvez également convertir un entrepôt des données mono-AZ existant en un entrepôt des données multi-AZ 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 d'un cluster mono-AZ existant vers Multi-AZ, vous pouvez être amené à doubler le nombre de nœuds de cluster nécessaires, afin de faciliter le maintien des performances des requêtes uniques. La plupart des charges de travail observent une augmentation du débit global de traitement des requêtes avec un entrepôt des données multi-AZ, car les ressources de calcul disponibles sont deux fois plus nombreuses.

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

pendant ou après une panne peuvent subir des retards d'exécution pendant la restauration de l'entrepôt des données Multi-AZ.

Note

Pour obtenir de meilleures performances et une meilleure disponibilité, nous vous recommandons d'utiliser SNAPSHOT ISOLATION avec vos clusters multi-AZ. Pour plus d'informations, consultez [CREATE DATABASE](#).

Limites

Un entrepôt des données multi-AZ possède les mêmes capacités fonctionnelles qu'un entrepôt des données mono-AZ, à l'exception des limitations suivantes qui s'appliquent à un entrepôt des données multi-AZ :

- Vous ne pouvez pas créer d'entrepôt des données Multi-AZ non chiffré. Assurez-vous d'ajouter un chiffrement lors de la création d'un nouvel entrepôt des données multi-AZ, de la conversion d'un entrepôt des données mono-AZ en entrepôt des données multi-AZ ou de la conversion d'un entrepôt des données mono-AZ en entrepôt des données multi-AZ.
- Vous ne pouvez pas créer de déploiement multi-AZ à nœud unique pour aucun des types d'instances RA3. Sélectionnez 2 nœuds ou plus par zone de disponibilité lors de la création d'un déploiement multi-AZ.
- 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.
- Vous ne pouvez pas relocaliser un déploiement multi-AZ vers une autre zone de disponibilité. La relocalisation sera automatiquement déterminée et menée par Amazon Redshift lors de l'utilisation d'un déploiement multi-AZ.
- Vous ne pouvez pas suspendre ni reprendre un déploiement multi-AZ.
- Vous ne pouvez pas exécuter votre déploiement multi-AZ en dehors des plages de ports prises en charge : de 5431 à 5455 et de 8191 à 8215.
- Vous ne pouvez pas utiliser les vues STL, SVCS, SVL, SVV ni STV avec les déploiements multi-AZ, car ces derniers prennent en charge uniquement 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 élastique à un cluster existant lorsque le mode multi-AZ est activé.
- Vous ne pouvez pas convertir un cluster auquel est attachée une adresse IP élastique de type mono-AZ en cluster multi-AZ.
- Le déploiement multi-AZ d'Amazon Redshift est disponible dans les versions suivantes : Régions AWS
 - 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 (Hyderabad) (ap-south-2)
 - Asie-Pacifique (Jakarta) (ap-southeast-3)
 - 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 (Tokyo) (ap-northeast-1)
 - Canada (Centre) (ca-central-1)
 - Europe (Francfort) (eu-central-1)
 - Europe (Irlande) (eu-west-1)
 - 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)
 - Moyen-Orient (Bahreïn) (me-south-1)
 - Moyen-Orient (Émirats arabes unis) (me-central-1)

Rubriques

- [Gestion d'un déploiement multi-AZ](#)
- [Basculement d'un déploiement multi-AZ](#)
- [Surveillance des requêtes pour le fonctionnement multi-AZ](#)

Gestion d'un déploiement multi-AZ

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 des données mono-AZ existant en entrepôt des données multi-AZ ou restaurer un instantané pour le configurer en entrepôt des données multi-AZ.

À l'aide de la console Amazon Redshift, vous pouvez facilement créer de nouveaux déploiements Multi-AZ. Pour créer un nouveau déploiement multi-AZ à l'aide de la console Amazon Redshift, sélectionnez l'option Multi-AZ lors de la création de l'entrepôt des 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 données multi-AZ à l'aide du `multi-az` paramètre.

Vous pouvez convertir un entrepôt de données mono-AZ existant en entrepôt de données multi-AZ. Vous pouvez utiliser la console Amazon Redshift ou AWS CLI `modify-cluster` la commande utilisant le paramètre. `multi-az` Vous pouvez également effectuer une restauration à partir d'un instantané pour configurer un entrepôt de données mono-AZ dans un entrepôt de données multi-AZ à l'aide de la console Amazon Redshift ou de AWS CLI `restore-from-cluster-snapshot` la commande utilisant le paramètre. `multi-az`

Le déploiement multi-AZ ne prend en charge que les types de nœuds 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.

Configuration de Multi-AZ lors de la création d'un cluster

Vous pouvez configurer un déploiement multi-AZ lors de la création d'un nouveau cluster à l'aide de la console Amazon Redshift ou de l' AWS Command Line Interface.

Utilisation de la console

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
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. Sélectionnez l'un des types de nœuds RA3 dans la liste déroulante Node type (Type de nœud). L'option de configuration AZ n'est disponible que lorsque vous choisissez un type de nœud RA3.
6. Sous 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 Tackit 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 AWS Key Management Service clé 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 sur Create 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.

En utilisant le AWS Command Line Interface

Pour configurer le mode 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 ra3.4xlarge
  --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
```

Conversion d'un entrepôt des données mono-AZ en entrepôt des données multi-AZ

Avec la conversion d'un entrepôt des données mono-AZ en entrepôt des données multi-AZ, votre entrepôt des données sera hautement disponible avec une garantie SLA de 99,99 %. Les performances d'une requête individuelle resteront les mêmes avec un entrepôt des données multi-

AZ. 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 autorise pas à diviser les ressources de calcul existantes lors de la conversion d'un fonctionnement mono-AZ en fonctionnement 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 cluster mono-AZ en un entrepôt des données multi-AZ à l'aide de la console

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
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 déploiement multi-AZ. La page des détails du cluster s'affiche.
4. Pour Actions, choisissez Activer Multi-AZ. Le récapitulatif des modifications s'affiche. Cliquez sur Activer 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.

En utilisant le 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
```

Conversion d'un entrepôt des données multi-AZ en entrepôt des données mono-AZ

Avec la conversion d'un entrepôt des données multi-AZ en entrepôt des données mono-AZ, votre entrepôt des données ne bénéficiera pas de la garantie SLA de 99,99 % offerte par le fonctionnement 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 mettre à l'échelle automatiquement le débit afin d'obtenir des performances constantes, même avec un fonctionnement mono-AZ.

Note

Amazon Redshift ne vous autorise pas à diviser les ressources de calcul existantes lors de la conversion d'un fonctionnement mono-AZ en fonctionnement 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
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 déploiement multi-AZ. 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.

En utilisant le 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 que votre entrepôt des données est converti en entrepôt des données mono-AZ, il perd 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 des données multi-AZ

Vous pouvez redimensionner un entrepôt des données multi-AZ et spécifier un nombre de nœuds ou un type de nœud différent de la configuration actuelle de l'entrepôt des données.

Utilisation de la console

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
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 pour lequel vous souhaitez redimensionner l'entrepôt des données multi-AZ. 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 RA3 dans la liste déroulante Type de nœud.
7. Cliquez sur Redimensionner le cluster.

En utilisant le AWS Command Line Interface

Pour redimensionner un entrepôt de données multi-AZ 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-identifiant test-maz-11 \  
  --cluster-type multi-node \  
  --node-type ra3.4xlarge \  
  --number-of-nodes 6
```

Configuration du fonctionnement multi-AZ pour un entrepôt des données restauré à partir d'un instantané

Vous pouvez également créer un nouveau cluster multi-AZ en le restaurant à partir d'un instantané.

Utilisation de la console

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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 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. Sélectionnez l'un des types de nœuds RA3 dans la liste déroulante Node type (Type de nœud). L'option de configuration AZ n'est disponible que lorsque vous choisissez un type de nœud RA3.
6. Sous 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 Tackit 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 transférer vos propres données vers votre cluster Amazon Redshift, suivez les étapes décrites dans [Charger des 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 AWS Key Management Service clé 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.

En utilisant le 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-identifiant test-snap1
--cluster-identifiant test-saz-11
--endpoint-url https://redshift.eu-west-1.amazonaws.com/
```

Basculement d'un déploiement multi-AZ

Votre entrepôt des données multi-AZ est un ensemble de ressources de calcul 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 des données multi-AZ peut être automatiquement récupéré sans aucune intervention de l'utilisateur au cours d'un événement peu probable tel qu'une défaillance de zone de disponibilité ou 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 des données multi-AZ Amazon Redshift, le RPO est généralement égal à zéro, car toutes les données sont stockées dans le stockage géré Amazon Redshift (RMS), soutenu par Amazon Simple Storage Service, un service 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 dans quelle mesure le fonctionnement multi-AZ peut aider votre application à augmenter la haute disponibilité et à améliorer la continuité.

Utilisation de la console

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
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).

En utilisant le 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 récupération du cluster se termine avec succès, le déploiement multi-AZ devient disponible. Votre entrepôt des données multi-AZ provisionnera également automatiquement un nouveau calcul secondaire dans une troisième zone de disponibilité dès qu'elle sera disponible.

Au cours de ce processus, le statut du cluster sur la console apparaît comme étant en constante évolution, car le cluster est automatiquement restauré et reconfiguré pour revenir à la configuration de déploiement Multi-AZ. 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.

Surveillance des requêtes pour le fonctionnement multi-AZ

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.

Affichage des requêtes et des charges pour les entrepôts des données multi-AZ

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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
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 déploiement multi-AZ

Un déploiement multi-AZ utilise des ressources de calcul déployées dans les deux zones de disponibilité et qui 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 au sein du déploiement Multi-AZ :

1. Accédez à la console Amazon Redshift, connectez-vous à la base de données dans votre déploiement Multi-AZ et exécutez des requêtes via l'éditeur de requêtes.
2. Exécutez n'importe quel exemple de requête sur le déploiement multi-AZ Amazon Redshift.
3. Pour un déploiement multi-AZ, vous pouvez identifier une requête et la zone de disponibilité dans laquelle elle est exécutée en utilisant la colonne `compute_type` de la table `SYS_QUERY_HISTORY`. `primary` (principal) désigne les requêtes exécutées sur le cluster principal dans le déploiement Multi-AZ, et `secondary` (secondaire) représente les requêtes exécutées sur le cluster secondaire dans le déploiement Multi-AZ.

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 des clusters

Résiliation d'une requête pour des clusters

La procédure s'applique aux clusters multi-AZ et mono-AZ.

Pour résilier une requête

Vous pouvez également utiliser l'onglet Requetes 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
2. Dans le menu de navigation, choisissez REQUÊTES, puis choisissez Requetes 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.

Gestion des clusters à l'aide de la console

Pour créer, modifier, redimensionner, supprimer, redémarrer et sauvegarder des clusters, utilisez la section Clusters de la console Amazon Redshift.

Pour afficher les clusters

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

Rubriques

- [Création d'un cluster](#)
- [Création d'un cluster de prévisualisation](#)
- [Modification d'un cluster](#)
- [Suppression d'un cluster](#)
- [Redémarrage d'un cluster](#)
- [Redimensionnement d'un cluster](#)
- [Mise à niveau de la version d'un cluster](#)
- [Obtention d'informations sur la configuration du cluster](#)
- [Obtention d'une vue d'ensemble de l'état du cluster](#)
- [Création d'un instantané de cluster](#)
- [Création ou modification d'une alarme d'espace disque](#)
- [Utilisation des données de performance du cluster](#)

Création d'un cluster

Avant de créer un cluster, listez [Présentation d'Amazon Redshift](#) et [Clusters et nœuds dans Amazon Redshift](#).

Pour créer un cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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 Région AWS environnement qui prend en charge les types de nœuds RA3. Pour obtenir la Régions AWS liste des types de nœuds RA3 compatibles, consultez la section [Présentation des types de nœuds RA3](#) 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 un environnement Région AWS où Amazon Redshift Serverless n'est pas disponible, vous pouvez 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 Essai gratuit, vous créez une configuration avec le type de nœud dc2.large. Pour plus d'informations sur le choix d'un essai gratuit, accédez à [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 en savoir plus sur la tarification AWS Secrets Manager , consultez [Tarification d'AWS Secrets Manager](#).
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 AWS GovCloud régions (USA Est) et AWS GovCloud (USA Ouest). 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 voulez utiliser AWS Key Management Service (AWS KMS) ou un module de sécurité matérielle (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 de base de données pour Amazon Redshift à l'aide de 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 pour Amazon Redshift 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 de snapshots automatisés.

Période de conservation de l'instantané manuel

Vous pouvez choisir le nombre de jours ou l'option `Indefinitely` pour conserver ces instantanés.


Création d'un cluster de prévisualisation

Vous pouvez créer un cluster Amazon Redshift dans Preview (Aperçu) pour tester les nouvelles fonctions d'Amazon Redshift. Vous ne pouvez pas utiliser ces fonctions en production ni déplacer votre cluster de Preview (Aperçu) vers un cluster de production ou un cluster sur une autre piste. Pour voir les conditions générales, consultez Beta and Previews (Bêtas et aperçus) dans les [Conditions de service AWS](#).

Pour créer un cluster dans Preview (Aperçu)

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`](https://console.aws.amazon.com/redshiftv2/).

2. Dans le menu de navigation, choisissez Provisioned clusters dashboard (Tableau de bord des clusters provisionnés), puis 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.
3. Une bannière s'affiche sur la page de la liste Clusters qui présente la version préliminaire. Cliquez sur le bouton Create preview cluster (Créer un cluster en version préliminaire) pour ouvrir la page de création d'un cluster.
4. Saisissez les propriétés de votre cluster. Choisissez Preview track (Piste en version préliminaire) qui contient les fonctions que vous voulez tester. Nous vous recommandons de saisir un nom pour le cluster qui indique qu'il est sur une piste en version préliminaire. Choisissez les options pour votre cluster, y compris les options étiquetées -preview, pour les fonctions que vous souhaitez tester. Pour plus d'informations sur la création de clusters, consultez [Création d'un cluster](#) dans le Guide de gestion Amazon Redshift.
5. Choisissez Créer un cluster pour créer un cluster en version préliminaire.

 Note

Le suivi `preview_2023` est le suivi en version préliminaire le plus récent disponible. Ce suivi prend en charge la création de clusters avec des types de nœuds RA3 uniquement. Le type de nœud DC2 et tout autre type de nœud plus ancien ne sont pas pris en charge.

6. Lorsque votre cluster en version préliminaire est disponible, utilisez votre client SQL pour charger et interroger des données.

Pour en savoir plus sur la version préliminaire dans les groupes de travail Redshift sans serveur, consultez [Création d'un groupe de travail de prévisualisation](#).

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 AWS GovCloud régions (USA Est) et AWS GovCloud (USA Ouest). 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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](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.

Suppression d'un cluster

Si vous n'avez plus besoin de votre cluster, vous pouvez le supprimer. 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 supprimez votre cluster, mais que vous ne créez pas d'instantané manuel final, les données du cluster sont supprimées. Dans les deux cas, les instantanés automatiques sont supprimés une fois que le cluster a été supprimé, mais les instantanés manuels sont conservés jusqu'à ce que vous les supprimiez. Les coûts de stockage Amazon Simple Storage Service des instantanés manuels peuvent vous être facturés, en fonction de la quantité de stockage dont vous disposez pour les instantanés Amazon Redshift de vos clusters. Pour plus d'informations, consultez [Arrêt et suppression de clusters](#).

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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](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 capture finale, ou vous pouvez le supprimer avec un instantané final une fois la restauration terminée.

Redémarrage d'un cluster

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 AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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.

Redimensionnement d'un cluster

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 que le cluster est en cours de redimensionnement, vous ne pouvez pas exécuter de requête d'écriture ou de lecture/écriture sur le cluster ; vous ne pouvez exécuter que des requêtes en 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 des clusters](#).

Pour redimensionner un cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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 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 des nœuds RA3, consultez [Mise à niveau vers des types de nœuds RA3](#).

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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](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.

Obtention d'informations sur la configuration du cluster

Pour afficher les informations sur un cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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. Les détails du cluster sont affichés, ce qui peut inclure les onglets Cluster performance (Performance du cluster), Query monitoring (Surveillance des requêtes), Databases (Bases de données), Datashares (Unités de partage des données), Schedules (Planifications), Maintenance et Properties (Propriétés).
3. Choisissez chaque onglet pour afficher davantage de détails.

Obtention d'une vue d'ensemble de l'état du cluster

Pour afficher le statut d'un cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dans le menu de navigation, choisissez Clusters.
3. Affichez le statut du cluster dans la colonne Statut.

Création d'un instantané de cluster

Pour créer un instantané de cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dans le menu de navigation, choisissez Clusters.
3. Choisissez le cluster pour lequel vous souhaitez créer un instantané.
4. Pour Actions, choisissez Créer un instantané. La page Créer un instantané s'affiche.
5. Suivez les instructions indiquées sur la page.

6. Choisissez Créer un instantané.

Création ou modification d'une alarme d'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 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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.

Utilisation des données de performance du cluster

Dans la console, vous pouvez utiliser les performances du cluster sur l'onglet Performance du cluster de la page de détails du cluster.

Gestion des clusters à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift

Vous pouvez utiliser les AWS CLI opérations suivantes pour gérer les clusters dans Amazon Redshift.

- [cancel-resize](#)
- [create-cluster](#)
- [delete-cluster](#)
- [describe-clusters](#)
- [describe-cluster-versions](#)
- [describe-node-configuration-options](#)
- [describe-orderable-cluster-options](#)
- [describe-resize](#)
- [modify-cluster](#)

- [pause-cluster](#)
- [reboot-cluster](#)
- [resize-cluster](#)
- [resume-cluster](#)

Vous pouvez utiliser les opérations d'API Amazon Redshift suivantes pour gérer les clusters.

- [CancelResize](#)
- [CreateCluster](#)
- [DeleteCluster](#)
- [DescribeClusters](#)
- [DescribeClusterVersions](#)
- [DescribeNodeConfigurationOptions](#)
- [DescribeResize](#)
- [DescribeOrderableClusterOptions](#)
- [ModifyCluster](#)
- [PauseCluster](#)
- [RebootCluster](#)
- [ResizeCluster](#)
- [ResumeCluster](#)

Gestion des clusters dans un VPC

Rubriques

- [Présentation](#)
- [Création d'un cluster dans un VPC](#)
- [Gestion des groupes de sécurité VPC pour un Cluster](#)
- [Configuration des paramètres de communication des groupes de sécurité pour un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur](#)
- [Comment Amazon Redshift fonctionne avec le partage VPC pour les ressources AWS](#)
- [Groupes de sous-réseaux du cluster Amazon Redshift](#)

Présentation

Amazon Redshift prend en charge les plateformes EC2-VPC et EC2-Classic pour lancer un cluster dans un cloud privé virtuel (VPC) basé sur le service Amazon VPC. Pour plus d'informations, consultez [Utilisez EC2-VPC lorsque vous créez votre cluster](#).

Note

Amazon Redshift ne prend pas en charge le lancement des clusters dans des VPC de location dédiée. Pour plus d'informations, consultez [Instances dédiées](#) dans le Guide de l'utilisateur Amazon VPC pour les instances Linux.

Lors de la mise en service d'un cluster dans un VPC, vous devez effectuer les opérations suivantes :

- Fournissez des informations de VPC.

Lorsque vous demandez à Amazon Redshift de créer un cluster 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 du cluster afin qu'Amazon Redshift puisse allouer votre cluster dans l'un des sous-réseaux du VPC. Pour plus d'informations sur la création de groupes de sous-réseaux dans Amazon Redshift, consultez [Groupes de sous-réseaux du cluster Amazon Redshift](#). Pour plus d'informations sur la configuration du VPC, consultez [Démarrer avec Amazon VPC](#) dans le Guide de mise en route Amazon VPC.

- Le cas échéant, configurez les options accessibles au public.

Si vous configurez votre cluster 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 à votre cluster. 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. Il est associé à votre AWS compte.
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 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, veuillez consulter 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`

Supposons que vous ayez un cluster 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 du cluster 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 que le cluster soit redimensionné. Cela se produit même avec l'ensemble de paramètres précédent. Les nouveaux clusters 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 au cluster en dehors d'un VPC. Elle n'est pas liée aux adresses IP publiques ni aux adresses IP privées du nœud de cluster qui sont affichées dans la console Amazon Redshift sous `Connection details` (Détails de la connexion). 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.

L'option permettant d'associer un cluster 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.

- Associer un groupe de sécurité VPC.

Ensuite, vous accordez l'accès entrant à l'aide d'un groupe de sécurité VPC. Ce groupe de sécurité VPC doit autoriser l'accès via le port de la base de données au cluster afin que vous puissiez vous connecter à l'aide d'outils clients SQL. Vous pouvez le configurer à l'avance ou y ajouter des règles après avoir lancé le cluster. 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. Notez que vous ne pouvez pas utiliser les groupes de sécurité du cluster Amazon Redshift pour accorder l'accès entrant au cluster.

Pour plus d'informations sur l'utilisation de clusters dans le VPC, consultez [Création d'un cluster dans un VPC](#).

Restauration d'un instantané d'un cluster dans le VPC

Un instantané d'un cluster dans le 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 dans un VPC

Voici les grandes étapes que vous devez suivre pour déployer un cluster dans votre cloud privé virtuel (VPC).

Pour créer un cluster dans un VPC

1. Configurez un VPC.

Vous pouvez créer votre cluster 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 [Utilisez EC2-VPC lorsque vous créez votre cluster](#). Pour créer un VPC, consultez [Create a VPC](#) (Créer un 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.

Note

Vous devez disposer d'au moins un sous-réseau défini dans votre VPC afin de l'ajouter au groupe de sous-réseaux du cluster 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.

Vous pouvez créer un groupe de sous-réseaux du cluster à l'aide de la console Amazon Redshift ou par programmation. Pour plus d'informations, consultez [Groupes de sous-réseaux du cluster Amazon Redshift](#).

3. Autorisez l'accès aux connexions entrantes dans un groupe de sécurité VPC que vous associez au cluster.

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 au port que vous avez utilisé lorsque vous avez lancé le cluster. Pour voir des exemples de règles des groupes de sécurité, consultez [Règles des groupes de sécurité](#) dans le Guide de l'utilisateur de Amazon VPC.

4. Suivez les étapes décrites dans les [clusters provisionnés par Amazon Redshift](#) dans le guide de démarrage Amazon Redshift pour créer un cluster. Apportez les modifications suivantes lorsque vous créez votre cluster :

- Pour afficher la section Configurations supplémentaires, désactivez Utiliser les valeurs par défaut.

- Dans la section 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.

Vous êtes à présent prêt à utiliser le cluster. Vous pouvez suivre les étapes de mise en route pour tester le cluster, par exemple en chargeant des exemples de données et en essayant d'exécuter des exemples de requêtes.

Gestion des groupes de sécurité VPC pour un Cluster

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 êtes sur la plateforme EC2-VPC, vous pouvez utiliser un groupe de sécurité Amazon Redshift existant ou en définir un nouveau. Vous l'associez ensuite à un cluster tel que décrit ci-après. Si vous vous trouvez sur la plateforme EC2-Classique, définissez un groupe de sécurité du cluster et associez-le à un cluster. Pour plus d'informations sur l'utilisation des groupes de sécurité de cluster sur la plateforme EC2-Classique, consultez [Groupes de sécurité du cluster 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, les règles définies dans le groupe de sécurité VPC contrôlent l'accès au cluster.

Chaque cluster que vous allouez sur la plateforme EC2-VPC dispose d'un ou de plusieurs groupes de sécurité Amazon VPC associés à celle-ci. 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 du cluster. 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.

Le tableau ci-après décrit les règles par défaut pour le groupe de sécurité VPC par défaut.

Inbound			
Source	Protocol	Port Range	Comments
The security group ID (sg-xxxxxxx)	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 de votre cluster Amazon Redshift.

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 à votre cluster. Par exemple, supposons que vous exécutiez un service sur un cluster Amazon Redshift 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.

Vous pouvez créer jusqu'à 100 groupes de sécurité VPC pour un VPC et associer un groupe de sécurité VPC à plusieurs clusters. Toutefois, vous pouvez uniquement associer jusqu'à cinq groupes de sécurité VPC à un cluster donné.

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 les groupes de sécurité VPC à partir de <https://console.aws.amazon.com/vpc/>. Vous pouvez également gérer les groupes de sécurité VPC par programmation à l'aide de la CLI AWS CLI 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 sur la source 0.0.0.0/0 ou sur une adresse IP publique CIDR. 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](#).

- 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.
- 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 RA3, sélectionnez un port compris dans les plages 5431-5455 ou 8191-8215. Lorsque vous avez terminé, enregistrez chaque règle.
- 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 du cluster 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. Vous pouvez également 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 vers 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](#).

Comment Amazon Redshift fonctionne avec le partage VPC pour les ressources AWS

Le partage VPC vous permet de créer des ressources d' AWS application, telles que des instances Amazon EC2 et AWS d'autres services, dans un cloud privé virtuel (VPC) partagé et géré de manière centralisée. Le compte propriétaire du VPC (le propriétaire) partage un ou plusieurs sous-réseaux avec d'autres comptes (participants) appartenant à la même organisation. AWS Cela décrit comment créer et utiliser un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur dans un VPC partagé.

Les avantages du partage de VPC incluent le fait que vous n'avez pas à gérer autant de VPC et qu'il peut vous aider à simplifier votre réseau. L'avantage spécifique pour les administrateurs et les utilisateurs d'Amazon Redshift est que les ressources Redshift peuvent fonctionner de manière productive dans le VPC partagé. Pour plus d'informations sur le partage de VPC, consultez [Partager votre VPC avec d'autres comptes](#), qui décrit plus en détail les avantages du partage de VPC et son fonctionnement.

Utilisation des ressources de l'entrepôt des données Amazon Redshift dans un VPC partagé

Tout d'abord, il est important de comprendre qu'un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur ne peuvent pas être rendus visibles aux participants d'un sous-réseau partagé. Toutefois, cela n'empêche pas les participants de travailler avec la base de données du propriétaire dans un VPC partagé. Ceci est détaillé plus précisément dans les étapes qui suivent.

Avant de créer un cluster Amazon Redshift provisionné dans un VPC partagé, vous devez créer un groupe de sous-réseaux que vous avez l'intention d'utiliser pour Amazon Redshift. Cela doit inclure les sous-réseaux du VPC partagé que vous souhaitez utiliser. Lorsque vous créez votre cluster Amazon Redshift, vous devez choisir ce sous-réseau et également spécifier le groupe de sécurité du VPC partagé. De même, vous devez spécifier les sous-réseaux partagés et le groupe de sécurité que vous avez créé dans le VPC partagé lorsque vous créez le groupe de travail et la base de données Amazon Redshift sans serveur. Après avoir configuré vos sous-réseaux, effectuez les étapes suivantes pour configurer les ressources Redshift dans l'environnement partagé :

1. Le propriétaire du VPC crée un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur en utilisant un sous-réseau dans le VPC partagé.
2. Le propriétaire du VPC rend le cluster ou le groupe de travail disponible dans un scénario entre VPC. Les étapes sont décrites dans [Utilisation des points de terminaison de VPC gérés par](#)

[RedShift dans Amazon Redshift](#) pour un cluster provisionné ou dans [Connexion à Amazon Redshift sans serveur à partir d'un point de terminaison de VPC géré par Amazon Redshift](#) pour Amazon Redshift sans serveur. En activant la disponibilité entre VPC, ils peuvent mettre la base de données à la disposition des utilisateurs du même AWS compte ou d'autres comptes.

3. À l'inverse, grâce au partage de VPC, un propriétaire peut partager un sous-réseau avec un participant, et ce dernier peut créer un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur dans le sous-réseau. Toutefois, dans ce cas, le propriétaire ne peut pas consulter une ressource Amazon Redshift créée par un participant. Le cluster ou le groupe de travail doit être rendu accessible en activant la disponibilité entre VPC de la même manière que cela est décrit à l'étape précédente.

Notes d'utilisation relatives aux ressources Amazon Redshift dans un VPC partagé

Notez les comportements suivants concernant l'utilisation d'Amazon Redshift dans un sous-réseau partagé :

- Comme indiqué en détail dans la section précédente, le propriétaire du VPC ne peut pas partager un cluster Amazon Redshift ni un groupe de travail Amazon Redshift sans serveur avec un participant via le partage de VPC. Toutefois, le participant peut créer un cluster ou un groupe de travail Amazon Redshift sans serveur dans le sous-réseau du propriétaire. Dans ce cas, Amazon Redshift n'est pas visible pour le propriétaire via le partage de VPC.
- Le propriétaire du VPC ne peut pas afficher, mettre à jour ni supprimer un cluster provisionné Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur créé par le participant dans le sous-réseau partagé.
- Aucune autorisation n'est disponible pour permettre à un autre AWS compte d'accéder aux ressources Amazon Redshift que vous créez dans le VPC partagé.

Groupes de sous-réseaux du cluster Amazon Redshift

Présentation

Vous créez un groupe de sous-réseaux de cluster si vous mettez en service votre cluster dans votre Virtual Private Cloud (VPC). Pour de plus amples informations sur le VPC, veuillez consulter la page de détails du produit [Amazon VPC](#).

Votre VPC peut disposer d'un ou de plusieurs sous-réseaux, 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. Un groupe de sous-réseaux de cluster vous permet de spécifier un ensemble de sous-réseaux dans votre VPC. Lors de l'allocation d'un cluster, vous fournissez le groupe de sous-réseaux et Amazon Redshift crée le cluster sur l'un des sous-réseaux du groupe.

Pour plus d'informations sur la création d'un VPC, veuillez consulter la documentation du [Guide de l'utilisateur Amazon VPC](#).

Après avoir créé un groupe de sous-réseaux, vous pouvez supprimer les sous-réseaux ajoutés précédemment ou ajouter des sous-réseaux supplémentaires. Amazon Redshift fournit des fonctions d'API vous permettant de créer, de modifier ou de supprimer un groupe de sous-réseaux de cluster. Vous pouvez également effectuer ces opérations dans la console.

Gestion des groupes de sous-réseaux du cluster à l'aide de la console

Vous pouvez gérer vos groupes de sous-réseaux de cluster à l'aide de la console Amazon Redshift. Vous pouvez créer un groupe de sous-réseaux de cluster, ou bien gérer ou supprimer un groupe de sous-réseaux existant. Toutes ces tâches démarrent à partir de la liste des groupes de sous-réseaux du cluster. Vous devez sélectionner un groupe de sous-réseaux du cluster à gérer.

Vous pouvez mettre en service un cluster sur l'un des sous-réseaux que vous fournissez au groupe de sous-réseaux. Un groupe de sous-réseaux de cluster vous permet de spécifier un ensemble de sous-réseaux dans votre VPC.

Création d'un groupe de sous-réseaux de cluster.

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

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

Modification d'un groupe de sous-réseaux de cluster

Pour modifier un groupe de sous-réseaux de cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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 AWS connaissances [intitulé Comment déplacer mon cluster Amazon Redshift provisionné vers un sous-réseau différent ?](#), décrit un cas d'utilisation qui couvre le déplacement d'un cluster.

Suppression d'un groupe de sous-réseaux de cluster

Vous ne pouvez pas supprimer un groupe de sous-réseaux de cluster utilisé par un cluster.

Pour supprimer un groupe de sous-réseaux de cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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).

Gérez les groupes de sous-réseaux du cluster à l'aide de l'API Amazon Redshift AWS CLI et de l'API Amazon Redshift

Vous pouvez utiliser les opérations de la CLI Amazon Redshift suivantes pour gérer les groupes de sous-réseaux du cluster.

- [create-cluster-subnet-group](#)

- [delete-cluster-subnet-group](#)
- [describe-cluster-subnet-groups](#)
- [modify-cluster-subnet-group](#)

Vous pouvez utiliser les opérations d'API Amazon Redshift suivantes pour gérer les groupes de sous-réseaux du cluster.

- [CreateClusterSubnetGroup](#)
- [DeleteClusterSubnetGroup](#)
- [DescribeClusterSubnetGroups](#)
- [ModifyClusterSubnetGroup](#)

Historique des versions de cluster

Amazon Redshift publie périodiquement de nouvelles versions de cluster utilisées pour mettre à jour votre cluster.

Important

Pour plus d'informations sur les versions de cluster Amazon Redshift disponibles, leurs fonctions, leurs améliorations et leurs correctifs, consultez [Versions de cluster pour Amazon Redshift](#).

Utilisation des intégrations zéro ETL

Cette rubrique inclut la documentation préliminaire relative aux intégrations zéro ETL d'Aurora PostgreSQL et de RDS for MySQL à Amazon Redshift, qui sont disponibles en version préliminaire. La documentation et les fonctionnalités sont toutes sujettes à modification. Nous vous recommandons d'utiliser les intégrations zéro ETL de RDS for MySQL et d'Aurora PostgreSQL uniquement dans des environnements de test et non dans des environnements de production. Pour voir les conditions générales, consultez [Beta and Previews \(Bêtas et aperçus\)](#) dans les [Conditions de service AWS](#).

L'intégration zéro ETL est une solution entièrement gérée qui met à disposition les données transactionnelles ou opérationnelles dans Amazon Redshift en temps quasi réel. 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.

Avec l'intégration Zero-ETL, vous disposez de données plus récentes pour les analyses, l'IA/ML et les rapports. Vous obtenez des informations plus précises et plus opportunes pour des cas d'utilisation tels que les tableaux de bord en temps réel, 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 dans l'ensemble de l'entreprise.

Les sources suivantes sont actuellement prises en charge pour les intégrations zéro ETL :

- Aurora Édition compatible avec MySQL
- Aurora Édition compatible avec PostgreSQL (version préliminaire)
- RDS for MySQL (version préliminaire)

Pour créer une intégration zéro ETL, vous spécifiez une source d'intégration et un entrepôt des données Amazon Redshift comme cible. L'intégration réplique les données de la source vers

l'entrepôt des données cible. Les données sont mises à disposition en quelques secondes dans 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. Une intégration zéro ETL maintient vos ressources de calcul isolées de vos ressources de données. Vous utilisez ainsi les outils les plus efficaces pour traiter les 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 quasi réel 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 [Notifications d'événements d'intégration sans ETL 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 dans 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.

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_STATE](#) fournit des informations sur l'état de l'intégration.
- [SYS_INTEGRATION_TABLE_STATE_CHANGE](#) fournit des informations sur le journal des modifications de l'état des tables pour les intégrations.

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](#)

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.

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 et création de vues matérialisées avec les données répliquées](#)
- [Gestion des intégrations zéro ETL](#)
- [Métriques 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 sans serveur ou d'un type de nœud RA3 (ra3.16xlarge, ra3.4xlarge ou ra3.xlplus).
 - Chiffré (si vous utilisez un cluster provisionné).
 - La sensibilité à la casse est activée.
- Vous ne pouvez pas activer le support VPC amélioré sur les entrepôts des données dont les intégrations sont configurées.
- Si vous supprimez une source d'intégration autorisée pour un entrepôt des données Amazon Redshift, toutes les intégrations associées passeront à l'état FAILED.
- 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. L'actualisation des vues matérialisées avec des données répliquées à partir d'intégrations zéro ETL entraîne une actualisation complète de la vue. L'actualisation incrémentielle, la réécriture automatique des requêtes, l'actualisation automatique et les vues matérialisées automatisées ne sont pas prises en charge. Pour en savoir plus sur la création de vues matérialisées avec des données répliquées via des intégrations zéro ETL, consultez [Création de vues matérialisées avec les données répliquées](#).
- Vous pouvez interroger les tables uniquement dans l'entrepôt des données cible qui se trouvent dans l'état Synced. Pour plus d'informations, consultez [Métriques pour les intégrations zéro ETL](#).
- Amazon Redshift n'acceptant que les caractères UTF-8, il est 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.
- 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 réplification ne se poursuit pas et la table est mise en état d'échec. 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 la section Différences entre les types de données entre Aurora et Amazon Redshift](#) dans le guide de l'utilisateur Amazon Aurora.

- Les tables de la source d'intégration doivent avoir une clé primaire. Dans le cas contraire, vos tables ne pourront pas être répliquées vers l'entrepôt de données cible dans Amazon Redshift.
- Pour les intégrations zéro ETL d'Aurora PostgreSQL et de RDS for MySQL à Amazon Redshift, créez votre entrepôt des données cible en version préliminaire. Pour plus d'informations, consultez [Création et configuration d'un entrepôt des données Amazon Redshift cible](#).
- L'intégration Zero-ETL ne prend pas en charge les transformations lors de la réplication des données 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.
- Cela peut avoir un impact sur les autres charges de travail exécutées dans Amazon Redshift. Pour éliminer l'impact de l'intégration zéro ETL sur les autres charges de travail, envisagez d'utiliser un point de terminaison distinct pour l'intégration zéro ETL et de partager les données avec d'autres points de terminaison qui ont besoin d'accéder à ces données par le biais du partage de données.
- L'intégration Zero-ETL s'exécute dans Amazon Redshift à l'aide de connexions parallèles. Il s'exécute à l'aide des informations d'identification de l'utilisateur qui a créé la base de données à partir de l'intégration. Lorsque la requête est exécutée, la mise à l'échelle de la simultanéité n'intervient pas pour ces connexions lors de la synchronisation (écritures). Les lectures de dimensionnement simultanées (provenant des clients Amazon Redshift) fonctionnent pour les objets synchronisés.

Pour des considérations qui s'appliquent également à la source d'intégration, consultez l'une des rubriques suivantes :

- Pour les sources Aurora, consultez [Limitations](#) dans le Guide de l'utilisateur Amazon Aurora.
- Pour les sources Amazon RDS, consultez [Limitations](#) dans le Guide de l'utilisateur Amazon RDS.

Bien démarrer avec les intégrations zéro ETL

Avant de configurer votre intégration zéro ETL sur Amazon Redshift, spécifiez votre source d'intégration et configurez-la avec les autorisations et paramètres requis. Passez ensuite au reste de la configuration initiale depuis la console Amazon Redshift et AWS CLI

Pour créer une intégration zéro ETL d'Aurora à Amazon Redshift

Pour créer une intégration zéro ETL d'Aurora à Amazon Redshift, procédez comme suit :

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 créer une intégration zéro ETL de RDS à Amazon Redshift

Pour créer une intégration zéro ETL de RDS à Amazon Redshift, procédez comme suit :

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 step-by-step d'intégration, dans lequel vous spécifiez la base de données source et l'entrepôt de 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.

Création et configuration d'un entrepôt des données Amazon Redshift cible

Avant cette étape, créez votre source d'intégration et configurez les paramètres requis par le type de source pour les intégrations zéro ETL.

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.

Votre entrepôt des données cible doit présenter les caractéristiques suivantes :

- Exécuter Amazon Redshift sans serveur ou un cluster alloué du type d'instance ra3.16xlarge, ra3.4xlarge ou ra3.xlplus.
- 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 plus d'informations, consultez [Chiffrement de base de données Amazon Redshift](#).
- Créé dans la même AWS région que la source d'intégration.

Note

Pour les intégrations zéro ETL d'Aurora PostgreSQL et de RDS for MySQL à Amazon Redshift, tenez également compte des points suivants pour votre entrepôt des données cible :

- Vous devez créer votre entrepôt des données en version préliminaire sur le suivi `preview_2023`. Vous ne pouvez pas utiliser les fonctionnalités de version préliminaire en production ni déplacer votre entrepôt des données en version préliminaire vers un déploiement en production.

- Si vous choisissez de créer un cluster provisionné Amazon Redshift, ce cluster doit comporter au moins deux nœuds.
- Pour les sources Aurora PostgreSQL, vous devez créer votre entrepôt de données cible dans la région USA Est (Ohio). AWS Notez que vous devez créer votre base de données source pour les intégrations zéro ETL d'Aurora PostgreSQL à l'aide de l'[environnement de version préliminaire de base de données Amazon RDS](#).

Pour les sources RDS pour MySQL, vous devez créer votre entrepôt de données cible dans une AWS région prise en charge. Pour obtenir la liste des régions AWS où les intégrations zéro ETL de RDS for MySQL sont disponibles, consultez [Régions prises en charge pour les intégrations zéro ETL avec Amazon Redshift](#) dans le Guide de l'utilisateur Amazon RDS.

Pour créer votre entrepôt des données cible en version préliminaire pour vos intégrations zéro ETL d'Aurora PostgreSQL et de RDS for MySQL, consultez l'une des rubriques suivantes en fonction de votre type de déploiement :

- Pour créer un cluster provisionné Amazon Redshift en version préliminaire, consultez [Création d'un cluster de prévisualisation](#). Assurez-vous de choisir la piste `preview_2023` afin d'utiliser les intégrations zéro ETL.
- Pour créer un groupe de travail Amazon Redshift sans serveur en version préliminaire, consultez [Création d'un groupe de travail de prévisualisation](#).

Pour créer votre entrepôt des données cible pour vos intégrations zéro ETL d'Aurora MySQL, 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.

Vous pouvez créer un groupe de paramètres personnalisé à l'aide de la console Amazon Redshift ou de la manière AWS CLI suivante :

- À l'aide de la console Amazon Redshift : [Gestion des groupes de paramètres à l'aide de la console](#).
- En utilisant le AWS CLI — [Gestion des groupes de paramètres à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift](#)

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. Ceci est requis pour prendre en charge la sensibilité à la casse de MySQL et de PostgreSQL. `enable_case_sensitive_identifier` est une valeur de configuration qui détermine si les identifiants de nom des bases de données, des tables et des 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 distinction 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 distinction majuscules/minuscules pour les clusters provisionnés par Amazon Redshift à l'aide du AWS CLI](#)

Activez la distinction majuscules/minuscules pour Amazon Redshift Serverless à l'aide du AWS CLI

Exécutez la AWS CLI commande suivante pour activer la distinction majuscules/majuscules 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
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 distinction 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, dans le programme de votre terminal, exécutez la AWS CLI commande suivante 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-1.0 \  
    --description "Param group for zero-ETL integrations"
```

2. Exécutez la AWS CLI commande suivante pour activer la distinction 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 sans 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",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "source_arn"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "source_principal"
      },
      "Action": "redshift:CreateInboundIntegration"
    }
  ]
}
```

Voici un résumé des opérations d'API Amazon Redshift applicables à la configuration des politiques de ressources pour les intégrations :

- Utilisez l'opération [PutResourcePolicy](#) 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.
- L'opération de l'API [GetResourcePolicy](#) permet d'afficher les politiques de ressources existantes.
- Utilisez l'opération [DeleteResourcePolicy](#) 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](#).

Étapes suivantes

Maintenant que vous avez configuré l'autorisation de votre entrepôt des données Amazon Redshift cible, vous pouvez créer une intégration zéro ETL et commencer à répliquer les données.

Selon votre source, effectuez l'une des actions suivantes :

- Pour créer des intégrations zéro ETL d'Aurora, consultez [Création d'intégrations zéro ETL d'Amazon Aurora à Amazon Redshift](#) dans le Guide de l'utilisateur Amazon Aurora.
- Pour créer 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.

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 RDS ou Amazon Redshift.

Création d'une base de données de destination dans 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.

Création d'une base de données de destination à l'aide de la console Amazon Redshift

1. Dans le panneau de navigation de gauche, choisissez `Intégrations Zero-ETL`.
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. Saisissez un nom de base de données. L'ID d'intégration et le nom de l'entrepôt des données sont préremplis.

Pour les sources Aurora PostgreSQL, entrez également la base de données nommée que vous avez spécifiée lors de la création de votre intégration zéro ETL.

6. Choisissez `Créer une base de données`.

Création d'une base de données de destination à l'aide de l'éditeur de requêtes 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 les sources Aurora PostgreSQL, vous devez également inclure une référence à la base de données nommée au sein du cluster que vous avez spécifiée lorsque vous avez créé l'intégration. Par exemple :

```
CREATE DATABASE destination_db_name FROM INTEGRATION 'integration_id'  
DATABASE named_db;
```

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 [Gestion des intégrations zéro ETL](#).

Ajout de données à votre source

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.

Interrogation et création de vues matérialisées avec les données répliquées

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 les 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'interface de ligne de commande Amazon Redshift.

Création de vues matérialisées avec les données répliquées

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 tables *sales_zetl* et *event_zetl* à partir de la source *ticketit_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 as  
(SELECT eventname, sum(pricepaid) as total_price  
FROM zetl_int_db.ticketit_zetl.sales_zetl S, zetl_int_db.ticketit_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
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        |
+-----+-----+
```


Gestion des intégrations zéro ETL

Vous pouvez consulter les détails d'une intégration zéro ETL pour voir ses informations de configuration et son statut dans la console Amazon Redshift.

Pour afficher les détails d'une intégration zéro ETL

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
2. Dans le panneau de navigation de gauche, choisissez Sans serveur ou Tableau de bord des clusters alloués. Choisissez ensuite Intégrations zéro ETL.
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 Zero-ETL envoie des données transactionnelles à l'entrepôt de données Amazon Redshift cible.
 - `Syncing`— L'intégration Zero-ETL a rencontré une erreur récupérable et est en train de réensemencer les données. Les tables concernées ne peuvent pas être interrogées dans Amazon Redshift tant que leur resynchronisation n'est pas terminée.
 - `Failed`— L'intégration Zero-ETL a rencontré un événement ou une erreur irrécupérable qui ne peut pas être corrigée. Vous devez supprimer et recréer l'intégration Zero-ETL.
 - `Creating`— L'intégration Zero-ETL est en cours de création.
 - `Deleting`— L'intégration Zero-ETL est en cours de suppression.
 - `Needs attention`— L'intégration Zero-ETL a rencontré un événement ou une erreur nécessitant une intervention manuelle pour le résoudre. Pour corriger le problème, suivez les instructions du message d'erreur.
 - ARN source est l'ARN des données source.
 - Destination est l'ARN de l'espace de noms de l'entrepôt des données cible.
 - 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 destination** est le type d'entrepôt des données Amazon Redshift.
- **Date de création** est la date et l'heure (UTC) de la création de l'intégration.

Note

Pour visualiser les détails de l'intégration d'un entrepôt des données, choisissez la page de détails de votre espace de noms sans serveur ou de cluster provisionné, puis choisissez l'onglet Intégrations zéro ETL.

Dans la liste Intégrations zéro ETL, vous pouvez choisir Données de requête 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 Amazon Redshift](#).

Dans la liste Intégrations zéro ETL, vous pouvez choisir Partager les données pour créer une unité de partage des 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;
```

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.

Important

Pour partager des données d'un entrepôt des données en version préliminaire Amazon Redshift vers un entrepôt des données client Amazon Redshift, votre entrepôt des données client doit être sur le suivi `preview_2023`. Pour plus d'informations sur les unités de partage des données, consultez [Qu'est-ce qu'une unité de partage des données ?](#) dans le Guide du développeur de base de données Amazon Redshift.

Pour créer un entrepôt des données cible en mode Aperçu, consultez l'une des rubriques suivantes en fonction de votre type de déploiement :

- Cluster provisionné Amazon Redshift : [Création d'un cluster de prévisualisation](#)
- Groupe de travail Redshift sans serveur : [Création d'un groupe de travail de prévisualisation](#)

Partage de 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 panneau de navigation de gauche, choisissez Intégrations zéro ETL.
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](#).

Partage de données dans les clusters provisionnés 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 panneau de navigation de gauche, choisissez Intégrations zéro ETL.
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](#).

Métriques pour les intégrations zéro ETL

Vous pouvez utiliser les métriques de la console Amazon Redshift et d'Amazon CloudWatch pour en savoir plus sur l'état et les performances de vos intégrations sans 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 visualiser les métriques relatives à votre intégration dans la console Amazon Redshift, choisissez Intégrations zéro ETL dans le volet de navigation de gauche et choisissez votre ID d'intégration.

Pour les intégrations zéro ETL d'Aurora et d'Amazon RDS, Amazon Redshift fournit deux types de métriques sur la page de détails d'intégration pour une intégration. Les types de métriques sont les suivants :

- Dans l'onglet Métriques d'intégration, voici les graphiques disponibles :

Métrique	Description
Lag	<p>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.</p> <p>Unités : seconde</p> <p>Dimensions : IntegrationLag</p>
Tables replicated	<p>Nombre de tables qui ont été répliquées depuis votre base de données source vers Amazon Redshift.</p> <p>Unités : nombre</p> <p>Dimensions : IntegrationNumTablesReplicated</p>
Tables failed	<p>Nombre de tables dont la réplication a échoué.</p> <p>Unités : nombre</p> <p>Dimensions : IntegrationNumTablesFailedReplication</p>

- 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 :
 - 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.

Résolution des problèmes liés aux 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](#)
- [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](#)
- [Table dans l'état Resynchronisation requise ou Resynchronisation initiée](#)

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 base de données Aurora source exécute MySQL version 3.05 ou supérieure. 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. veuillez consulter [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. veuillez consulter [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](#).

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 plus d'informations, consultez [Création d'une base de données de destination dans Amazon Redshift](#).

Table dans l'état Resynchronisation requise ou Resynchronisation initiée

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 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](#)
- [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](#)
- [Table dans l'état Resynchronisation requise ou Resynchronisation initiée](#)

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 Aurora PostgreSQL version 15.4.99 ou ultérieure. 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. veuillez consulter [Activation de la sensibilité à la casse pour votre entrepôt des données](#).
- Vous avez ajouté le principal autorisé et la bonne source d'intégration 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](#).

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 plus d'informations, consultez [Création d'une base de données de destination dans Amazon Redshift](#).

Table dans l'état Resynchronisation requise ou Resynchronisation initiée

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](#)
- [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](#)
- [Table dans l'état Resynchronisation requise ou Resynchronisation initiée](#)

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 RDS pour MySQL version 8.0.32 ou supérieure. 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. veuillez consulter [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. veuillez consulter [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](#).

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 plus d'informations, consultez [Création d'une base de données de destination dans Amazon Redshift](#).

Table dans l'état Resynchronisation requise ou Resynchronisation initiée

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](#).

Interrogation d'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' AWS Management Console 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](#).

Rubriques

- [Connexion à Amazon Redshift](#)
- [Interrogation d'une base de données à l'aide de l'éditeur de requête v2 Amazon Redshift](#)

- [Interrogation d'une base de données à l'aide de l'éditeur de requête](#)
- [Connexion à un entrepôt de données Amazon Redshift à l'aide des outils client SQL](#)
- [Utilisation de l'API de données Amazon Redshift](#)

Connexion à Amazon Redshift

Vous pouvez vous connecter à votre base de données en utilisant 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 un compte donné Région AWS ont les mêmes caractéristiques `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 Amazon Redshift

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. Vous pouvez visualiser vos résultats dans des diagrammes et collaborer en partageant vos requêtes avec d'autres membres de votre équipe. 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 une 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 l'éditeur de requête v2 Amazon Redshift](#).

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.

Rubriques

- [Configuration de votre Compte AWS](#)
- [Utilisation de l'éditeur de requête v2](#)
- [Interaction avec l'assistant SQL génératif de l'éditeur de requêtes v2 \(version préliminaire\)](#)
- [Chargement de données dans une base de données](#)
- [Création et exécution de requêtes](#)

- [Création et exécution de blocs-notes](#)
- [Interrogation du AWS Glue Data Catalog](#)
- [Interrogation d'un lac de données](#)
- [Utilisation des unités de partage des données](#)
- [Planification d'une requête avec l'éditeur de requête v2](#)
- [Visualisation des résultats de requêtes](#)
- [Collaborer et partager en équipe](#)

Configuration de votre Compte AWS

Lorsque vous choisissez l'éditeur de requête v2 dans la console Amazon Redshift, un nouvel onglet de votre navigateur s'ouvre avec l'interface de l'éditeur de requête v2. Avec les autorisations appropriées, vous pouvez accéder aux données d'un cluster ou d'un groupe de travail Amazon Redshift dont vous êtes propriétaire et Compte AWS qui se trouve actuellement dans le cluster. 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'une clé gérée par le AWS KMS 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 plus d'informations, consultez [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 vous ou en votre nom Compte AWS et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour 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 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 AWS Resource Groups balises.

Vous pouvez configurer des rôles IAM avec des politiques IAM afin de partager des requêtes avec d'autres utilisateurs du même nom Compte AWS dans la Région AWS.

Création d'une clé gérée par le AWS KMS 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 de l'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 manuel du AWS Key Management Service développeur.

Stratégie de clé

Les politiques 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

[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 l'éditeur de requête v2 Amazon Redshift, 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' 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 par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez [Tâches nécessitant les informations d'identification de l'utilisateur racine](#) dans le Guide de l'utilisateur IAM.

```
{
  "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.region.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:region:111122223333:key/key_ID"
  }
]
}

```

Les ressources suivantes fournissent des informations supplémentaires sur AWS KMS les clés :

- Pour plus d'informations sur AWS KMS les politiques, consultez la section [Spécification des autorisations dans une politique](#) du Guide du AWS Key Management Service développeur.
- Pour plus d'informations sur AWS KMS les politiques de résolution des problèmes, 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 une autorisation.

(Nous vous recommandons d'associer des politiques à un rôle IAM et de l'attribuer à un utilisateur.) Ces politiques AWS gérées sont rédigées avec différentes options qui contrôlent la manière dont le balisage des ressources permet le partage des requêtes. Vous pouvez attacher des politiques IAM à l'aide de la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.

- `AmazonRedshiftQueryEditorV2 FullAccess` — Accorde 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.
- `AmazonRedshiftQueryEditorV2 NoSharing` — 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.
- `AmazonRedshiftQueryEditorV2 ReadSharing` — 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.
- `AmazonRedshiftQueryEditorReadWritePartage V2` — 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. Il a également besoin de l'autorisation `redshift:GetClusterCredentials` 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 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.

Au fur et 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. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du 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](#) du 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 administrateur AWS IAM Identity Center supprime toutes les associations d'ensembles d'autorisations pour un ensemble d'autorisations particulier dans l'ensemble du compte, l'accès aux ressources de l'éditeur de requêtes initialement associé à l'ensemble d'autorisations supprimé n'est plus disponible. Ultérieurement, si les mêmes autorisations sont recrées, 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 AWS Identity and Access Management, 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 à la console IAM AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/iam/>.
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 Add tag (Ajouter une balise) et entrez une valeur Key (Clé) de `RedshiftDbUser`, puis entrez la Value (Valeur) du nom d'utilisateur fédéré.
7. Vous pouvez également sélectionner Add tag (Ajouter une balise) et entrer la Key (Clé) de `RedshiftDbGroups`, puis entrer la Value (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 correctement configurés, 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 le signe 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 le transfert de balises principales personnalisées directement à l'éditeur de requêtes v2.

Utilisation de l'éditeur de requête v2

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.

Rubriques

- [Ouverture de l'éditeur de requête v2](#)
- [Connexion à une base de données Amazon Redshift](#)
- [Navigation dans une base de données Amazon Redshift](#)
- [Création d'objets de base de données](#)
- [Afficher l'historique des requêtes et des onglets](#)
- [Remarques concernant l'utilisation de l'éditeur de requête v2](#)
- [Modification des paramètres de compte](#)

Ouverture de l'éditeur de requête v2

Pour ouvrir l'éditeur de requête v2

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
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



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 (Raccourcis)



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 [Création et exécution de blocs-notes](#).

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 l'éditeur de requête v2 Amazon Redshift. 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 [Modification des paramètres de compte](#).

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 sur la configuration des connexions à IAM Identity Center, consultez [Connexion de Redshift à IAM Identity Center pour offrir aux utilisateurs 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 AWS Identity and Access Management 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 de connexion à la 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
 - fx* f_py_greater(float8,float8)
 - fx* f_sql_greater(float8,float8)
 - ▼  Stored procedures 1
 - fx* 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 AWS Glue, voir [Qu'est-ce que c'est 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 Create using 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 d'interroger une base de données créée à partir d'un AWS Glue Data Catalog, connectez-vous à votre 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 en utilisant AWS Glue Data Catalog, au

schéma que vous avez nommé dans le 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 reçu 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 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 sections [Travailler avec des partages de données gérés par Lake Formation en tant que consommateur](#) et [Travailler avec des partages de données gérés par Lake Formation en tant que producteur](#) dans le manuel [Amazon Redshift Database Developer Guide](#).

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



(Créer), puis Database (Base de données).

Create

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



(Créer), puis Schema (Schéma).

2. Saisissez un nom de schéma.
3. Choisissez Local ou External (Externe) pour le Schema type (Type de schéma).

Create

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 for PostgreSQL ou Amazon Aurora compatible PostgreSQL. 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 for MySQL ou Amazon Aurora compatible MySQL. 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 entêtes 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.

Remarques concernant l'utilisation de l'éditeur de requête v2

Tenez compte des points suivants lorsque vous utilisez l'éditeur de requête v2.

- La taille maximale du résultat de la requête est la plus petite, avec 5 Mo ou 100 000 lignes.
- 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 le bloc BEGIN-COMMIT ou BEGIN-ROLLBACK s'exécutent en une seule transaction. 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 IAM RoleSessionName contenant des virgules (.). Un message d'erreur similaire au suivant peut s'afficher :
« 'AROA123456789Example:MyText, yourtext' n'est pas une valeur valide pour TagValue - il contient des caractères non autorisés » Ce problème survient lorsque vous définissez un IAM contenant une virgule, puis RoleSessionName que vous utilisez l'éditeur de requêtes v2 avec ce rôle IAM.

Pour plus d'informations sur un IAMRoleSessionName, consultez la section [Attribut RoleSessionName SAML](#) dans le guide de l'utilisateur IAM.

Modification des paramètres de 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.

Interaction avec l'assistant SQL génératif de l'éditeur de requêtes v2 (version préliminaire)

Ceci est une documentation préliminaire pour l'assistant SQL génératif de l'éditeur de requêtes v2, qui est proposé en version préliminaire. La documentation et la fonction sont toutes deux sujettes à modification. Nous vous recommandons d'utiliser cette fonction uniquement dans des environnements de test et non dans des environnements de production. Pour connaître les conditions générales de la version préliminaire, consultez Participation au service Bêta dans les [AWS Conditions générales du service](#).

Note

Actuellement, le support SQL génératif n'est disponible que dans les domaines suivants Régions AWS :

- Région USA Est (Virginie du Nord) (us-east-1)
- Région USA Ouest (Oregon) (us-west-2)
- Région Europe (Francfort) (eu-central-1)

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.

Lorsque vous interagissez avec l'assistant SQL génératif, 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 « find top venues that sold the most tickets » (rechercher les sites qui ont vendu le plus de billets), fournissez plus de détails, comme « find names/ids of top three venues that sold the most tickets in 2008 » (rechercher les noms/identifiants des trois sites qui ont vendu le plus de billets en 2008). Utilisez des noms d'objets cohérents dans votre base de données, tels que les 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).

Considérations relatives à l'interaction avec l'assistant SQL génératif

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 de l'éditeur de requêtes v2, vous devez disposer d'une autorisation `sqlworkbench:GetQsSqlRecommendations` dans votre stratégie IAM, en plus des autres autorisations spécifiées dans la stratégie AWS gérée pour l'éditeur de requêtes v2. Pour plus d'informations sur les politiques AWS gérées, consultez [Accès 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 "IAM: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 la discussion de l'assistant SQL génératif de l'éditeur de requêtes v2 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'éditeur de requêtes v2 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) Choisissez Régénérer SQL pour générer une autre réponse pour la même invite. Vous pouvez choisir de régénérer SQL une fois pour l'invite en cours.
5. (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.

3. Sélectionnez SQL génératif pour activer l'assistant SQL génératif pour les utilisateurs du compte.

Exemple d'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 d'exemples 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 de l'éditeur de requêtes v2

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.

- 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
```

- 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 de l'éditeur de requêtes v2. 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.

Chargement d'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 enregistrés dans votre dossier Notebooks (Bloc-notes).

Les exemples de jeux de données suivants sont disponibles.

ticket

La plupart des exemples de la documentation Amazon Redshift utilisent un exemple de données appelé `ticket`. Ces données sont composées de sept tables : deux tables de faits et cinq dimensions. Lorsque vous chargez ces données, le schéma `ticket` est mis à jour avec des exemples de données. Pour plus d'informations sur les données `ticket`, 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



data (Charger les données).

Load

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 (Target table), notamment le cluster ou le groupe de travail (Cluster or workgroup), la base de données (Database), le schéma (Schema) et le nom de la Table où sont stockées 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



data (Charger les données).

Load

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 le 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`. L'option *optional-prefix* peut être spécifiée pour limiter l'utilisation de ce compartiment en rapport avec l'éditeur de requête v2 aux objets présentant 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 accorde des autorisations Amazon S3 à *<staging-bucket-name>* avec un accès en lecture/écriture uniquement sur les objets Amazon S3 ayant le préfixe `aws:userid`.

```
{
  "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 illustre une politique de compartiment qui sépare les données entre les utilisateurs de *<staging-bucket-name>*.

```

{
  "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  data (Charger les données). Load
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 (Target table), notamment le cluster ou le groupe de travail (Cluster or workgroup), la base de données (Database), le schéma (Schema) et le nom de la Table où sont stockées 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  data (Charger les données). Load
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 le 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 et exécution de requêtes

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 Export result set (Exporter l'ensemble de résultats) et 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.
- Si aucune ligne n'est sélectionnée, choisissez Export current page (Exporter la page actuelle) et soit JSON soit CSV pour télécharger les lignes de la page actuelle dans un fichier.

- Si des lignes sont sélectionnées, choisissez Export selected rows (Exporter les lignes sélectionnées) et soit JSON soit CSV pour télécharger les lignes sélectionnées dans un fichier.
- Si des lignes sont sélectionnées, choisissez Copy rows (Copier les lignes) pour copier les lignes sélectionnées dans le presse-papiers.
- Si des lignes sont sélectionnées, choisissez Copy rows with headers (Copier les lignes avec les en-têtes) pour copier les lignes sélectionnées avec les en-têtes de colonne dans le presse-papiers.

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 WorkGroup (Groupe de travail), et Database (Base de données) dans chaque onglet de l'éditeur avec la liste de contrôles déroulante située à côté de l'en-tête `Isolated session` (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 l'éditeur de requête v2 Amazon Redshift](#).

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 d'exemples 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 `${numerooforders}`. 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
...		

Création et exécution de blocs-notes

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 Run all (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 et exécution de requêtes](#). 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.

Lorsque vous exécutez un bloc-notes, avec Tout exécuter ou Exécuter, un panneau Statut d'exécution devient disponible. Choisissez l'icône



pour ouvrir le panneau. Ce panneau contient un résumé du statut des dernières opérations Tout exécuter ou Exécuter des cellules SQL de votre bloc-notes. Si vous exécutez plusieurs cellules SQL, vous pouvez voir en un coup d'œil le statut, le temps écoulé et certains détails relatifs à l'exécution. Vous pouvez filtrer les cellules affichées en fonction du statut : All, Succeeded, Error, In progress ou Canceled. Vous pouvez également utiliser ce panneau pour accéder à une cellule SQL dans l'éditeur.

Pour créer un bloc-notes

1. Dans le menu du navigateur, choisissez



Editor (Éditeur).

2. Choisissez



puis Notebook (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



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



puis SQL pour insérer une cellule SQL.

Vous pouvez renommer des blocs-notes à l'aide de l'icône



(crayon).

Dans le menu



(plus), 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 plus d'informations, consultez [Partage d'une requête](#).



Export (Exporter) : pour exporter le bloc-notes vers un fichier local portant l'extension `.ipynb`.



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.

Pour ouvrir un bloc-notes enregistré

1. Dans le menu du navigateur, choisissez



Notebooks (Blocs-notes). Vos blocs-notes et dossiers de blocs-notes enregistrés s'affichent.

2. Choisissez le bloc-notes que vous souhaitez ouvrir et double-cliquez dessus.

Vous pouvez afficher My notebooks (Mes blocs-notes), les blocs-notes Shared by me (Partagé par moi) et les blocs-notes Shared to my team (Partagé avec mon équipe) dans l'onglet Notebooks (Blocs-notes).

Pour importer un bloc-notes depuis un fichier local vers My notebooks (Mes blocs-notes), choisissez



Import (Importer), puis accédez au fichier `.ipynb` qui contient 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.

Dans le menu contextuel (clic droit) d'un bloc-notes, vous pouvez effectuer les opérations suivantes :

- Open notebook (Ouvrir le bloc-notes) : pour ouvrir le bloc-notes dans l'éditeur.
- Save version (Enregistrer la version) : pour enregistrer une version du bloc-notes.
- Version history (Historique des versions) : pour afficher les versions d'un bloc-notes. Dans la fenêtre Version history (Historique des versions), vous pouvez supprimer et annuler des versions. Vous pouvez également créer un bloc-notes à partir de la version actuellement sélectionnée.
- Edit tags (Modifier les balises) : pour créer et modifier des balises sur un bloc-notes.
- Share with my team (Partager avec mon équipe) : pour partager un bloc-notes avec votre équipe.

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 un bloc-notes vers un fichier local.
- Rename (Renommer) : pour renommer un bloc-notes.
- Duplicate (Dupliquer) : pour créer une copie d'un bloc-notes.
- Delete (Supprimer) : pour supprimer un bloc-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 requête v2 pour interroger les données cataloguées dans votre AWS Glue Data Catalog. Par défaut, il AWS Glue Data Catalog est répertorié sous la forme d'une base de données de l'éditeur de requêtes v2 nommée `awsdatacatalog`. L'interrogation de n' AWS Glue Data Catalog est pas disponible dans tous les Amazon Régions AWS 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 RA3 et 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.myglue;
```

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, procédez comme suit

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 awsdatalog to "IAM:myIAMUser"
```

Où *IAM:myIAMUser* est un utilisateur IAM auquel vous souhaitez accorder des privilèges d'utilisation du AWS Glue Data Catalog. Vous pouvez également accorder des privilèges d'utilisation à *IAMR:myIAMRole* pour 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 `awsdatalog` 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 `awsdatalog` 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 `awsdatalog`. 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 et exécution de requêtes](#) et [Création et exécution de blocs-notes](#). La base de données nommée `awsdatalog` est réservée pour référencer la base de données du catalogue de données externe dans votre compte. Les requêtes exécutées sur la base de données `awsdatalog` 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 awsdatalog.<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 d'un lac de données

Vous pouvez interroger des données dans un lac de données Amazon S3. 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](#).

Prérequis

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 :

- Indexez 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 du catalogue de données compatible avec AWS Glue pour AWS Lake Formation. Pour plus de détails sur cette procédure, consultez [Pour créer](#)

[un rôle IAM pour Amazon Redshift à l'aide d'un AWS Glue Data Catalog activé pour AWS Lake Formation](#). Pour plus d'informations sur l'utilisation de Redshift Spectrum et Lake Formation, consultez [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 Autorisations, page Autorisations Data lake, que le rôle IAM, la base de données AWS Glue et les tables ont les 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 `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



puis Schéma.

Créer,

2. Saisissez un nom de schéma.
3. Pour le Type de schéma, choisissez Externe.
4. Dans les détails du Catalogue de données, la Région est par défaut la Région AWS où se trouve votre base de données Redshift.
5. Choisissez la base de données AWS Glue vers laquelle le schéma externe sera mappé et qui contient des références aux tables AWS Glue.

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 suivant de SQL a été généré par l'éditeur de requête v2 pour interroger toutes les lignes de la table AWS Glue nommée `flightscsv`. 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
2016	4	10	19	3	10/19/16	00	20304
		N753SK	3086				
2016	4	10	19	3	10/19/16	00	20304
		N753SK	3086				
2016	4	10	19	3	10/19/16	00	20304
		N778SK	3087				
2016	4	10	19	3	10/19/16	00	20304
		N778SK	3087				
...							

Utilisation des 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 du 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;
```

Planification d'une 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 Requetes planifiées.

La vue Requetes

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

Configuration des autorisations pour planifier une requête

Pour planifier des requêtes, l'utilisateur AWS Identity and Access Management (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 souhaitez peut-être limiter les autorisations autorisées.

Pour modifier l'utilisateur IAM connecté à l'éditeur de requête v2, utilisez 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.

```
{
  "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 modifier le rôle IAM que vous spécifiez pour autoriser la requête planifiée à s'exécuter, utilisez 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 Serverless pour lequel vous planifiez des requêtes doit être marqué 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 :

```
{
  "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 de connexion à la 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`.

```
{
  "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.

L'exemple de politique d'approbation suivant s'applique à un rôle IAM qui autorise l'utilisateur IAM *myIAMusername* à consulter l'historique des requêtes planifiées. Au lieu d'accorder à un utilisateur IAM l'autorisation `sts:AssumeRole`, vous pouvez choisir d'accorder à un rôle IAM cette autorisation.

```

{
  "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 Stratégie d'accès qui est créé dans la rubrique Amazon SNS. Dans l'exemple, les rubriques Région AWS *us-west-2*, Compte AWS *123456789012* et Amazon SNS sont utilisées. *select-version-pdx-testunload*

```
{
  "Version": "2008-10-17",
  "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 la requête planifiée QS2-May25a qui s'est exécutée sur Région AWS eu-north-1 au Compte AWS 123456789012 à l'aide de la 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 [Trouver des informations sur les requêtes planifiées avec AWS CloudShell](#).

Trouver des informations sur les requêtes planifiées 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 assumer ce rôle, recherchez le rôle IAM associé à la requête planifiée dans l'éditeur de requêtes v2 et utilisez-le dans la AWS CLI commande dans AWS CloudShell. Par exemple, pour le rôle, `scheduler` entrez une AWS STS commande pour assumer 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": "AROA35B2NH6WBTP70NL4E: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"
}
```

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.](#)

Visualisation des résultats de requêtes

Une fois que vous avez exécuté une requête et que les résultats sont affichés, vous pouvez activer `Chart` (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.

Transformations

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.

Choisissez Traces (Suivis) pour afficher les résultats sous forme de diagramme. Pour Type, choisissez le style de diagramme, comme Bar (À barres), Line (Linéaire), etc. Pour Orientation, vous pouvez choisir Vertical ou Horizontal. Pour X, choisissez la colonne du tableau que vous souhaitez utiliser pour l'axe horizontal. Pour Y, choisissez la colonne du tableau que vous souhaitez utiliser pour l'axe vertical.

Pour mettre à jour l'affichage du diagramme, choisissez Refresh (Actualiser). Choisissez Full screen (Plein écran) pour développer l'affichage du diagramme.

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.

Pour enregistrer un diagramme

1. Choisissez Save Chart (Enregistrer le diagramme).
2. Saisissez un nom pour votre diagramme.
3. Choisissez Enregistrer.

Pour exporter un diagramme

1. Cliquez sur Exporter.
2. Choisissez PNG ou JPEG.
3. Définissez la largeur et la hauteur de votre diagramme.
4. Cliquez sur Exporter.
5. Choisissez d'ouvrir le fichier dans votre application graphique par défaut ou d'enregistrer le fichier avec le nom par défaut.

Pour rechercher et ouvrir un diagramme enregistré

1. Choisissez l'onglet Charts (Diagrammes).
2. Ouvrez le diagramme de votre choix.

Pour organiser vos diagrammes en dossiers

1. Dans le panneau de navigation, choisissez Charts (Diagrammes).
2. Choisissez New folder (Nouveau dossier) et nommez le dossier.
3. Choisissez Create (Créer) pour créer un dossier dans l'onglet Charts (Diagrammes).

Vous pouvez déplacer des graphiques dans et hors du dossier à l'aide de drag-and-drop.

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 0, 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.

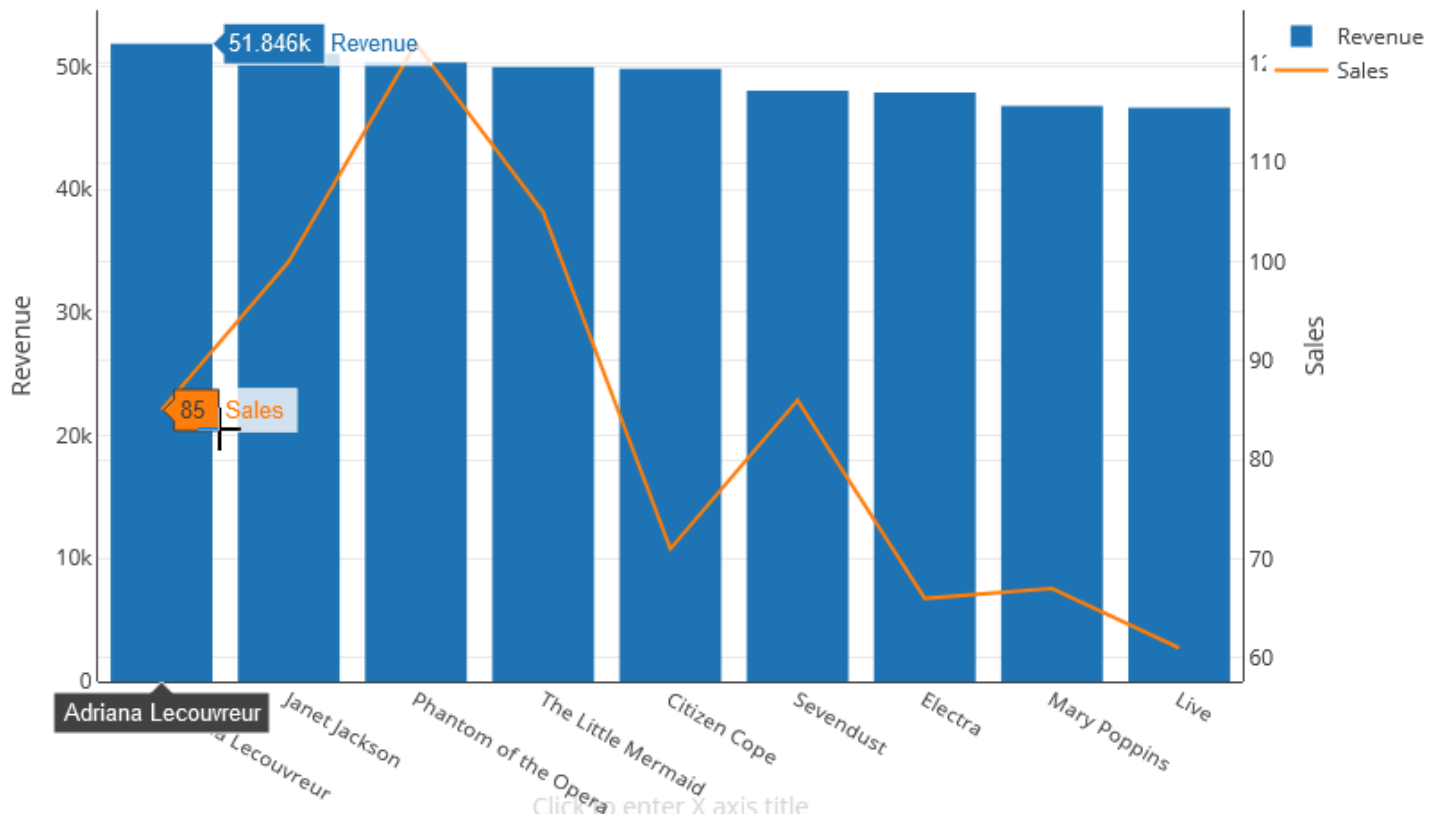
12. Pour Type, choisissez Ligne.
13. Pour X, choisissez eventname.
14. Pour Y, choisissez total_qty_sold.
15. Sous Axes à utiliser, pour Axe des Y choisissez

+

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 : Ventes.
20. Sous Ligne d'axe, choisissez Afficher, puis pour Position, choisissez Droite.

Revenue and Sales



Démo : créez des visualisations à l'aide de l'éditeur de requête v2 Amazon Redshift

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](#).

Enregistrement, recherche et suppression de 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.

Pour supprimer une requête enregistrée

1. Ouvrez le menu contextuel (clic droit) correspondant à une requête enregistrée.
2. Choisissez Delete (Supprimer) et confirmez l'action.

Pour organiser vos requêtes enregistrées dans des dossiers

1. Dans le panneau de navigation, choisissez Queries (Requêtes).
2. Choisissez New folder (Nouveau dossier) et nommez le dossier.
3. Choisissez Create (Créer) pour créer le dossier dans l'onglet Queries (Requêtes).

Vous pouvez désormais déplacer des requêtes dans et hors du dossier à l'aide de drag-and-drop.

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).

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 requête

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 AWS Identity and Access Management (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, comme décrit dans [Connexion à l'éditeur de requête](#).

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.

Activation de l'accès à l'éditeur de requête

Pour accéder à l'éditeur de requête, vous avez besoin d'une autorisation. Pour activer l'accès, nous vous recommandons d'associer les politiques `AmazonRedshiftQueryEditor` et les politiques `AmazonRedshiftReadOnlyAccess` AWS gérées pour les autorisations IAM au rôle IAM que vous utilisez pour accéder à votre cluster. Vous pouvez ensuite attribuer le rôle à un utilisateur. Vous pouvez attacher des politiques IAM à l'aide de la console IAM à l'adresse <https://console.aws.amazon.com/iam/>. Pour plus d'informations, consultez [Utilisation des politiques basées sur l'identité \(politiques IAM\) pour Amazon Redshift](#).

Si vous avez déjà créé un utilisateur pour accéder à Amazon Redshift, vous pouvez associer `AmazonRedshiftQueryEditor` les politiques `AmazonRedshiftReadOnlyAccess` AWS gérées à cet utilisateur au moyen d'un rôle attribué. Si vous n'avez pas encore créé d'utilisateur, créez-en un et attachez la politique au rôle IAM et assignez le rôle à l'utilisateur.

La politique AWS gérée `AmazonRedshiftQueryEditor` autorise l'action `quiredshift:GetClusterCredentials`, par défaut, donne accès à la base de données aux superutilisateurs. Pour limiter l'accès, vous pouvez effectuer l'une des actions suivantes :

- Créez une politique personnalisée qui autorise l'appelant `redshift:GetClusterCredentials` et limite la ressource à une valeur donnée pour `DbUser`.
- Ajoutez une politique qui refuse l'autorisation `redshift:GetClusterCredentials`. Tout utilisateur avec un rôle associé à cette autorisation doit se connecter à l'éditeur de requêtes avec des informations d'identification temporaires. Cette politique de refus illustre cet exemple.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "*"
  }
}
```

Pour plus d'informations sur la création d'un rôle avec les autorisations requises, consultez [Création d'un rôle IAM avec des autorisations d'appel GetClusterCredentials](#).

Tout utilisateur autorisé à accéder à l'éditeur de requêtes Amazon Redshift par le biais de la politique AWS gérée `AmazonRedshiftQueryEditor` peut répertorier tous les secrets. Toutefois, cette politique autorise la création et la récupération de secrets uniquement marqués avec la clé `RedshiftQueryOwner` et la valeur `${aws:userid}`. Si vous créez la clé à partir de l'éditeur de requête Amazon Redshift, la clé est automatiquement balisée. Pour utiliser un secret qui n'a pas été créé avec l'éditeur de requête Amazon Redshift, vérifiez que le secret est labélisé avec la clé `RedshiftQueryOwner` et une valeur de votre identifiant utilisateur IAM unique, par exemple `AIDACKCEVSQ6C2EXAMPLE`.

Les autorisations requises pour utiliser l'éditeur de requêtes Amazon Redshift sont `AmazonRedshiftQueryEditor` et `AmazonRedshiftReadOnlyAccess`.

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. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du 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](#) du 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.

Connexion à l'éditeur de requête

Lorsque vous vous connectez à un cluster avec l'éditeur de requêtes, vous utilisez l'une des méthodes d'authentification suivantes. Chaque méthode nécessite une combinaison différente d'entrées à partir de la console Amazon Redshift.

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.

Informations d'identification temporaires

Avec cette méthode, fournissez les valeurs de votre base de données et de votre utilisateur de base de données.

Stockage des identifiants de base de données dans AWS Secrets Manager

Lorsque vous appelez l'éditeur de requêtes, vous pouvez utiliser un secret dans AWS Secrets Manager pour transmettre les informations d'identification du cluster. Pour ce faire, vous devez spécifier le nom du secret ou son Amazon Resource Name (ARN).

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 .

Pour sauvegarder vos informations d'identification dans un secret pour un cluster Amazon Redshift

1. AWS Secrets Manager À utiliser pour créer un secret contenant les informations d'identification du cluster. Lorsque vous choisissez Store a new secret (Sauvegarder un nouveau secret), sélectionnez Credentials for Redshift cluster (Informations d'identification pour le cluster Redshift). Stockez une valeur pour User name (Nom d'utilisateur) (l'utilisateur de la base de données), Password (Mot de passe) et DB cluster (Cluster de la base de données) (identifiant du cluster) dans votre secret.

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.

Si vous avez choisi d'utiliser les informations d'identification d'administrateur de votre cluster AWS Secrets Manager, vous pouvez vous connecter à la base de données à l'aide des informations d'identification d'administrateur stockées dans le Gestionnaire de Secrets.

Utilisation de l'éditeur de requête

Dans l'exemple suivant, vous utilisez l'éditeur de requête pour effectuer les tâches suivantes :

- Exécutez des commandes SQL.
- Affichez les détails d'exécution de requête.
- Enregistrez une requête.
- Téléchargez un jeu de résultats de requête.

Pour terminer l'exemple suivant, vous avez besoin d'un cluster Amazon Redshift existant. Si vous n'avez pas de cluster, créez-en un en suivant la procédure décrite dans [Création d'un cluster](#).

Pour utiliser l'éditeur de requête sur la console Amazon Redshift

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dans le menu de navigation, choisissez Éditeur de requête, puis connectez-vous à une base de données dans votre cluster.
3. Pour Schéma, choisissez public pour créer une nouvelle table basée sur ce schéma.

- Entrez ce qui suit dans la fenêtre de l'éditeur de requête et choisissez Exécuter pour créer une nouvelle table.

```
create table shoes(  
    shoetype varchar (10),  
    color varchar(10));
```

- Choisissez Effacer.
- Entrez l'instruction suivante dans la fenêtre de l'éditeur de requête et choisissez Exécuter la requête pour ajouter des lignes dans la table.

```
insert into shoes values  
( 'loafers', 'brown'),  
( 'sandals', 'black');
```

- Choisissez Effacer.
- Entrez la commande suivante dans la fenêtre de l'éditeur de requête et choisissez Exécuter la requête pour interroger la nouvelle table.

```
select * from shoes;
```

La zone Résultats de la requête affiche les résultats.

Type de chaussure	Couleur
sandals	black
loafers	brown

- Choisissez Exécution pour afficher les détails de l'exécution.
- Choisissez Données, puis Exporter pour télécharger les résultats de la requête en tant que fichier.

Planification d'une requête

Important

L'éditeur de requêtes Amazon Redshift v2 prend désormais en charge la planification d'une requête. Nous vous recommandons d'utiliser l'éditeur de requêtes v2. Pour plus d'informations, consultez [Planification d'une requête avec l'éditeur de requête v2](#).

Pour créer une planification d'exécution d'une instruction SQL, vous pouvez utiliser l'éditeur de requêtes sur la console Amazon Redshift. Vous pouvez créer une planification pour exécuter votre instruction SQL aux intervalles de temps qui correspondent aux besoins de votre activité. Au moment de l'exécution de la requête planifiée, Amazon EventBridge lance la requête.

Pour créer une planification afin d'exécuter une instruction SQL

1. Ouvrez la console et l'éditeur de requêtes comme décrit dans [Utilisation de l'éditeur de requête](#). Vous ne pouvez utiliser cet éditeur de requêtes qu'avec des clusters provisionnés.
2. Choisissez Schedule (Planification) afin de créer une planification pour exécuter une instruction SQL.

Lorsque vous définissez la planification, vous fournissez les informations suivantes :

- Un rôle IAM qui est utilisé pour assumer les autorisations requises pour l'exécution de la requête. Pour plus d'informations, consultez [Configuration des autorisations pour planifier une requête](#).
- 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. Pour plus d'informations, consultez [Authentification d'une requête planifiée](#).
- Le nom de la requête planifiée et une instruction SQL unique à exécuter.
- Les options de fréquence et de répétition de la planification ou une valeur au format cron.
- Si nécessaire, vous pouvez activer les notifications Amazon SNS pour surveiller la requête planifiée. Si votre requête est en cours d'exécution mais que vous ne voyez aucun message publié dans votre rubrique SNS, consultez [Ma règle est déclenchée mais je ne vois aucun message publié dans ma rubrique Amazon SNS](#) dans le guide de l'utilisateur EventBridge Amazon.

Vous pouvez également gérer et mettre à jour les requêtes planifiées à l'aide de la console Amazon Redshift. Selon votre version de la console, les requêtes planifiées peuvent être répertoriées aux endroits suivants :

- Dans l'onglet Planification (Schedules) de la page de détails de votre cluster.
- Dans l'onglet Scheduled queries (Requêtes planifiées) de l'éditeur de requête.

Si vous choisissez Schedule name (Nom de la planification) dans l'un de ces emplacements, vous pouvez afficher et modifier la définition de votre requête planifiée.

Configuration des autorisations pour planifier une requête sur la console Amazon Redshift

Pour planifier des requêtes, l'utilisateur AWS Identity and Access Management (IAM) qui définit le calendrier et le rôle IAM associé au calendrier doivent être configurés comme suit.

Pour l'utilisateur IAM connecté à la console Amazon Redshift, procédez comme suit :

- Associez la politique AmazonEventBridgeFullAccess AWS gérée à un rôle IAM.
- Attachez une politique avec l'autorisation `sts:AssumeRole` du rôle IAM que vous spécifiez lorsque vous définissez l'instruction SQL planifiée.

L'exemple suivant illustre une politique qui assume un rôle IAM spécifié.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AssumeIAMRole",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::account-id:role/sql-statement-iam-role"
    }
  ]
}
```

Pour le rôle IAM que vous spécifiez en vue de permettre au planificateur d'exécuter une requête, procédez comme suit :

- Assurez-vous que ce rôle IAM spécifie le principal EventBridge de service (events.amazonaws.com). Voici un exemple de relation d'approbation.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Pour plus d'informations sur la création d'un rôle IAM pour les EventBridge événements, consultez [Autorisations requises pour utiliser le EventBridge planificateur Amazon](#).

- Associez la politique AmazonRedshiftDataFullAccess AWS gérée au rôle IAM.
- Pour permettre aux utilisateurs d'afficher l'historique des planifications, modifiez le rôle IAM pour ajouter l'autorisation sts:AssumeRole.

L'exemple de politique d'approbation suivant est défini pour un rôle IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Authentification d'une requête planifiée

Lorsque vous planifiez une requête, vous utilisez l'une des méthodes d'authentification suivantes lors de l'exécution de la requête SQL. Chaque méthode nécessite une combinaison différente d'entrées à partir de la console Amazon Redshift.

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. Le secret doit être étiqueté avec la clé `RedshiftDataFullAccess`.

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, fournissez les valeurs de votre base de données et de votre utilisateur de base de données.

La politique `AmazonRedshiftDataFullAccess` accorde à l'utilisateur de la base de données nommé `redshift_data_api_user` les autorisations 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 pour accorder l'autorisation `redshift:GetClusterCredentials`. L'exemple de stratégie suivant autorise les utilisateurs de base de données `awsuser` et `myuser`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UseTemporaryCredentialsForAllDbUsers",
      "Effect": "Allow",
      "Action": "redshift:GetClusterCredentials",
      "Resource": [
        "arn:aws:redshift:*:*:dbuser:*/awsuser",
        "arn:aws:redshift:*:*:dbuser:*/myuser"
      ]
    }
  ]
}
```

```
}
```

Créez une EventBridge règle Amazon qui s'exécute à la fin d'une requête

Vous pouvez créer une règle d'événement pour envoyer une notification lorsqu'une requête se termine. Pour la procédure à suivre à l'aide de la EventBridge console Amazon, consultez [la section Création de EventBridge règles Amazon qui réagissent aux événements](#) dans le guide de EventBridge l'utilisateur Amazon. Pour plus d'informations sur les modèles d'événements, consultez la section [Modèles EventBridge d'événements Amazon](#) dans le guide de EventBridge l'utilisateur Amazon.

Par exemple, l'exemple d'événement suivant est envoyé lorsqu'une requête est FINISHED.

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "Redshift Data Statement Status Change",
  "source": "aws.redshift-data",
  "account": "123456789012",
  "time": "2020-12-22T17:00:00Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:redshift:us-east-2:123456789:cluster:t1"
  ],
  "detail": {
    "statementId": "01bdaca2-8967-4e34-ae3f-41d9728d5644",
    "clusterId": "test-dataapi",
    "statementName": "awesome query",
    "state": "FINISHED",
    "pages": 5,
    "expireAt": "2020-12-22T18:43:48Z",
    "principal": "arn:aws:sts::123456789012:assumed-role/any",
    "queryId": 123456
  }
}
```

Vous pouvez créer une règle de modèle d'événement pour filtrer l'événement.

```
{
  "source": [
    "aws.redshift-data"
  ]
}
```

```
    ],
    "detail-type": [
        "Redshift Data Statement Status Change"
    ],
    "detail": {
        "state": [
            "FINISHED"
        ]
    }
}
```

Connexion à un entrepôt de données Amazon Redshift à l'aide des outils client SQL

Vous pouvez vous connecter aux entrepôts de données Amazon Redshift à partir des 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 sur une instance Amazon EC2. Vous pouvez utiliser la plupart des outils clients SQL qui prennent en charge les pilotes ODBC, Python ou JDBC.

Utilisez la liste des sections à la fin de cette rubrique pour vous aider à suivre le processus de configuration de votre ordinateur client ou de votre instance Amazon EC2 pour utiliser une connexion JDBC, Python ou ODBC. Les rubriques traitent 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 SQL Workbench/J, un outil tiers, et [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 votre entrepôt de données par programmation. Enfin, si vous rencontrez des problèmes lorsque vous tentez de vous connecter à votre entrepôt de données, vous pouvez consulter les informations de dépannage pour identifier des solutions.

Recommandations pour la connexion aux outils clients

Si vous vous connectez à votre cluster Redshift à l'aide d'une adresse IP, cela peut entraîner des temps d'arrêt 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 cluster (virtual-private-cloud VPC). 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](#)
- [Configuration des options de sécurité des connexions](#)
- [Connexion à partir d'outils et de codes clients](#)
- [Connexion avec SQL Workbench/J](#)
- [Connectez-vous à votre entrepôt de données par programmation](#)
- [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 AWS 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 le pilote JDBC version 2.1 pour Amazon Redshift](#), [Configuration du connecteur Amazon Redshift Python](#) et [Configuration d'une connexion ODBC](#).

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 AWS Management Console 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 le pilote JDBC version 2.1 pour Amazon Redshift

Vous pouvez utiliser une connexion au pilote JDBC version 2.1 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 utiliser une connexion JDBC, consultez les sections suivantes.

Rubriques

- [Télécharger le pilote Amazon Redshift JDBC, version 2.1](#)
- [Installation du pilote Amazon Redshift JDBC, version 2.1](#)
- [Obtention de l'URL JDBC](#)
- [Création de l'URL de connexion](#)
- [Configuration des keepalives TCP pour votre connexion JDBC](#)
- [Configuration de votre connexion JDBC avec Apache Maven](#)
- [Configuration de l'authentification et du protocole SSL](#)
- [Configuration de la journalisation](#)
- [Conversion de types de données](#)
- [Utilisation du support d'instructions préparées](#)

- [Différences entre les versions 2.1 et 1.x du pilote JDBC](#)
- [Création de fichiers d'initialisation \(.ini\) pour le pilote JDBC version 2.1](#)
- [Options de configuration du pilote JDBC version 2.1](#)
- [Versions précédentes du pilote JDBC version 2.1](#)

Télécharger le pilote Amazon Redshift JDBC, version 2.1

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 2.1, assurez-vous que le Java Runtime Environment (JRE) 8.0 est installé.

Si vous utilisez le pilote JDBC d'Amazon Redshift pour l'authentification de la base de données, assurez-vous que vous avez AWS SDK for Java 1.11.118 ou une version ultérieure dans votre chemin de classe Java. Si ce n'est pas le cas AWS SDK for Java , téléchargez le fichier ZIP contenant le pilote compatible avec JDBC 4.2 et les bibliothèques dépendantes du pilote pour le SDK : AWS

- [Version 2.1 du pilote compatible avec JDBC 4.2 et bibliothèques dépendantes du pilote du AWS SDK Dans la région de](#) pilote du SDK AWS

Ce fichier ZIP contient la version 2.1 du pilote compatible avec JDBC 4.2 et les fichiers de bibliothèque dépendants du pilote SDK for AWS Java 1.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 1.x. Toutefois, il inclut les bibliothèques dépendantes du pilote AWS SDK for Java 1.x requises pour l'authentification (IAM) des bases AWS Identity and Access Management 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 1.x, [AWS consultez la section SDK pour Java](#) AWS SDK for Java 1.x dans le manuel du développeur.

- [Version 2.1 du pilote compatible JDBC 4.2 \(sans le AWS SDK\) Dans la région de Chine \(Pékin\)](#)

Examinez la licence logicielle du pilote JDBC version 2.1 et modifiez le fichier journal :

- [Licence du pilote JDBC version 2.1](#)
- [Journal des modifications du pilote JDBC version 2.1](#)

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 2.1

Pour installer la version 2.1 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 2.1 du pilote compatible avec Amazon Redshift JDBC 4.2 (sans le AWS SDK), 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;
    //
    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	Valeur
<code>jdbc</code>	Protocole de la connexion.
<code>redshift</code>	Le sous-protocole qui spécifie l'utilisation du pilote Amazon Redshift pour se connecter à la base de données.
<code><i>endpoint</i></code>	Le point de terminaison du cluster Amazon Redshift.
<code><i>port</i></code>	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.
<code><i>database</i></code>	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`

Assurez-vous de saisir les valeurs d'URL, par exemple SessionToken les valeurs, au format URL codé.

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 2.1. 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];
```

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=false;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev?ssl=false;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=false;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev;ssl=false&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 2.1](#).

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 des keepalives TCP pour votre connexion JDBC

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.

Configuration de votre connexion JDBC avec Apache Maven

Apache Maven est un outil de gestion et de compréhension de projets logiciels. Il AWS SDK for 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 for 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

Configuration du pilote JDBC en tant que dépendance Maven

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 un référentiel Amazon Maven, utilisez ce qui suit.

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>http://redshift-maven-repository.s3-website-us-east-1.amazonaws.com/
release</url>
  </repository>
</repositories>
```

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 [Télécharger le pilote Amazon Redshift JDBC, version 2.1.](#)

Ajoutez une dépendance pour le pilote comme indiqué ci-dessous.

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>
```

Mise à niveau du pilote vers la dernière version

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 2.1 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 2.1 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](#).

SSL indique TLS/SSL, à la fois Transport Layer Security et Secure Sockets Layer. Le pilote prend en charge les versions standard de TLS/SSL.

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 sur 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.

L'authentification unidirectionnelle nécessite un certificat SSL signé et approuvé 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 `autrecacerts`).

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 RootCert propriété SSL 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 RootCert propriété SSL 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 :
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.

```
-Djavax.net.ssl.trustStore=[TrustStoreName]  
-Djavax.net.ssl.trustStorePassword=[TrustStorePassword]  
-Djavax.net.ssl.trustStoreType=[TrustStoreType]
```

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
<code>jdbc:redshift:iam:// [host]:[port]/[db]</code>	Chaîne de connexion régulière. Le pilote déduit les valeurs de ClusterID et Region de l'hôte.
<code>jdbc:redshift:iam:// [cluster-id]: [region]/[db]</code>	Le pilote récupère les informations sur l'hôte, en fonction des valeurs de ClusterID et Region.
<code>jdbc:redshift:iam:// [host]/[db]</code>	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 for 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 plug-ins du fournisseur d'informations d'identification des services suivants :

- 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 votre classe de plugin 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.
- `User` : nom d'utilisateur du serveur `idp_host`.
- `Password` : 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` : ID client associé au nom d'utilisateur dans le portail Azure AD. Utilisé uniquement pour Azure AD.
- `Client_Secret` : 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` : ID de l'appli Okta pour votre application Amazon Redshift. Utilisé uniquement pour Okta.
- `App_Name` : nom facultatif de l'appli Okta pour votre application Amazon Redshift. Utilisé uniquement pour Okta.

- `Partner_SPID` : valeur SPID du partenaire facultative (ID du fournisseur de services). Utilisé uniquement pour PingFederate.

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` : URL de la ressource sur le site Web du fournisseur d'identité lors de l'utilisation des services SAML (Security Assertion Markup Language) ou Azure AD via un plugin 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 lors de l'utilisation des services SAML ou Azure AD via un plugin de navigateur.
- `IdP_Response_Timeout` : temps, en secondes, pendant lequel 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.

Pour plus d'informations sur les propriétés supplémentaires de la chaîne de connexion, consultez [Options de configuration du pilote JDBC version 2.1](#).

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`, consultez [Utilisation des fichiers journaux](#).
- Pour envoyer les informations enregistrées au LogStream ou LogWriter spécifiées dans le DriverManager, voir [En 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 les 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 2.1, 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.

Pour désactiver la journalisation qui utilise le LogStream ou LogWriter :

1. Supprimez la LogLevel propriété de l'URL de connexion.
2. Pour vous assurer que les nouveaux paramètres prennent effet, redémarrez votre application JDBC et reconnectez-vous au serveur.

Conversion de types de données

Le pilote Amazon Redshift JDBC version 2.1 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 2.1 et 1.x du pilote JDBC

Cette section décrit les différences dans les informations renvoyées par les versions 2.1 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 `getDatabaseProductName ()` et `getDatabaseProduct Version ()` pour chaque version du pilote JDBC. Le pilote JDBC version 2.1 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	obtenir DatabaseProduct le résultat Name ()	obtenir le résultat de DatabaseProduct la version ()
2.1	Redshift	8,0.2
1.x	PostgreSQL	08,00.0002

Le tableau suivant répertorie les DatabaseMetadata informations renvoyées par la `getTypeInfo` fonction pour chaque version du pilote JDBC.

Version du pilote JDBC	getTypeInfo résultat
2.1	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 2.1

En utilisant des fichiers d'initialisation (.ini) pour le pilote JDBC Amazon Redshift version 2.1, 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 2.1 qui contient des options de configuration pour les clients SQL. Le nom par défaut du fichier est `rsjdbc.ini`. Le pilote JDBC version 2.1 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 2.1 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 2.1

Vous trouverez ci-dessous des descriptions des options que vous pouvez spécifier pour la version 2.1 du pilote JDBC Amazon Redshift. 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](#)
- [Autoriser DB UserOverride](#)
- [App_ID](#)
- [App_Name](#)
- [ApplicationName](#)
- [AuthProfile](#)
- [AutoCreate](#)
- [Client_ID](#)
- [Client_Secret](#)
- [ClusterID](#)
- [Compression](#)
- [connectTimeout](#)

- [connectionTimezone](#)
- [base de données MetadataCurrent DbOnly](#)
- [DbUser](#)
- [DbGroups](#)
- [DBNAME](#)
- [RowFetchTaille par défaut](#)
- [DisableIsValidQuery](#)
- [activer FetchRing Buffer](#)
- [activer le MultiSql Support](#)
- [taille de récupération RingBuffer](#)
- [ForceLowercase](#)
- [groupFederation](#)
- [HOST](#)
- [IAM DisableCache](#)
- [IAMDuration](#)
- [Identity_Namespace](#)
- [IdP_Host](#)
- [IdP_Port](#)
- [IdP_Tenant](#)
- [IdP_Response_Timeout](#)
- [IniFile](#)
- [IniSection](#)
- [isServerless](#)
- [Login_URL](#)
- [loginTimeout](#)
- [se connecter ToRp](#)
- [LogLevel](#)
- [LogPath](#)
- [OverrideSchemaPatternType](#)

- [Partner_SPID](#)
- [Mot de passe](#)
- [Plugin_Name](#)
- [PORT](#)
- [Preferred_Role](#)
- [Profil](#)
- [PWD](#)
- [queryGroup](#)
- [readOnly](#)
- [Région](#)
- [WriteBatchedEncarts rouges](#)
- [re WriteBatched InsertsSize](#)
- [roleArn](#)
- [rôle SessionName](#)
- [scope](#)
- [SecretAccessClé](#)
- [SessionToken](#)
- [sans serveur AcctId](#)
- [sans serveur WorkGroup](#)
- [socketFactory](#)
- [socketTimeout](#)
- [SSL](#)
- [SSL_Insecure](#)
- [SSLCert](#)
- [SSLFactory](#)
- [SSLKey](#)
- [SSLMode](#)
- [SSLPassword](#)
- [SSL RootCert](#)

- [StsEndpointURL](#)
- [tcp KeepAlive](#)
- [jeton](#)
- [type_jeton](#)
- [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.

Autoriser DB UserOverride

- 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'ID unique fourni par Okta 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 : désactivée
- 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 MetadataCurrent DbOnly

- 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.

RowFetchTaille par défaut

- 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 spécifie si le pilote soumet une nouvelle requête de base de données lors de l'utilisation de 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 lors de l'utilisation de `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 soumet une requête lors de l'utilisation de `Connection.isValid()` pour déterminer si la connexion à la base de données est active.

activer FetchRing Buffer

- 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 paramètre `fetchRingBuffer Size` indique la taille de la mémoire tampon en anneau.

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`. `enableFetchRingLa` la valeur du tampon ne change pas.

Ce paramètre est facultatif.

activer le MultiSql Support

- 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.

taille de récupération RingBuffer

- 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'API GetClusterCredentials V2.

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.

IAM DisableCache

- 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.

Identity_Namespace

- Valeur par défaut – Aucune
- Types de données – Chaîne

L'espace de noms d'identité à utiliser lors de l'authentification à l'aide du. IdpTokenAuthPlugin Cela aide Redshift à déterminer l'instance IAM Identity Center à utiliser.

S'il existe une seule instance IAM Identity Center ou si l'espace de noms d'identité par défaut est défini, ce paramètre est facultatif ; sinon, il est obligatoire.

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_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 2.1.](#)

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 2.1](#).

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.

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 LogLevel propriété DSI 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**— Service de fédération Active Directory.
- **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.
- **BrowserSamlCredentialsProvider**— Navigateur SAML pour les services SAML tels qu'Okta, Ping ou ADFS.
- **IdpTokenAuthPlugin**— Un plugin d'autorisation qui accepte un jeton IAM Identity Center ou des jetons d'identité basés sur le JSON OpenID Connect (OIDC) (JWT) provenant de n'importe quel fournisseur d'identité Web 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.

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.

`WriteBatchedEncarts rouges`

- 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 WriteBatched InsertsSize`

- 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'option `Plugin_Name`. Spécifiez l'ARN au format suivant :

`arn:partition:service:region:account-id:resource-id`

Ce paramètre est obligatoire si vous spécifiez BasicJwtCredentialsProvider l'option Plugin_Name.

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'option Plugin_Name.

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 BrowserAzure OAuth2 CredentialsProvider pour l'option Plugin_Name.

Ce paramètre est obligatoire pour le plug-in BrowserAzure OAuth2. CredentialsProvider

SecretAccessClé

- 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 via 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 comment le pilote valide les certificats lorsque TLS/SSL est activé.

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.

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.

SSL RootCert

- 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 IAM Identity Center ou un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web lié à IAM Identity Center. Votre application doit générer ce jeton en authentifiant l'utilisateur de votre application auprès d'IAM Identity Center ou d'un fournisseur d'identité lié à IAM Identity Center.

Ce paramètre fonctionne avec `IdpTokenAuthPlugin`.

type_jeton

- Valeur par défaut – Aucune
- Types de données – Chaîne

Type de jeton utilisé dans `IdpTokenAuthPlugin`.

Vous pouvez spécifier les valeurs suivantes :

JETON D'ACCÈS

Entrez cette valeur si vous utilisez un jeton d'accès fourni par IAM Identity Center.

EXT_JET

Entrez cette valeur si vous utilisez un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web intégré à 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'option Plugin_Name.

Ce paramètre est obligatoire si vous spécifiez BasicJwtCredentialsProvider l'option Plugin_Name.

Versions précédentes du pilote JDBC version 2.1

Ne téléchargez une version antérieure du pilote JDBC Amazon Redshift version 2.1 que si votre outil nécessite une version spécifique du pilote.

Il s'agit des anciens pilotes JDBC 4.2 compatibles avec la version 2.1 des pilotes JDBC :

- <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>

Configuration du 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 GitHub référentiel](#).

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 :

- AWS Identity and Access Management Authentication (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 [Federate access to your Amazon Redshift cluster with 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 [JumpCloudsite](#).
- 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 plug-ins 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 RedshiftPythonDriver
$ 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.

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.

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_identifiant

- 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`
- `BrowserAzure0Auth2CredentialsProvider`
- `BrowserSamlCredentialsProvider`
- `IdpTokenAuthPlugin`— Un plugin d'autorisation qui accepte un jeton Identity Center (iDC) ou des jetons d'identité basés sur OpenID Connect (OIDC) JSON (JWT) provenant de n'importe quel fournisseur d'identité Web lié à l'iDC.
- `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
- Types 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.

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.

identity_namespace

- Valeur par défaut : null
- Types de données – Chaîne

L'espace de noms d'identité à utiliser lors de l'authentification à l'aide de `IdpTokenAuthPlugin`. Cela aide Redshift à choisir l'instance Identity Center à utiliser.

S'il n'existe qu'une seule instance d'Identity Center ou si l'espace de noms d'identité par défaut est défini, ce paramètre est facultatif. Sinon, elle est obligatoire.

`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.

`listen_port`

- Valeur par défaut – 7890
- Type de données – Entier

Port d'écoute auquel l'IdP envoie l'assertion SAML.

Ce paramètre est facultatif.

login_url

- Valeur par défaut – Aucune
- Types 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 pouvant être ouvertes simultanément.

Ce paramètre est obligatoire.

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
- Types 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
- Types 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
- Types de données – Chaîne

Nom du fournisseur d'authentification native Redshift.

Ce paramètre est facultatif.

region

- Valeur par défaut – Aucune
- Types 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
- Types 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 `BrowserAzure OAuth2 CredentialsProvider` pour l'option `credentials_provider`.

Ce paramètre est obligatoire pour le plug-in `BrowserAzure OAuth2. CredentialsProvider`

`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
- Types de données – Chaîne

ID du compte Amazon Redshift Serverless.

Ce paramètre est facultatif.

serverless_work_group

- Valeur par défaut – Aucune
- Types 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 – True

- Types de données – Booléen

Valeur qui indique si le certificat de serveur d'hôtes IdP doit être vérifié.

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

Ce paramètre est obligatoire.

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 IAM Identity Center ou un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web lié à IAM Identity Center. Votre application doit générer ce jeton en authentifiant l'utilisateur de votre application auprès d'IAM Identity Center ou d'un fournisseur d'identité lié à IAM Identity Center.

Ce paramètre fonctionne avec `IdpTokenAuthPlugin`.

type_jeton

- Valeur par défaut – Aucune
- Types de données – Chaîne

Type de jeton utilisé dans `IdpTokenAuthPlugin`.

Vous pouvez spécifier les valeurs suivantes :

JETON D'ACCÈS

Entrez cette valeur si vous utilisez un jeton d'accès fourni par IAM Identity Center.

EXT_JET

Entrez cette valeur si vous utilisez un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web intégré à IAM Identity Center.

Ce paramètre fonctionne avec `IdpTokenAuthPlugin`.

utilisateur

- 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
```

Importation NumPy et connexion à Amazon Redshift

Pour importer le connecteur Amazon Redshift Python et Numerical Python (NumPy), exécutez les commandes suivantes.

```
import redshift_connector
import numpy
```

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 à 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_identifieur='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_identifieur='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 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.

L'authentification multifacteur a lieu dans le navigateur, où les informations d'identification 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_identfier='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_identfier='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 d'informations d'identification AWS](#)
- [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 d'informations d'identification AWS

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 données volumineuses. 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 3.3.0, 3.3.1, 3.3.2 et 3.4.0 de Spark avec cette intégration.

Cette intégration fournit les éléments suivants :

- Authentification AWS Identity and Access Management 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 AWS différentes. Pour utiliser des régions AWS distinctes, définissez le paramètre `tempdir_region` sur la région du compartiment S3 utilisé pour `tempdir`.
- Écritures entre régions entre S3 et Redshift en cas d'écriture de données Parquet à l'aide du paramètre `tempformat`.
- 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 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 ou AWS Glue, assurez-vous que votre rôle IAM dispose des autorisations nécessaires pour récupérer les 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 sans serveur)
- [Redshift:GetCredentials](#) (pour Amazon Redshift sans serveur ; les groupes de travail)
- [s3:ListBucket](#)
- [s3:GetBucket](#)
- [s3:GetObject](#)
- [s3:PutObject](#)
- [s3:GetBucketLifecycleConfiguration](#)

Pour plus d'informations sur GetClusterCredentials, consultez [Politiques de ressources pour GetClusterCredentials](#).

Vous devez également vous assurer qu'Amazon Redshift peut assumer le rôle IAM pendant les opérations COPY et UNLOAD.

```
{
  "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 gèrera 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 :

- L'AWS SDK pour Java tentera automatiquement de trouver des informations d'identification AWS en utilisant la chaîne de fournisseurs d'informations d'identification par défaut implémentée par la

classe `DefaultAWSCredentialsProviderChain`. Pour plus d'informations, consultez [Utilisation de la chaîne de fournisseur d'informations d'identification par défaut](#).

- Vous pouvez spécifier des clés AWS 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")
```

- Encodage des 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 services AWS](#), 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 connexions SQL pour Java de AWS Secrets Manager 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 obtenir la liste complète des fonctions de Spark, consultez [Built-in Functions](#) (Fonctions intégrées).

- Fonctions d'agrégation
 - avg
 - count
 - max
 - min
 - sum
 - stddev_samp
 - stddev_pop
 - var_samp
 - var_pop
- Opérateurs booléens
 - dans
 - 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
- dans
- 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
 - Limites
 - Unions, union all
 - ScalarSubquery
 - Sorts (par ordre croissant et décroissant)
 - UnscaledValue

Autres options de configuration

Modification de la 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))
}
```

Définition d'un 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))
}
```

Définition d'un encodage de compression sur 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](#).

Définition de la description d'une colonne

Pour définir une description, utilisez le champ `description`.

Authentification entre Redshift et Amazon S3

Par défaut, le résultat est téléchargé sur Amazon S3 au format Parquet. Pour télécharger le résultat sous forme de fichier texte séparé par une barre verticale, spécifiez l'option suivante.

```
.option("unload_s3_format", "TEXT")
```

Exécution lente des 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.

Paramètre	Obligatoire	Par défaut	Description
			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
<code>dbtable</code>	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 réenregistrement de données dans Redshift.
<code>query</code>	Oui, sauf si <code>dbtable</code> est spécifié	N/A	La requête à partir de laquelle lire dans Redshift.
<code>utilisateur</code>	Non	N/A	Le nom d'utilisateur Redshift. Doit être utilisé avec le paramètre de mot de passe. Valide uniquement si l'utilisa

Paramètre	Obligatoire	Par défaut	Description
			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 utilisateur. Valide uniquement si l'utilisateur et le mot de passe ne sont pas des paramètres dans l'URL. Utiliser les deux entraînera une erreur.

Paramètre	Obligatoire	Par défaut	Description
url	Non	N/A	<p>Une URL JDBC. Le format est le suivant : jdbc:subprotocol:// host:port/database? user=username&pa ssword=password.</p> <p>Le sous-protocole peut être postgresq l 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.</p> <p>L'hôte et le port doivent pointer vers le nœud principal Redshift. Vous devez donc configurer des groupes de sécurité et/ou un VPC pour autoriser l'accès depuis votre applicati on pilote.</p> <p>Database est le nom de la base de données Redshift.</p>

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	Clé d'accès AWS. Vous devez disposer d'autorisations d'écriture sur le compartiment S3.
temporary_aws_secret_access_key	Non	N/A	Clé d'accès secrète AWS qui correspond à la clé d'accès.

Paramètre	Obligatoire	Par défaut	Description
temporary_aws_session_token	Non	N/A	Jeton de session AWS correspondant à la clé d'accès fournie.
tempdir	Non	N/A	Emplacement accessible en écriture dans Amazon S3. Utilisé pour télécharger 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 automatiquement déterminé par le sous-protocole de l'URL JDBC.
diststyle	Non	Even	Styles de distribution 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 <code>description</code> 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	<p>Liste d'options supplémentaires à ajouter à la commande Redshift COPY lors du chargement de données (par exemple TRUNCATECOLUMNS ou MAXERROR n).</p> <p>Consultez Paramètres facultatifs pour obtenir la liste complète des paramètres disponibles.</p> <p>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.</p>

Paramètre	Obligatoire	Par défaut	Description
sse_kms_key	Non	N/A	L'ID de clé AWS KMS à utiliser pour le chiffrement côté serveur dans S3 lors de l'opération Redshift UNLOAD plutôt que pour le chiffrement AWS par défaut. 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 d'un accès approprié.
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 et CSV GZIP (CSV compressé).

Paramètre	Obligatoire	Par défaut	Description
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.
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 télécharger 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 télécharger les résultats de la requête. Les options valides sont Parquet et Text, qui indiquent de télécharger 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	<p>La région AWS où se trouve tempdir. La définition de cette option améliore les performances du connecteur pour les interactions avec tempdir et fournit automatiquement cette valeur dans le cadre des opérations COPY et UNLOAD au cours des opérations de lecture et d'écriture du connecteur.</p> <p>Ce paramètre est recommandé dans les situations suivantes :</p> <ol style="list-style-type: none">1) Lorsque le connecteur fonctionne en dehors d'AWS, car la découverte automatique des régions échouera et aura une incidence négative sur les performances du connecteur.2) Quand tempdir se trouve dans une

Paramètre	Obligatoire	Par défaut	Description
			<p>autre région que le cluster Redshift, car l'utilisation de ce paramètre évite d'avoir à fournir la région manuellement à l'aide des paramètres <code>extracopy_options</code> et <code>extraunl_options</code>. <code>tempdir</code> ne peut se trouver dans une autre région que le cluster Redshift lors de l'utilisation de PARQUET en tant que <code>tempformat</code> même si cela utilise ce paramètre.</p> <p>3) Lorsque le connecteur fonctionne dans une région différente de <code>tempdir</code>, car cela améliore les performances d'accès du connecteur à <code>tempdir</code>.</p>

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 <code>DbUser</code> 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	<p>Région AWS principale, telle que USA Est (Virginie du Nord), dans laquelle rechercher la valeur <code>secret.id</code> .</p> <p>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 <code>secret.id</code> .</p> <p>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 :</p> <p>1) Lorsque le connecteur fonctionne en dehors d'AWS, car la découverte automatique des régions échouera et empêchera</p>

Paramètre	Obligatoire	Par défaut	Description
			<p>l'authentification avec Redshift</p> <p>Lorsque le connecteur s'exécute dans une région différente de <code>secret.id</code>, car cela améliore les performances d'accès du secret du connecteur.</p>
<code>secret.vpcEndpointUrl</code>	Non	N/A	URL du point de terminaison DNS PrivateLink pour AWS Secrets Manager lors du remplacement de la chaîne de fournisseur d'informations d'identification par défaut .
<code>secret.vpcEndpointRegion</code>	Non	N/A	Région du point de terminaison DNS PrivateLink pour AWS Secrets Manager lors du remplacement de la chaîne de fournisseur d'informations d'identification par défaut .

Paramètre	Obligatoire	Par défaut	Description
jdbc.*	Non	N/A	<p>Paramètres supplémentaires à transmettre au pilote JDBC sous-jacent quand le caractère générique est le nom du paramètre JDBC, tels que jdbc.ssl.</p> <p>Notez que le préfixe jdbc sera supprimé avant d'être transmis au pilote JDBC.</p> <p>Pour voir toutes les options possibles pour le pilote JDBC Redshift, consultez Options de configuration du pilote JDBC version 2.1.</p>

Paramètre	Obligatoire	Par défaut	Description
étiquette	Non	" "	<p>Identifiant à inclure dans le groupe de requêtes défini lors de l'exécution de requêtes avec le connecteur. Doit comporter 100 caractères ou moins, et tous les caractères doivent être des unicodeIdentifierParts valides. Si votre identifiant comporte plus de 100 caractères, 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</p> <pre>{"spark-redshift-connector": {"svc": "", "ver": "5.1.0-amzn-1-spark_3.3", "op": "Read", "tbl": ""}}`)</pre>

Paramètre	Obligatoire	Par défaut	Description
			. Cette option remplace la valeur de la clé 1b1.

 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	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	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 télécharger l'intégralité de la structure de données imbriquée lors de l'accès à une simple partie des données.

Lorsque vous écrivez des `DataFrames` à partir du connecteur, toute colonne de type `MapType` (utilisant `StringType`), `StructType` ou `ArrayType` est écrite dans une colonne de type de données Redshift SUPER. 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]")
```

Limites

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 et Windows. Les pilotes ODBC 32 bits sont interrompus. Actuellement, macOS X n'est pas pris en charge. Aucune mise à jour des pilotes ODBC 32 bits ne sera publiée, sauf pour les correctifs de sécurité urgents. Pour télécharger et installer les pilotes ODBC pour les systèmes d'exploitation macOS X et 32 bits, consultez [Configuration d'une connexion ODBC](#).

Pour obtenir les dernières informations sur les modifications du pilote ODBC, consulter le [journal des modifications](#).

Rubriques

- [Obtention de l'URL ODBC](#)
- [Installation et configuration du pilote ODBC Amazon Redshift sur Microsoft Windows](#)
- [Installation et configuration du pilote ODBC Amazon Redshift sur Linux](#)

- [Configuration de l'authentification](#)
- [Conversion de types de données](#)
- [Configuration des 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 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 :

Valeurs du champ de l'URL ODBC

Champ	Valeur
<i>Driver</i>	Nom du pilote ODBC 64 bits à utiliser : Pilote ODBC Amazon Redshift (x64).
<i>Server</i>	L'hôte du point de terminaison du cluster Amazon Redshift.
<i>Database</i>	Base de données que vous avez créée pour votre cluster.
<i>UID</i>	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.
<i>PWD</i>	Mot de passe du compte utilisateur de la base de données vous permettant de vous connecter à la base de données.

Champ	Valeur
<i>Port</i>	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](#).

Installation et configuration du pilote ODBC Amazon Redshift sur Microsoft Windows

Configuration requise

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 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).

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 2.1.2.0 Dans la région de Chine \(Pékin\)](#), utilisez le lien suivant : [pilote](#) version 2.1.2.0

Le nom de ce pilote est Pilote ODBC Amazon Redshift (x64).

Note

Les pilotes ODBC 32 bits sont interrompus. D'autres mises à jour ne seront pas publiées, sauf pour les correctifs de sécurité urgents. Pour télécharger et installer les pilotes ODBC pour les systèmes d'exploitation 32 bits, consultez [Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows](#).

2. Vérifiez la [licence de la version 2.x du pilote ODBC Amazon Redshift](#).
3. Double-cliquez sur le fichier .msi et 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 AWS Identity and Access Management (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 minimum

Vous pouvez éventuellement choisir la version minimale de TLS/SSL que le pilote autorise le magasin de données à utiliser pour chiffrer les connexions. Par exemple, si vous spécifiez le protocole TLS 1.2, le protocole TLS 1.1 ne peut pas être utilisé pour chiffrer les 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 des valeurs pour `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.

Installation et configuration du pilote ODBC Amazon Redshift sur Linux

Configuration requise

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 :
 - Red Hat® Enterprise Linux® (RHEL) 8 ou version ultérieure
 - CentOS 8 ou version ultérieure.
- 150 Mo d'espace disque disponible.
- unixODBC 2.2.14 ou version ultérieure.
- glibc 2.26 ou version ultérieure.

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 : [pilote RPM 64 bits version 2.1.2.0](#) version 2.1.2.0

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. 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-2.x.xx.xxxx.x86_64.rpm
```

Utilisation d'un gestionnaire de pilotes ODBC pour configurer le pilote ODBC sur Linux

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.redshiftdbc.ini`
- `odbc.ini`
- `odbcinst.ini`

Si vous l'avez installé à l'emplacement par défaut, le fichier de configuration `amazon.redshiftdbc.ini` se trouve dans `/opt/amazon/redshiftdbcx64`.

De plus, sous `/opt/amazon/redshiftdbcx64`, 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.redshiftdbc.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`. Ensuite, fournissez une chaîne de connexion sans DSN 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/redshiftdbcx64/librsodbc64.so
```

Configuration de l'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 ODBC obligatoire et options de connexion facultatives


Méthode d'authentification	Obligatoire	Facultatif
Standard	<ul style="list-style-type: none"> Host (Hôte) Port Base de données UID Mot de passe 	
Profil IAM	<ul style="list-style-type: none"> Host (Hôte) Port Base de données 	<ul style="list-style-type: none"> ClusterID Région AutoCreate

Méthode d'authentification	Obligatoire	Facultatif
	<ul style="list-style-type: none"> • IAM • Profil 	<ul style="list-style-type: none"> • EndpointURL • StsEndpointURL • InstanceProfile <div data-bbox="1068 436 1507 846" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.</p> </div>
Informations d'identification IAM	<ul style="list-style-type: none"> • Host (Hôte) • Port • Base de données • IAM • AccessKeyID • SecretAccessClé 	<ul style="list-style-type: none"> • ClusterID • Région • AutoCreate • EndpointURL • StsEndpointURL • SessionToken • UID <div data-bbox="1068 1335 1507 1745" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.</p> </div>


Méthode d'authentification	Obligatoire	Facultatif
AD FS	<ul style="list-style-type: none"> • Host (Hôte) • Port • Base de données • IAM • plugin_name • UID • Mot de passe • IdP_Host • IdP_Port 	<ul style="list-style-type: none"> • ClusterID • Région • AutoCreate • EndpointUrl • StsEndpointURL • Preferred_Role • se connecter ToRp • SSL_Insecure <div data-bbox="1068 737 1510 1146" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.</p> </div>

Méthode d'authentification	Obligatoire	Facultatif
Azure AD	<ul style="list-style-type: none"> • Host (Hôte) • Port • Base de données • IAM • plugin_name • UID • Mot de passe • IdP_Tenant • Client_ID • Client_Secret 	<ul style="list-style-type: none"> • ClusterID • Région • AutoCreate • EndpointUrl • StsEndpointURL • Preferred_Role • dbgroups_filter <div data-bbox="1068 678 1510 1087" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.</p> </div>
JWT	<ul style="list-style-type: none"> • Host (Hôte) • Port • Base de données • IAM • plugin_name • web_identity_token 	<ul style="list-style-type: none"> • provider_name


Méthode d'authentification	Obligatoire	Facultatif
Okta	<ul style="list-style-type: none">• Host (Hôte)• Port• Base de données• IAM• plugin_name• UID• Mot de passe• IdP_Host• App_Name• App_ID	<ul style="list-style-type: none">• ClusterID• Région• AutoCreate• EndpointUrl• StsEndpointURL• Preferred_Role <div data-bbox="1068 621 1507 1029"><p> Note</p><p>Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.</p></div>


Méthode d'authentification	Obligatoire	Facultatif
Ping Federate	<ul style="list-style-type: none">• Host (Hôte)• Port• Base de données• IAM• plugin_name• UID• Mot de passe• IdP_Host• IdP_Port	<ul style="list-style-type: none">• ClusterID• Région• AutoCreate• EndpointUrl• StsEndpointURL• Preferred_Role• SSL_Insecure• partner_spid <div data-bbox="1068 739 1510 1146" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.</p></div>

Méthode d'authentification	Obligatoire	Facultatif
Navigateur Azure AD	<ul style="list-style-type: none">• Host (Hôte)• Port• Base de données• IAM• plugin_name• IdP_Tenant• Client_ID• UID	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> • Host (Hôte) • Port • Base de données • IAM • plugin_name • login_url • UID 	<ul style="list-style-type: none"> • ClusterID • Région • AutoCreate • EndpointUrl • StsEndpointURL • Preferred_Role • dbgroups_filter • IdP_Response_Timeout • listen_port <div data-bbox="1068 793 1507 1205" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 20px;"> <p> Note</p> <p>Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.</p> </div>
Profil d'authentification	<ul style="list-style-type: none"> • Host (Hôte) • Port • Base de données • AccessKeyID • SecretAccessClé 	

Méthode d'authentification	Obligatoire	Facultatif
Navigateur Azure AD OAUTH2	<ul style="list-style-type: none"> • Host (Hôte) • Port • Base de données • IAM • plugin_name • IdP_Tenant • Client_ID • UID 	<ul style="list-style-type: none"> • ClusterID • Région • EndpointUrl • IdP_Response_Timeout • listen_port • scope • provider_name <div data-bbox="1068 680 1507 1087" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.</p> </div>

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 plug-in de fournisseur d'informations d'identification basé sur SAML 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 codé en ASCII et doit contenir la paire clé-valeur suivante, où `PluginPath` est le chemin complet de l'application du plug-in :

```
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.

Conversion de types 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
GEOMETRY	SQL_LONGVARBINARY
INTEGER	SQL_INTEGER
REAL	SQL_REAL
SMALLINT	SQL_SMALLINT
SUPER	SQL_LONGVARCHAR

Type Amazon Redshift	Type SQL
TEXT	SQL_LONGVARCHAR
TIME	SQL_TYPE_TIME
TIMETZ	SQL_TYPE_TIME
TIMESTAMP	SQL_TYPE_TIMESTAMP
TIMESTAMPZ	SQL_TYPE_TIMESTAMP
VARBYTE	SQL_LONGVARBINARY
VARCHAR	SQL_VARCHAR

Configuration des 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`. Pour plus d'informations sur la configuration d'une DSN, consultez [Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows](#).

Sous Linux, vous définissez les options de configuration du pilote dans vos fichiers `odbc.ini` et `amazon.redshiftdbc.ini`, comme décrit à la section [Utilisez un gestionnaire de pilotes ODBC pour configurer le pilote sur les systèmes d'exploitation Linux et macOS X](#). Les options de configuration définies dans un fichier `amazon.redshiftdbc.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.redshiftdbc.ini`.

Vous trouverez ci-dessous des descriptions des options que vous pouvez spécifier pour le pilote ODBC Amazon Redshift version 2.x :

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 spécifier `SecretAccessKey`.

Ce paramètre est facultatif.

app_id

- Valeur par défaut – Aucune
- Types de données – Chaîne

L'ID unique fourni par Okta associé à votre application Amazon Redshift.

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` la clé.

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 IAM Identity Center ou des jetons d'identité basés sur OpenID Connect (OIDC) JSON (JWT) provenant de n'importe quel fournisseur d'identité Web lié à IAM Identity Center.
- 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.

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 : désactivée
- 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 lz4 Redshift sur.
- zstd : définit la méthode de compression utilisée pour les communications par protocole filaire avec Amazon Redshift sur. zstd
- off : 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.

DatabaseMetadataCurrentDbUniquement

- 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'DriverConnect API SQL.

Ce paramètre est obligatoire si vous ne définissez pas le 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.

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 tout DbGroups ce qui est envoyé 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'getClusterCredentialsWithIAMAPI est utilisée pour obtenir des informations d'identification de cluster temporaires dans les clusters provisionnés. Cette option

permet aux utilisateurs IAM d'intégrer les rôles de base de données Redshift dans les clusters provisionnés. Notez que cette option ne s'applique pas aux espaces de noms Redshift Serverless.

- 1 | VRAI : Le pilote utilise `getClusterCredentialsWithIAMAPI` pour obtenir des informations d'identification de cluster temporaires dans les clusters provisionnés.
- 0 | FALSE : le pilote utilise `getClusterCredentialsAPI` par défaut pour obtenir des informations d'identification de cluster temporaires dans les clusters provisionnés.

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.

`identity_namespace`

- Valeur par défaut – Aucune
- Types de données – Chaîne

L'espace de noms d'identité à utiliser lors de l'authentification à l'aide de `IdpTokenAuthPlugin`. Cela aide Redshift à déterminer l'instance IAM Identity Center à utiliser.

S'il existe une seule instance IAM Identity Center ou si l'espace de noms d'identité par défaut est défini, ce paramètre est facultatif ; sinon, il est obligatoire.

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_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 liés par chaîne spécifié par l'option Nom du profil (Profil) à la place.

Ce paramètre est facultatif.

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.

KeepAliveCompter

- 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.

KeepAliveIntervalle

- 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.

KeepAliveHeure

- 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 lors de l'utilisation des services SAML ou Azure AD 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

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 : ERROR. Enregistre les événements d'erreur qui pourraient permettre au pilote de continuer à fonctionner, mais qui produisent une erreur.
- 2 : API_CALL. Enregistre les appels de fonctions de l'API ODBC avec les valeurs des arguments de fonction.
- 3 : INFO. Enregistre les informations générales qui décrivent la progression du pilote.
- 4 : MSG_PROTOCOL. Enregistre les informations détaillées sur le protocole de messages du pilote.
- 5 : DEBUG. Enregistre toutes les activités du pilote.
- 6 : DEBUG_APPEND. Continue d'ajouter des journaux pour toutes les activités du pilote.

Lorsque la journalisation est activée, le pilote produit les fichiers journaux suivants à l'emplacement que vous spécifiez dans la `LogPath` propriété :

- 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 TEMP spécifique au système d'exploitation
- Types de données – Chaîne

Le chemin complet du dossier dans lequel le pilote enregistre les fichiers journaux lorsqu'il `LogLevel` est supérieur à 0.

Ce paramètre est facultatif.

Min_TLS

- Valeur par défaut : 1,2
- Types de données – Chaîne

Version minimale de 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 | PWS

- 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.
- `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 IAM Identity Center ou des jetons d'identité basés sur le JSON OpenID Connect (OIDC) (JWT) provenant de n'importe quel fournisseur d'identité Web 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.

`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.

SecretAccessClé

- 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.

Ce paramètre est facultatif.

StsConnectionDélai d'expiration

- Valeur par défaut : 0
- Type de données – Entier

Durée d'attente maximale pour les connexions IAM, en secondes. Si la valeur est définie sur 0 ou si elle n'est pas spécifiée, 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 indique le point de terminaison secondaire utilisé pour communiquer avec le 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 IAM Identity Center ou un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web lié à IAM Identity Center. Votre application doit générer ce jeton en authentifiant l'utilisateur de votre application auprès d'IAM Identity Center ou d'un fournisseur d'identité lié à IAM Identity Center.

Ce paramètre fonctionne avec `IdpTokenAuthPlugin`.

type_jeton

- Valeur par défaut – Aucune
- Types de données – Chaîne

Type de jeton utilisé dans `IdpTokenAuthPlugin`.

Vous pouvez spécifier les valeurs suivantes :

JETON D'ACCÈS

Entrez cette valeur si vous utilisez un jeton d'accès fourni par IAM Identity Center.

EXT_JET

Entrez cette valeur si vous utilisez un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web intégré à 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.

`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/2.1.1.0/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/ AmazonRedshift ODBC64-2.0.1.0.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/ AmazonRedshift ODBC64-2.0.0.11.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/ AmazonRedshift ODBC64-2.0.0.9.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/ AmazonRedshift ODBC64-2.0.0.8.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/ AmazonRedshift ODBC64-2.0.0.7.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/ AmazonRedshift ODBC64-2.0.0.6.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/ AmazonRedshift ODBC64-2.0.0.5.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/ AmazonRedshift ODBC64-2.0.0.3.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/ AmazonRedshift ODBC64-2.0.0.1.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/2.1.1.0/ AmazonRedshift ODBC-64-bit-2.1.1.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.0.0/ AmazonRedshift ODBC-64-bit-2.1.0.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/ AmazonRedshift ODBC-64-bit-2.0.1.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/ AmazonRedshift ODBC-64-bit-2.0.0.11.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/ AmazonRedshift ODBC-64-bit-2.0.0.9.x86_64.rpm

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/ AmazonRedshift ODBC-64-bit-2.0.0.8.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/ AmazonRedshift ODBC-64-bit-2.0.0.7.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/ AmazonRedshift ODBC-64-bit-2.0.0.6.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/ AmazonRedshift ODBC-64-bit-2.0.0.5.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/ AmazonRedshift ODBC-64-bit-2.0.0.3.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/ AmazonRedshift ODBC-64-bit-2.0.0.1.x86_64.rpm

Configuration d'une connexion ODBC

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 X. 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](#).

Si vous souhaitez utiliser une connexion ODBC, procédez comme suit.

Rubriques

- [Obtenir l'URL ODBC pour votre cluster](#)
- [Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows](#)

- [Installer le pilote ODBC Amazon Redshift sous Linux](#)
- [Installer le pilote ODBC d'Amazon Redshift sur macOS X](#)
- [Utilisez un gestionnaire de pilotes ODBC pour configurer le pilote sur les systèmes d'exploitation Linux et macOS X](#)
- [Configurer les options du pilote ODBC](#)
- [Versions antérieures du pilote ODBC](#)

Obtenir l'URL ODBC pour votre cluster

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=password`

Les champs du format indiqué ci-dessus ont les valeurs suivantes.

Champ	Valeur
Driver	Nom du pilote ODBC 64 bits à utiliser :Amazon Redshift (x64). 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](#).

Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows

Configuration système requise

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](#).

Installation du pilote Amazon Redshift sur les systèmes d'exploitation Windows

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 1.5.9 du pilote ODBC 64 bits](#) version 1.5.9.

Le nom de ce pilote est Amazon Redshift (x64).

- [Version du pilote ODBC 32 bits 1.4.52](#) 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-cliquez sur le fichier .msi et 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 sur Microsoft Windows

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 AWS Identity and Access Management (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 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. Utilisez 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.

Installer le pilote ODBC Amazon Redshift sous Linux

Configuration système requise

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](#).

Installation du pilote Amazon Redshift sur les systèmes d'exploitation Linux

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/redshiftdbc/lib/64` (pour le pilote 64 bits)

- /opt/amazon/redshiftdbc/ErrorMessage
- /opt/amazon/redshiftdbc/Setup
- /opt/amazon/redshiftdbc/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 1.5.9 du pilote RPM 64 bits](#) 1.5.9.
 - [Version 1.5.9 du pilote Debian 64 bits](#) 1.5.9.
 - [Version 1.4.52 du pilote RPM 32 bits](#) 1.4.52
 - [Version du pilote Debian 32 bits 1.4.52](#) version 1.4.52

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 [Utilisez un gestionnaire de pilotes ODBC pour configurer le pilote sur les systèmes d'exploitation Linux et macOS X](#).

Installer le pilote ODBC d'Amazon Redshift sur macOS X

Configuration système requise

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](#).

Installation du pilote ODBC d'Amazon Redshift sur macOS X

Suivez les étapes de cette section pour télécharger et installer le pilote ODBC Amazon Redshift sur une version prise en charge de macOS X. Le processus d'installation installe les fichiers du pilote dans les répertoires suivants :

- /opt/amazon/redshift/lib/universal
- /opt/amazon/redshift/ErrorMessage
- /opt/amazon/redshift/Setup

Pour installer le pilote ODBC Amazon Redshift sur macOS X

1. Si votre système macOS X utilise une architecture Intel, téléchargez le [pilote Intel pour macOS X version 1.5.9](#). Si votre système utilise une architecture ARM, téléchargez le [pilote ARM pour macOS X version 1.5.9](#). Dans les deux cas, le nom de ce pilote est Amazon Redshift ODBC driver.

Ensuite, téléchargez et consultez le [Contrat de licence du pilote ODBC et JDBC d'Amazon Redshift](#).

2. Double-cliquez sur AmazonRedshiftODBC.dmg pour monter l'image disque.
3. Double-cliquez sur AmazonRedshiftODBC.pkg pour exécuter le programme d'installation.
4. 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 [Utilisez un gestionnaire de pilotes ODBC pour configurer le pilote sur les systèmes d'exploitation Linux et macOS X](#).

Utilisez un gestionnaire de pilotes ODBC pour configurer le pilote sur les systèmes d'exploitation Linux et macOS X

Sur les systèmes d'exploitation Linux et macOS X, 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 dépend du système d'exploitation que vous utilisez :

- Gestionnaire de pilotes unixODBC (pour les systèmes d'exploitation Linux)
- Gestionnaire de pilotes iODBC (pour système d'exploitation macOS X)

Pour plus d'informations sur les gestionnaires de pilotes ODBC pris en charge pour configurer les pilotes ODBC Amazon Redshift, consultez [Configuration système requise](#) pour les systèmes d'exploitation Linux et [Configuration système requise](#) pour les systèmes d'exploitation macOS X. 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.redshiftdbc.ini`, `odbc.ini` et `odbcinst.ini`.

Si vous l'avez installé à l'emplacement par défaut, le fichier de configuration `amazon.redshiftdbc.ini` se trouve dans l'un des répertoires suivants :

- `/opt/amazon/redshiftdbc/lib/64` (pour le pilote 64 bits sur les systèmes d'exploitation Linux)
- `/opt/amazon/redshiftdbc/lib/32` (pour le pilote 32 bits sur les systèmes d'exploitation Linux)
- `/opt/amazon/redshift/lib` (pour le pilote sur macOS X)

En outre, sous `/opt/amazon/redshiftdbc/Setup` sous Linux ou `/opt/amazon/redshift/Setup` sous macOS X, il existe des exemples `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 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.redshiftdbc.ini` dans un répertoire autre que le répertoire d'installation. Si vous copiez ce fichier vers le répertoire de base de l'utilisateur, ajoutez 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 ou macOS X 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.redshiftdbc.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 et 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 « [Création d'un nom de source de données sur un ordinateur autre que Windows](#) » dans le guide d'[installation et de configuration du connecteur ODBC Amazon Redshift](#). Pour la

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
```

Sur les systèmes d'exploitation macOS X, utilisez le format suivant :

```
[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 illustre la configuration de `odbc.ini` sur les systèmes d'exploitation macOS X :

```
[ODBC Data Sources]
Amazon_Redshift_dylib=Amazon Redshift DSN for macOS X

[Amazon Redshift DSN for macOS X]
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 Linux et macOS X

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`. Ensuite, fournissez une chaîne de connexion sans DSN dans votre application.

Pour plus d'informations sur la configuration du fichier `odbcinst.ini` dans ce cas de figure, consultez « [Configuring a DSN-less Connection on a Non-Windows Machine](#) » (Configuration d'une connexion sans DSN sur une machine non Windows) 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
```

Sur les systèmes d'exploitation macOS X, utilisez le format suivant :

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/lib/amazonredshiftodbc.dylib
...
```

L'exemple suivant illustre la configuration du fichier `odbcinst.ini` pour le pilote installé dans le répertoire par défaut sur les systèmes d'exploitation macOS X.

```
[ODBC Drivers]
```

```
Amazon RedshiftODBC DSN=Installed
```

```
[Amazon RedshiftODBC DSN]
```

```
Description=Amazon Redshift ODBC Driver for macOS X
```

```
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. Consultez également la rubrique « 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](#).

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](#).

Configurer les 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 [Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows](#).

Sous Linux et macOS X, vous définissez les options de configuration du pilote dans vos fichiers `odbc.ini` et `amazon.redshiftdbc.ini`, comme décrit à la section [Utilisez un gestionnaire de pilotes ODBC pour configurer le pilote sur les systèmes d'exploitation Linux et macOS X](#). Les options de configuration définies dans un fichier `amazon.redshiftdbc.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.redshiftdbc.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.

Utiliser les versions antérieures du pilote ODBC pour Windows

Voici les pilotes 64 bits :

- <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/ AmazonRedshift ODBC64-1.4.59.1000.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/ AmazonRedshift ODBC64-1.4.56.1000.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/ AmazonRedshift ODBC64-1.4.53.1000.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/ AmazonRedshift ODBC64-1.4.52.1000.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.

Utiliser les versions antérieures du pilote ODBC pour Linux

Les versions suivantes sont celles du pilote 64 bits :

- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/ AmazonRedshift ODBC-64-bit-1.5.7.1007-1.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/ AmazonRedshift ODBC-64-bit-1.4.65.1000-1.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/ AmazonRedshift ODBC-64-bit-1.4.62.1000-1.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/ AmazonRedshift ODBC-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.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift odbc-64-bit-1.4.59.1000-1.x86_64.deb](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/ AmazonRedshift ODBC-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.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift odbc-64-bit-1.4.56.1000-1.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.deb)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC-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.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift odbc-64-bit-1.4.52.1000-1.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.deb)

Les pilotes 32 bits ont été abandonnés et les versions précédentes ne sont pas prises en charge.

Utiliser les versions antérieures du pilote ODBC pour macOS X

Voici les versions du pilote ODBC Amazon Redshift pour macOS X :

- 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>

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.

Connexion à l'aide du protocole 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 :

- Téléchargez la solution groupée 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 [sur https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt](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 Federal Information Processing Standard (FIPS) 140-2. Par défaut, le mode SSL conforme à la norme FIPS est désactivé.

Important

N'activez le mode SSL compatible FIPS que si votre système doit être compatible FIPS.

Pour activer le mode SSL conforme à la norme FIPS, définissez le `use_fips_ssl` paramètre et le paramètre `true` dans le groupe de `require_ssl` 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 dans un groupe de travail, consultez [Configuration d'une connexion SSL conforme à la norme FIPS 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.

Utilisation du protocole SSL et des certificats d'autorités de certification approuvées 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 ODBC](#).

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 [Connexion à l'aide du protocole 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 X.

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.

sslmode (client)	require_SSL (serveur)	Résultat
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 [Connexion à l'aide du protocole 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 ODBC](#).

Utilisation du protocole SSL et des 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 [Connexion à l'aide du protocole 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 chinoises, 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 ODBC](#) ou [Configuration d'une connexion pour le pilote JDBC version 2.1 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 [Connexion à l'aide du protocole 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 [Connexion à l'aide du protocole 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 [Connexion à l'aide du protocole 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 [Connexion à l'aide du protocole SSL](#).
2. Placez les certificats du bundle dans votre fichier `root.crt`.
 - Sur les systèmes d'exploitation Linux et macOS X, 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 l'éditeur de requêtes d'Amazon Redshift 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 Amazon Redshift](#).

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. Tel est le cas des éléments suivants :

- Vous pouvez utiliser l'authentification unique à l'aide d'ADFS, Okta PingIdentity, Azure AdM ou d'autres fournisseurs d'identité basés sur SAML/JWT. 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 de tables externes dans un catalogue AWS Glue ou Apache Hive Metastore, des bases de données externes dans Amazon RDS for PostgreSQL, Amazon Aurora Édition compatible avec PostgreSQL, RDS for MySQL (prévisualisation) et Amazon Aurora Édition compatible avec MySQL (prévisualisation), ainsi que des tables partagées 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 X.

Pour signaler les problèmes liés à Amazon Redshift RSQL, écrivez à [`<redshift-rsql-support@amazon.com>`](mailto: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

- RPM Linux 64 bits : [RSQL version 1.0.8](#)
- DMG Mac OS 64 bits : [RSQL version 1.0.8](#)
- MSI Windows 64 bits : [RSQL version 1.0.8](#)

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 openssl
```

OpenSSL est requis pour les distributions Linux. La bibliothèque OpenSSL se trouve dans le référentiel GitHub [Linux OpenSSL](#). Pour plus d'informations sur OpenSSL, consultez [OpenSSL](#).

2. Installez le pilote ODBC : [Installation du pilote Amazon Redshift sur les systèmes d'exploitation Linux](#).
3. Copiez le fichier ini dans votre répertoire de base :

```
cp /opt/amazon/redshiftdbc/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/redshiftdbc/Setup
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshiftdbc/lib/64/
amazon.redshiftdbc.ini
```

Pour plus d'informations sur la configuration des variables d'environnement ODBC, consultez [Configuration des variables d'environnement](#).

5. Vous pouvez désormais installer RSQL en exécutant la commande suivante.

```
sudo rpm -i AmazonRedshiftRsql-<version>-1.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 openssl@1.1 --build-from-source
```

2. Installez le pilote ODBC : [Installer le pilote ODBC d'Amazon Redshift sur macOS X](#).
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
```

Pour plus d'informations sur la configuration des variables d'environnement ODBC, consultez [Configuration des variables d'environnement](#).

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-cliquez sur le fichier dmg pour monter l'image disque.
7. Double-cliquez sur le fichier pkg pour exécuter le programme d'installation.
8. 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 instructions sur [Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows](#) pour installer le pilote. Windows ne nécessite pas de gestionnaire de pilotes.

OpenSSL est requis pour Amazon Redshift RSQL sous Windows. La bibliothèque Windows OpenSSL se trouve dans le référentiel [Windows OpenSSL](#). GitHub Pour plus d'informations sur OpenSSL, consultez [OpenSSL](#).

Double-cliquez sur le fichier de téléchargement de RSQL pour exécuter le programme d'installation, puis suivez les étapes pour terminer l'installation.

Journal des modifications Amazon Redshift RSQL

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 messages ERROR/INFO en double.

New

- 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).

New

- 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.

New

- 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 RSPASSWORD=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 `\l` 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

- [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

- [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

- [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

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 disposant des autorisations permettant de se connecter au cluster.
- *<databasename>* est le Nom de 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 du mot de passe psql, saisissez le mot de passe de l'utilisateur *<username>*.

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 à l'aide d'un DSN

Vous pouvez connecter RSQL à Amazon Redshift à l'aide d'un nom de source de données (DSN) pour simplifier l'organisation des propriétés de la connexion. Pour plus d'informations, consultez [Configuration des fonctions de connexion](#). Cette rubrique contient des instructions pour l'installation du pilote ODBC et des descriptions des propriétés DSN. Par exemple, la section suivante, [Installation et configuration du pilote ODBC Amazon Redshift sur Microsoft Windows](#), montre comment se connecter à un DSN via Windows.

Utilisation d'une connexion DSN avec un mot de passe

L'exemple suivant montre une configuration de connexion DSN 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. L'exemple suivant montre une configuration de connexion DSN utilisant 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 une configuration de connexion DSN utilisant 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 affichent `n/a` (Non applicable).

`Unique Constraints` (Contraintes uniques) répertorie les contraintes uniques et les contraintes de clé principale sur la table.

`Foreign-key constraints` (Contraintes de clé étrangère) répertorie les contraintes de clé étrangère sur la table.

`\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" assignment	polygon	polygon	in
abstime	date	date	in
abstime	integer	(binary coercible)	no
abstime	time without time zone	time	in
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
bigint	character varying	text	in
bigint	double precision	float8	yes
bigint	integer	int4	in
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 catalogue de AWS Glue données, Hive Metastore et les tables fédérées des tables de partage de données Amazon RDS/Aurora MySQL, Amazon RDS/Aurora PostgreSQL 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_linenumbr  | 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 titedashes on
select * from td_dwh.accounts;
\export reset
```

Sortie de console

```
Rformat is off.
Target width is 1500.
Heading is set to: General Title
Titedashes 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 `\echo` en 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';
\rif :ACTIVITYCOUNT = 0
\rremark 'views do not exist'
\rendif
```

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.rsq1 :

```
\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.rsq1` :

```

\remark Starting...
\pset border 2
\pset format wrapped
\pset expanded on
\pset title 'Great Title'
select * from rsql_test.tbl_long where id = 500;
\reset rformat
select * from rsql_test.tbl_long where id = 500;
\reset rformat off
select * from rsql_test.tbl_long where id = 500;
\reset 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.rsq1 :

```
\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;
\reset 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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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
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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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 transaction non valide	invalid_transaction_state
25001	Classe 25 – État de transaction non valide	active_sql_transaction
25002	Classe 25 – État de transaction non valide	invalid_transaction_state

Code d'erreur	Classe d'erreur	Nom de la condition
25008	Classe 25 – État de transaction non valide	held_cursor_requires_same_isolation_level
25003	Classe 25 – État de transaction non valide	inappropriate_access_mode_for_branch_transaction
25004	Classe 25 – État de transaction non valide	inappropriate_isolation_level_for_branch_transaction
25005	Classe 25 – État de transaction non valide	no_active_sql_transaction_for_branch_transaction
25006	Classe 25 – État de transaction non valide	read_only_sql_transaction
25007	Classe 25 – État de transaction non valide	no_active_sql_transaction_for_branch_transaction
25P01	Classe 25 – État de transaction non valide	no_active_sql_transaction
25P02	Classe 25 – État de transaction 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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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

Code d'erreur	Classe d'erreur	Nom de la condition
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
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
```

Connexion avec SQL Workbench/J

Vous pouvez vous connecter à une base de données en utilisant SQL Workbench/J, un outil de requête SQL gratuit, indépendant du SGBD et multiplateforme.

Amazon Redshift ne fournit ni n'installe aucun outil ou bibliothèque client SQL tiers, vous devez donc installer ceux que vous souhaitez utiliser avec votre base de données. Pour installer SQL Workbench/J, suivez les instructions de la documentation de SQL Workbench/J ([SQL Workbench/J](#)). En général, pour utiliser SQL Workbench/J, vous devez procéder comme suit :

- Vérifiez la licence logicielle de SQL Workbench/J.
- Téléchargez le package SQL Workbench/J approprié pour votre système d'exploitation sur votre ordinateur client ou votre instance Amazon EC2.

- Installez SQL Workbench/J sur votre système.

Installez l'Environnement d'exécution Java (JRE) sur votre système. Vérifiez que vous utilisez la version correcte du JRE requise par le client SQL Workbench/J.

- Connectez-vous à votre base de données via une connexion JDBC dans SQL Workbench/J.

Vérifiez que votre ordinateur client ou votre instance Amazon EC2 dispose du pilote JDBC Amazon Redshift recommandé. Pour accéder aux liens permettant de télécharger les pilotes les plus récents, consultez [Télécharger le pilote Amazon Redshift JDBC, version 2.1](#). Vérifiez également que vous avez configuré les paramètres du pare-feu pour autoriser l'accès à votre base de données. Pour plus d'informations, consultez [Étape 4 : Autoriser l'accès au cluster dans le Guide de mise en route Amazon Redshift](#).

- Créez un nouveau profil de connexion dans SQL Workbench/J qui utilise le pilote Amazon Redshift.

Connectez-vous à votre entrepôt de données par programmation

Pour en savoir plus sur les outils permettant de créer des applications pour se connecter à votre entrepôt des données, consultez [Outils pour créer sur AWS](#).

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.

Après avoir créé un profil d'authentification, les utilisateurs peuvent l'ajouter 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` la section Profil.](#)

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 référez 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 la section [CreateAuthenticationProfil](#).

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.

Utilisation des profils d'authentification

Une fois que vous avez créé un profil d'authentification, vous pouvez inclure le nom du profil comme option de connexion pour JDBC version 2.0 `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](#).

⚠ 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.

Rubriques

- [Connexion depuis l'extérieur d'Amazon EC2 — problème de dépassement de délai du pare-feu](#)
- [La connexion est refusée ou échoue](#)
- [Le client et le pilote sont incompatibles](#)
- [Des requêtes semblent se bloquer et parfois échouent à atteindre le cluster](#)
- [Définition du paramètre de taille d'extraction JDBC](#)

Connexion depuis l'extérieur d'Amazon EC2 — problème de dépassement de délai du pare-feu**Exemple de problème**

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 l'expiration TCP/IP. 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 [Modification des paramètres d'expiration de TCP/IP](#).
- 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](#).

Modification des paramètres d'expiration de TCP/IP

Pour modifier les paramètres d'expiration de TCP/IP, 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 \ CurrentControl Set \ Services \ Tcpip \ Parameters \` :
 - KeepAliveDurée : 30000
 - KeepAliveIntervalle : 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 spécifier 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` :

KeepAlivesCompter

Nombre de paquets TCP `keepalive` qui peuvent être perdus avant que la connexion soit considérée comme interrompue.

KeepAlivesInactif

Nombre de secondes d'inactivité avant que le pilote envoie un paquet TCP keepalive.

KeepAlivesIntervalle

Nombre de secondes entre chaque retransmission de paquet TCP keepalive.

Sous Windows, vous modifiez ces paramètres dans le registre en ajoutant ou en modifiant les clés de HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI*you_DSN*. Sous Linux et macOS, vous ajoutez ou modifiez ces paramètres directement dans l'entrée DSN cible du fichier odbc.ini. Pour plus d'informations sur la modification du fichier odbc.ini sur les ordinateurs Linux et macOS, consultez [Utilisez un gestionnaire de pilotes ODBC pour configurer le pilote sur les systèmes d'exploitation Linux et macOS X](#).

Si ces paramètres n'existent pas ou s'ils ont une valeur égale à 0, le système utilise les paramètres keepalive spécifiés pour TCP/IP afin de déterminer le comportement DSN keepalive. Sous Windows, vous pouvez trouver les paramètres TCP/IP dans le registre dans HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\. Sous Linux et macOS, les paramètres TCP/IP sont disponibles dans le fichier sysctl.conf.

La connexion est refusée ou échoue

Exemples d'erreurs

- « Impossible d'établir une connexion à *<endpoint>*. »
- « Impossible de se connecter au serveur : la connexion a expiré. Le serveur s'exécute-t-il sur l'hôte '*<endpoint>*' et accepte-t-il les connexions TCP/IP sur le port '*<port>*' ? »
- « Connexion refusée. Vérifiez que le nom d'hôte et le port sont corrects et que l'administrateur accepte les connexions TCP/IP. »

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 la règle d'entrée au groupe de sécurité du VPC qui spécifie l'adresse CIDR/IP de votre client dans Amazon VPC. Pour plus d'informations sur la configuration des groupes de sécurité du VPC pour votre cluster et les options publiquement accessibles, consultez [Gestion des clusters dans un VPC](#).
- Si vous avez créé votre cluster Amazon Redshift en dehors d'un VPC, ajoutez l'adresse CIDR/IP de votre 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 du cluster 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

Exemple d'erreur

« La DSN spécifiée contient une incompatibilité d'architecture entre le pilote et l'application. »

Solution possible

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

Exemple de problème

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.

Solution possible

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 (trames jumbo TCP/IP).

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 plateforme EC2-VPC, 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 plateforme EC2-Classique ou si vous ne pouvez pas autoriser la règle de trafic entrant ICMP, désactivez les trames jumbo TCP/IP afin que des 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 du cluster Amazon Redshift](#). Pour les clusters utilisant la plateforme EC2-VPC, Amazon Redshift utilise les 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 instances EC2-Classic ou EC2-VPC, consultez la section [Différences entre les instances dans 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 [Gestion des groupes de sécurité VPC pour un Cluster](#). Pour plus d'informations sur les paramètres PMTUD spécifiques requis par cette règle, consultez la section [Path MTU discovery](#) dans le guide de l'utilisateur Amazon EC2.

Configuration de la MTU d'une instance

Dans certains cas, votre cluster peut utiliser la plate-forme EC2-Classic 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. Cet ajustement désactive les trames jumbo TCP/IP pour s'assurer que les connexions utilisent systématiquement 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 sur le site de support macOS sur [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 JDBC collecte tous les résultats pour une requête à la fois. Par conséquent, lorsque vous tentez de récupérer un ensemble de résultats volumineux via une connexion JDBC, vous risquez de rencontrer une erreur côté client `out-of-memory`. Pour permettre à votre client de récupérer des ensembles de résultats par lots plutôt que par une seule `all-or-nothing` extraction, définissez le paramètre de taille de lecture JDBC dans votre application cliente.

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 des ensembles de données volumineux, 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

Vous pouvez accéder à votre base de données Amazon Redshift en utilisant l'API de données Amazon Redshift intégrée. À l'aide de cette API, vous pouvez accéder aux données Amazon Redshift via des applications basées sur des services Web, notamment des blocs-notes AWS Lambda Amazon SageMaker et. AWS Cloud9 Pour plus d'informations sur ces applications [AWS Lambda](#), consultez [Amazon SageMaker](#) et [AWS Cloud9](#).

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 avec AWS les 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 de données utilise soit des informations d'identification stockées dans la base de données, AWS Secrets Manager soit 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 AWS Secrets Manager, voir [Qu'est-ce que c'est AWS Secrets Manager ?](#) dans le guide de AWS Secrets Manager l'utilisateur.

Pour plus d'informations sur les fonctions de l'API de données, consultez la [Référence de l'API de données Amazon Redshift](#).

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 ou avec des informations d'identification temporaires. Pour plus d'informations, consultez [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 identifiants de base de données dans AWS Secrets Manager](#).
4. Passez en revue les considérations et les limitations lors de l'appel de l'API de données. Pour plus d'informations, consultez [Considérations relatives à l'appel à l'API de données Amazon Redshift](#).
5. Appelez l'API Data depuis 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 des exemples d'appels depuis le AWS CLI, voir [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 [Redshift](#) Data dans le. Référence générale d'Amazon Web Services
- La durée maximale d'une requête est de 24 heures.
- Le nombre maximal de requêtes actives (requêtes STARTED et SUBMITTED) par cluster Amazon Redshift est de 200.
- La taille maximale du résultat de la requête est de 100 Mo (après compression gzip). Si l'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.

- L'API de données est à même de lancer des requêtes sur des clusters à un ou plusieurs nœuds des types de nœuds suivants :
 - dc2.large
 - dc2.8xlarge
 - ra3.xlplus
 - ra3.4xlarge
 - ra3.16xlarge
- Le cluster doit être dans un cloud privé virtuel (VPC) basé sur le service Amazon VPC.
- Par défaut, les utilisateurs ayant le même rôle IAM ou les mêmes autorisations IAM que l'exécutant d'une fonction API `ExecuteStatement` ou `BatchExecuteStatement` peuvent agir sur la même déclaration avec des fonctions API `CancelStatement`, `DescribeStatement`, `GetStatementResult` 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 paramètre `Sqls` de l'opération d'API `BatchExecuteStatement` sont exécutées en tant que transaction unique. Ils s'exécutent en série dans l'ordre du tableau. Les instructions SQL suivantes ne démarrent pas tant que l'instruction précédente du tableau n'est pas terminée. Si une instruction SQL échoue, c'est parce qu'elle est exécutée comme une seule transaction que tout le travail est annulé.
- La durée de conservation maximale d'un jeton client utilisé dans une opération d'API `ExecuteStatement` ou `BatchExecuteStatement` est de 8 heures.
- 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 mise en œuvre automatiquement pour limiter les erreurs dans certains 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 Secrets Manager

Avec cette méthode, fournissez `secret-arn` le 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 plus d'informations, consultez [Stockage des identifiants de base de données dans AWS Secrets Manager](#).

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 ces méthodes, vous pouvez également fournir une `region` valeur qui indique 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

Type de données JDBC	Type de données API de données
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 `execute-statement` AWS CLI commande.

```
--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) > :val1`.
- 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.
- Seule l'opération `execute-statement` prend en charge les instructions SQL avec des paramètres.

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 le `ClientToken`. Pour un exemple de CloudTrail journal, voir [Exemples d'API de données Amazon Redshift](#).

La commande `aws redshift-data execute-statement` illustre le paramètre facultatif `client-token` pour l'idempotence.

```
aws redshift-data execute-statement
  --region us-west-2
  --secret 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	Recommandation	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	<p>La demande présente un problème, parmi les suivants :</p> <ul style="list-style-type: none"> 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. <p>Si la demande concerne une ressource en train de changer d'état, il est possible que la nouvelle tentative aboutisse.</p>
Codes de réponse de la série 500	Réessayer	L'erreur est due à un problème AWS côté serveur et est généralement transitoire.

Réponse	Recommandation	Commentaires
		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.

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 AWS Identity and Access Management (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, reportez-vous à la console IAM (<https://console.aws.amazon.com/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'Amazon Redshift AWS Secrets Manager et d'API IAM nécessaires pour authentifier et accéder à un cluster Amazon Redshift ou à un groupe de travail Redshift Serverless.

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 utilisez cette AWS Secrets Manager option pour vous authentifier, vérifiez que la politique autorise l'utilisation de `secretsmanager:GetSecretValue` 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 source AWS Identity and Access Management (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.

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 :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::accountID-of-account-A:role/someRoleA"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Enfin, le rôle IAM du compte A doit être en mesure d'assumer le rôle IAM du compte B.

```
{
  "Version": "2012-10-17",
```

```
"Statement": {
  "Effect": "Allow",
  "Action": "sts:AssumeRole",
  "Resource": "arn:aws:iam::accountID-of-account-B:role/someRoleB"
}
```

Les liens suivants fournissent des informations supplémentaires sur AWS Identity and Access Management 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](#).

Stockage des identifiants de base de données dans 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 `AmazonRedshiftDataFullAccess` gérée par AWS permet uniquement l'action

`secretsmanager:GetSecretValue` pour les secrets marqués avec la clé `RedshiftDataFullAccess`.

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.

Pour créer un point de terminaison Amazon VPC (AWS PrivateLink) pour l'API de données

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. Grâce à AWS PrivateLink, vous pouvez créer des points de terminaison Amazon VPC, qui vous permettent de vous connecter aux services sur différents comptes et VPC basés sur Amazon VPC. Pour plus d'informations AWS PrivateLink, consultez la section [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 sur le AWS réseau, 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 à la console Amazon VPC AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/vpc/`.](https://console.aws.amazon.com/vpc/)
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 VPC de l'API de données à l'aide des AWS SDK AWS CLI ou SDK sans apporter de modifications de code ou de configuration pour mettre à jour l'URL du point de terminaison de l'API de données.

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, choisissez le lien dans le AWS Management Console 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 points de terminaison spécifiques au VPC pour appeler l'API de données dans l'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 prise 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 ajouter des groupes de base de données sous forme de balise à un rôle IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/iam/>.
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 les RedshiftDbgroupes de clés et une valeur qui est une liste de groupes de *base de données séparés par des deux-points*.
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.

Appel à l'API de données

Vous pouvez appeler l'API Data ou le AWS CLI pour exécuter des instructions SQL sur votre cluster ou votre 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 relatifs à l'appel de l'API de données, consultez [Getting Started with Redshift Data API](#) 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 Runtime. SageMaker 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-identifiant` 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.

Pour exécuter une instruction SQL

Pour exécuter une instruction SQL, utilisez la `aws redshift-data execute-statement` AWS CLI commande.

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 AWS Secrets Manager d'authentification.

```
aws redshift-data execute-statement
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwN
  --cluster-identifiant mycluster-test
  --sql "select * from stl_query limit 1"
  --database dev
```

Voici un exemple de réponse.

```
{
  "ClusterIdentifiant": "mycluster-test",
  "CreatedAt": 1598323175.823,
  "Database": "dev",
  "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
  "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:yanruiz-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
  --region us-west-2
  --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 AWS Secrets Manager d'authentification et un jeton d'idempuissance.

```
aws redshift-data execute-statement
  --region us-west-2
  --secret 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:yanruiz-secret-hKgPwn"
}
```

Pour exécuter une instruction SQL avec des paramètres

Pour exécuter une instruction SQL, utilisez la `aws redshift-data execute-statement` AWS CLI commande.

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 AWS Secrets Manager d'authentification. 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
  --region us-west-2
  --secret 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:yanruiz-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 my-test-cluster
--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 my-test-cluster
--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 my-test-cluster
--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 my-test-cluster
--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
```



```
}
```

Pour exécuter plusieurs instructions SQL

Pour exécuter plusieurs instructions SQL avec une seule commande, utilisez la `aws redshift-data batch-execute-statement` AWS CLI commande.

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
  --region us-west-2
  --db-user myuser
  --cluster-identifiant mycluster-test
  --database dev
  --sqls "set timezone to BST" "select * from mytable" "select * from another_table"
```

Voici un exemple de réponse.

```
{
  "ClusterIdentifiant": "mycluster-test",
  "CreatedAt": 1598306924.632,
  "Database": "dev",
  "DbUser": "myuser",
  "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

Pour 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
  --region us-west-2
```

```
--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
    }
  ]
}
```

Pour 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. L'autorisation d'exécuter cette commande est basée sur les autorisations IAM de l'appelant.

La AWS CLI commande suivante décrit une instruction SQL.

```
aws redshift-data describe-statement
  --id d9b6c0c9-0747-4bf4-b142-e8883122f766
  --region us-west-2
```

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
}

```

Pour récupérer les résultats d'une instruction SQL

Pour récupérer le résultat d'une instruction SQL exécutée, utilisez la `redshift-data get-statement-result` AWS CLI commande. 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.

L'instruction suivante renvoie le résultat d'une instruction SQL exécutée par `execute-statement`.

```

aws redshift-data get-statement-result
  --id d9b6c0c9-0747-4bf4-b142-e8883122f766

```

```
--region us-west-2
```

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
--region us-west-2
```

Voici un exemple de réponse à un appel à `get-statement-result`.

```
{
  "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
}
```

Pour décrire une table

Pour obtenir des métadonnées décrivant 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 décrivant une table. Cet exemple utilise la méthode AWS Secrets Manager d'authentification.

```
aws redshift-data describe-table
  --region us-west-2
  --cluster-identifiant mycluster-test
  --database dev
  --schema information_schema
  --table sql_features
  --secret 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
--region us-west-2
--db-user myuser
--cluster-identifiant 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"
  }
]
}
```

Pour répertorier les bases de données d'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
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifiant 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
  --region us-west-2
  --db-user myuser
  --cluster-identifiant mycluster-test
  --database dev
```

Voici un exemple de réponse.

```
{
  "Databases": [
    "dev"
  ]
}
```

```
}
```

Pour répertorier les schémas d'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
  --region us-west-2
  --secret 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
  --region us-west-2
  --db-user mysuser
  --cluster-identifier mycluster-test
  --database dev
```

Voici un exemple de réponse.

```
{
  "Schemas": [
    "information_schema",
    "pg_catalog",
    "pg_internal",
    "public"
  ]
}
```

Pour répertorier les tables d'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
  --region us-west-2
  --secret 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
  --region us-west-2
  --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 taille de l'API de données ne doit pas dépasser 100 Mo dans l'ensemble de résultats renvoyé par la base de données.

Pour résoudre ce problème, assurez-vous que les appels à l'API de données renvoient au maximum 100 Mo. Si vous avez besoin de renvoyer plus de 100 Mo, vous pouvez utiliser plusieurs appels d'instruction avec la clause LIMIT 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 de données avec EventBridge, le rôle IAM associé doit faire confiance au principal pour les 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 confiance du AWS service 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 name règle que vous créez dans Amazon EventBridge doit correspondre StatementName à celle duRedshiftDataParameters.

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 est utilisée pour 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 s'exécuter 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 est utilisée pour 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 s'exécuter 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 est utilisée pour 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 s'exécuter 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 est utilisée pour 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 s'exécuter 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 de données et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller l'API de données, signaler un 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 des ressources. Les événements liés AWS aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Pour plus d'informations, consultez le [guide de EventBridge l'utilisateur Amazon](#).
- AWS CloudTrail capture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour en savoir plus sur la façon dont Amazon Redshift est intégré AWS CloudTrail, consultez [Logging with CloudTrail](#). Pour plus d'informations CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Rubriques

- [Surveillance des événements pour l'API de données Amazon Redshift sur Amazon EventBridge](#)

Surveillance des événements pour l'API de données Amazon Redshift sur Amazon EventBridge

Vous pouvez surveiller les événements de l'API de données dans EventBridge, qui fournit un flux de données en temps réel à partir de vos propres applications, applications software-as-a-service (SaaS) et AWS services. EventBridge achemine ces données vers des cibles telles qu' AWS Lambda Amazon SNS. Ces événements sont les mêmes que ceux qui apparaissent dans CloudWatch Events, qui fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux 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 les [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
  }
}
```


Groupes de paramètres Amazon Redshift

Présentation

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.

A propos des groupes de paramètres

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 groupe de paramètres est la version du moteur Amazon Redshift à laquelle les paramètres du groupe de paramètres s'appliquent. Le format du nom de famille de groupe de paramètres est `redshift-version` où *version* désigne la version de moteur. Par exemple, la version actuelle du moteur est `redshift-1.0`.

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`, où *parameter_group_family* est la version du moteur auquel appartient le groupe de paramètres. Par exemple, le groupe de paramètres par défaut de la version `redshift-1.0` se nomme `default.redshift-1.0`.

Note

Pour l'instant, `redshift-1.0` est la seule version du moteur Amazon Redshift. Par conséquent, `default.redshift-1.0` est le seul groupe de paramètres par défaut.

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 ou l'un des AWS SDK pour consulter 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 modifiez les valeurs des paramètres d'un groupe de paramètres déjà associé à un cluster ou associez 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

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-1.0`.

Nom du paramètre	Valeur	En savoir plus
<code>auto_analyze</code>	<code>true</code>	auto_analyze dans le Manuel du développeur de base de données Amazon Redshift
<code>auto_mv</code>	<code>true</code>	Automated materialized views (Vues matérialisées automatisées) dans le Guide du développeur de base de données Amazon Redshift
<code>datestyle</code>	<code>ISO, MDY</code>	datestyle dans le Manuel du développeur de base de données Amazon Redshift

Nom du paramètre	Valeur	En savoir plus
<code>enable_case_sensitive_identifier</code>	false	enable_case_sensitive_identifier dans le Manuel du développeur de base de données Amazon Redshift
<code>enable_user_activity_logging</code>	false	Journalisation des audits de base de données dans ce guide
<code>extra_float_digits</code>	0	extra_float_digits dans le Manuel du développeur de base de données Amazon Redshift
<code>max_concurrency_scaling_clusters</code>	1	max_concurrency_scaling_clusters dans le Manuel du développeur de base de données Amazon Redshift
<code>query_group</code>	default	query_group dans le Manuel du développeur de base de données Amazon Redshift
<code>require_ssl</code>	false	Configuration des options de sécurité des connexions dans ce guide
<code>search_path</code>	\$user, public	search_path dans le Manuel du développeur de base de données Amazon Redshift
<code>statement_timeout</code>	0	statement_timeout dans le Manuel du développeur de base de données Amazon Redshift
<code>wlm_json_configuration</code>	[{"auto_wlm":true}]	Configuration de la gestion de la charge de travail dans ce guide
<code>use_fips_ssl</code>	false	N'activez le mode SSL compatible FIPS que si votre système doit être compatible FIPS.

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.

Configuration des valeurs des paramètres à l'aide du AWS CLI

Pour configurer les paramètres Amazon Redshift à l'aide de AWS CLI, vous devez utiliser la `modify-cluster-parameter-group` commande pour un groupe de paramètres spécifique. Vous spécifiez le groupe de paramètres à modifier dans `parameter-group-name`. Vous utilisez le paramètre `parameters` (pour la commande `modify-cluster-parameter-group` afin de spécifier les paires nom/valeur de chaque paramètre que vous voulez 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, consultez [Configuration de la gestion 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](#).

Syntaxe

La syntaxe suivante montre comment utiliser la commande `modify-cluster-parameter-group` pour configurer un paramètre. Vous spécifiez *parameter_group_name* et vous remplacez *parameter_name* et *parameter_value* par un véritable paramètre 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
```

Exemple

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 en réalité, il ne s'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
```

Vous pouvez gérer les groupes de paramètres à l'aide de la console. Pour plus d'informations, consultez [Gestion des groupes de paramètres à l'aide de la console](#).

Configuration de la 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 `wlm_json_configuration`

Vous pouvez configurer le WLM à l'aide de la console Amazon Redshift, de AWS CLI l'API Amazon Redshift ou de l'un des 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
Priorité	Oui	Non
Type de requête	Oui	Oui
Nom de la file d'attente	Oui	Oui
Mode de mise à l'échelle de la simultanéité	Oui	Oui
Simultanéité	Non	Oui

Propriété WLM	Gestion automatique de la charge de travail	Gestion manuelle de la charge de travail
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
Expiration	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. L'argument 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`. L'argument 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`. L'argument 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 `WLM`, `WLM QueueWait TimeQueueLength`, `WLM`, `WLM QueriesCompletedPerSecond`, `WLM`, `WLMQueryDuration`, etc.) `RunningQueries` change également. Ainsi, si vous modifiez le nom d'une file d'attente, vous devrez peut-être modifier les CloudWatch 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. L'argument 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 utilisateurs, consultez [Contrôle d'accès basé sur les rôles \(RBAC\)](#).

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, veuillez consulter [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_json_configuration` 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 formatée en notation JavaScript d'objet (JSON). Si vous configurez WLM à l'AWS CLI aide de l'API Amazon Redshift ou de AWS l'un des SDK, consultez le reste de cette section pour savoir comment créer la structure JSON du 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 paire nom-valeur ; name et value définissent ensemble les propriétés WLM de 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`.

Mise en forme de la commande de l' AWS CLI

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 d'informations sur la façon de construire la commande appropriée dans les systèmes d'exploitation Linux, Mac OS X et Windows, consultez les sections suivantes. Pour plus d'informations sur les différences entre les structures de données JSON et les structures de données AWS CLI en général, consultez la section [Quoting strings](#) 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 en utilisant le AWS CLI dans la ligne de commande avec un fichier JSON

Vous pouvez modifier le `wlm_json_configuration` paramètre à l'aide du AWS CLI et transmettre la valeur de l'`parameters` argument sous forme de 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 de AWS CLI la ligne de commande sur les systèmes d'exploitation Linux et macOS X

Suivez ces règles pour exécuter une AWS CLI commande avec des paramètres sur une 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 paires nom-valeur, un signe deux-points (:) sépare chaque propriété de sa valeur.
- Chaque paire nom-valeur est séparée d'une autre paire 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 de AWS CLI Windows PowerShell sur les systèmes d'exploitation Microsoft Windows

Suivez ces règles pour exécuter une AWS CLI commande avec des paramètres sur une 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 paires nom-valeur, un signe deux-points (:) sépare chaque propriété de sa valeur.
- Chaque paire nom-valeur est séparée d'une autre paire 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 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 paires nom-valeur, un signe deux-points (:) sépare chaque propriété de sa valeur.
- Chaque paire nom-valeur est séparée d'une autre paire 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 ({}).

Gestion des groupes de paramètres à l'aide de la console

Vous pouvez afficher, créer, modifier et supprimer des groupes de paramètres sur la console Amazon Redshift.

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). 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.

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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
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 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.

Pour modifier un groupe de paramètres

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
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 WLM.
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 wlm_json_configuration](#).

 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, WLM, WLMQueriesCompletedPerSecond, WLMQueryDuration, etc.) RunningQueries change également. Ainsi, si vous modifiez le nom d'une file d'attente, vous devrez peut-être modifier les CloudWatch alarmes 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.

Création ou modification d'une règle de surveillance de requête à l'aide de la console

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, veuillez consulter [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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`](https://console.aws.amazon.com/redshiftv2/).
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 WLM.
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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
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.

Association d'un groupe de paramètres à un cluster

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.

Gestion des groupes de paramètres à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift

Vous pouvez utiliser les opérations Amazon Redshift suivantes dans le AWS CLI pour gérer les groupes de paramètres.

- [create-cluster-parameter-group](#)
- [delete-cluster-parameter-group](#)
- [describe-cluster-parameters](#)
- [describe-cluster-parameter-groups](#)
- [describe-default-cluster-parameters](#)
- [modify-cluster-parameter-group](#)
- [reset-cluster-parameter-group](#)

Vous pouvez utiliser les opérations d'API Amazon Redshift suivantes pour gérer les groupes de paramètres.

- [CreateClusterParameterGroup](#)
- [DeleteClusterParameterGroup](#)
- [DescribeClusterParamètres](#)
- [DescribeClusterParameterGroups](#)
- [DescribeDefaultClusterParameters](#)
- [ModifyClusterParameterGroup](#)
- [ResetClusterParameterGroup](#)

Intégrer Amazon Redshift à un partenaire AWS

En utilisant Amazon Redshift, vous pouvez intégrer des AWS partenaires depuis la page de détails du cluster 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.

Intégration avec un AWS partenaire à l'aide de la console Amazon Redshift

Utilisez la procédure suivante pour intégrer un cluster à un AWS partenaire.

Pour intégrer un cluster Amazon Redshift à un partenaire AWS

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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. Achèvement la suppression sur le site web du partenaire.

Chargement de données auprès de 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 [Autoriser le 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](#) – [Adresses IP](#)

Pour intégrer un cluster Amazon Redshift à Informatica

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

Achat de nœuds réservés pour Amazon Redshift

Présentation

Dans AWS, les frais que vous devez payer 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.

La tarification de nœud à la demande est l'option la plus onéreuse, mais la plus souple 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, un nombre 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](#).

A propos des offres de 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 [A propos des offres de nœuds réservés](#).

Comparaison des offres de nœuds réservés

Option de paiement	Calendrier de paiement	Comparaison des économies	Durée	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.	Durée d'un an ou de trois ans	Aucun	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.	Durée d'un an ou 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.	Durée d'un an ou de trois ans	Oui	Aucun

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 retired 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](#).

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.

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 nœud : 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 de l'ouest des États-Unis (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 de l'ouest des États-Unis (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 de l'ouest des États-Unis (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 de l'ouest des États-Unis (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 de l'ouest des États-Unis (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 de l'ouest des États-Unis (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'une offre de nœuds réservés avec la console Amazon Redshift

Vous utilisez la page Reserved Nodes (Nœuds réservés) de la console Amazon Redshift pour acheter des offres de nœuds réservés et afficher les réservations actuelles et passées.

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 acheter un nœud réservé

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
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.

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.

Mise à niveau des nœuds réservés avec le AWS CLI

Pour mettre à niveau une réservation de nœud réservé avec le AWS CLI

1. Obtenez une liste des ReservedNodeOffering identifiants 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-xxxxxxxxxxxxx
{
  "ReservedNodeOfferings": [
    {
      "Duration": 31536000,
      "ReservedNodeOfferingId": "yyyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyyy",
      "UsagePrice": 0.0,
      "NodeType": "dc2.large",
      "RecurringCharges": [
        {
          "RecurringChargeFrequency": "Hourly",
          "RecurringChargeAmount": 0.2
        }
      ],
      "CurrencyCode": "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 l' `ReservedNodeOfferingId` que 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-xxxxxxxxxxxxx --target-reserved-node-offering-id yyyyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyyy
```



```
{
  "ExchangedReservedNode": {
    "UsagePrice": 0.0,
    "OfferingType": "No Upfront",
    "State": "exchanging",
    "FixedPrice": 0.0,
    "CurrencyCode": "USD",
    "ReservedNodeId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzzz",
    "NodeType": "dc2.large",
    "NodeCount": 1,
    "RecurringCharges": [
      {
        "RecurringChargeFrequency": "Hourly",
        "RecurringChargeAmount": 0.2
      }
    ],
    "ReservedNodeOfferingType": "Regular",
    "StartTime": "2018-06-27T18:02:58Z",
    "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
    "Duration": 31536000
  }
}
```

Vous pouvez confirmer que l'échange est terminé en appelant [describe-reserved-nodes](#) et en vérifiant la valeur de `Node type`.

Achat d'une offre de nœud réservé à l'aide de l'AWS CLI et de l'API Amazon Redshift

Vous pouvez utiliser les opérations de l'AWS CLI pour acheter des offres de nœuds réservés.

- [purchase-reserved-node-offering](#)
- [describe-reserved-node-offerings](#)
- [describe-orderable-cluster-options](#)

Vous pouvez utiliser les opérations d'API Amazon Redshift pour acheter des offres de nœuds réservés.

- [PurchaseReservedNodeOffering](#)
- [DescribeReservedNodeOfferings](#)
- [DescribeOrderableClusterOptions](#)

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.

Sécurité dans Amazon Redshift

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le [modèle de responsabilité partagée](#) décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les 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 conformité AWS](#). 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 service AWS 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 de cluster : la possibilité de créer, de configurer et de supprimer des clusters est contrôlée par les autorisations accordées à l'utilisateur ou au compte IAM associé à vos informations d'identification de sécurité AWS. Les utilisateurs ayant les autorisations appropriées peuvent utiliser la AWS Management Console, AWS Command Line Interface (CLI) ou l'interface de programme d'application (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 plus d'informations, consultez [Identity and Access Management dans Amazon Redshift](#).

- **Connectivité du cluster** : les groupes de sécurité Amazon Redshift spécifient les instances AWS qui sont autorisées à se connecter à un cluster Amazon Redshift au format CIDR (Classless Inter-Domain Routing). 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 du cluster 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 Manuel 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'AWS Identity and Access Management (IAM). Si vous gérez déjà des identités utilisateur en dehors d'AWS, vous pouvez utiliser un fournisseur d'identité (IdP) conforme SAML 2.0 pour gérer l'accès aux ressources Amazon Redshift. À l'aide d'un rôle IAM, vous pouvez configurer votre IdP et AWS de manière à permettre à vos utilisateurs fédérés de générer des informations d'identification temporaires de bases de données et de se connecter aux bases de données Amazon Redshift. Pour plus d'informations, consultez [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 pouvez également apprendre à utiliser d'autres services AWS qui vous aident à contrôler 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 partagée](#) AWS s'applique à la protection des données dans Amazon Redshift. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. 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 en savoir plus sur la confidentialité des données, consultez [Questions fréquentes \(FAQ\) sur la confidentialité des données](#). Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog [Modèle de responsabilité partagée AWS et RGPD \(Règlement général sur la protection des données\)](#) sur le AWSBlog de sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (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.
- Utilisez les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et le journal de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des 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 FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez [Federal Information Processing Standard \(FIPS\) 140-2](#) (Normes de traitement de l'information fédérale).

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 Name (Nom). Ce conseil s'applique notamment lorsque vous utilisez Amazon Redshift ou d'autres Services AWS avec la console, l'API, AWS CLI ou les kits SDK AWS. Toutes les données que vous saisissez 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

Le cryptage côté serveur concerne le chiffrement des données au repos, c'est-à-dire qu'Amazon Redshift chiffre en option vos données lorsqu'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. En option, vous pouvez 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 le cryptage et le décryptage de vos ressources Amazon Redshift, vous utilisez [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. En utilisant 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 de vous permettre de vérifier que l'utilisation des clés est appropriée. Vous pouvez utiliser vos clés AWS KMS en combinaison avec Amazon Redshift et les services AWS pris en charge. Pour obtenir une liste des services qui prennent en charge AWS KMS, consultez [Comment les services AWS utilisent AWS KMS](#) dans le Guide du développeur AWS Key Management Service.

Si vous choisissez de gérer le mot de passe d'administrateur de votre cluster provisionné ou espace de noms sans serveur en utilisant AWS Secrets Manager, Amazon Redshift accepte également une clé AWS KMS supplémentaire qu'AWS Secrets Manager utilise pour chiffrer vos informations d'identification. Cette clé supplémentaire peut être une clé générée automatiquement à partir d'AWS Secrets Manager, ou une clé personnalisée que vous fournissez.

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, vous pouvez activer le chiffrement des bases de données pour vos clusters afin de protéger les données au repos. Lorsque vous activez le chiffrement pour un cluster, les blocs de données et les métadonnées système sont chiffrés pour le cluster et ses instantanés.

Vous pouvez activer le chiffrement lorsque vous lancez votre cluster, ou 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 gérée par le client ou une clé AWS 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. 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 le chiffrement soit un paramètre facultatif dans Amazon Redshift, nous vous recommandons de l'activer pour les clusters qui contiennent 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 PCI DSS (Payment Card Industry Data Security Standard), les lois américaines Sarbanes-Oxley (SOX) et HIPAA (Health Insurance Portability et Accountability Act) et d'autres règlements similaires fournissent des directives permettant de gérer des types de données spécifiques.

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.

Améliorations du processus de chiffrement pour améliorer les performances et la disponibilité

Chiffrement avec des nœuds RA3

Les mises à jour du processus de chiffrement pour les nœuds 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 RA3. Seules les requêtes de lecture peuvent être exécutées.

Notes d'utilisation pour le chiffrement avec des nœuds 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 appliquer à nouveau toutes les nouvelles mises à jour (mises à jour/suppressions/insertions) 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 qu'étant donné qu'une backup-and-restore opération 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 de base de données pour Amazon Redshift à l'aide de AWS KMS](#)
- [Chiffrement pour Amazon Redshift à l'aide de modules de sécurité matérielle](#)
- [Rotation des clés de chiffrement dans Amazon Redshift](#)
- [Modification du chiffrement d'un cluster](#)
- [Configuration du chiffrement de base de données à l'aide de la console](#)
- [Configuration du chiffrement de la base de données à l'aide de l'API Amazon Redshift et l'AWS CLI](#)

Chiffrement de base de données pour Amazon Redshift à l'aide de 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 que votre AWS compte a créés ou dans lesquels vous êtes 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 votre clé par défaut en tant que clé racine. Votre clé par défaut est une clé AWS gérée créée pour que votre AWS compte puisse l'utiliser dans Amazon Redshift. AWS KMS crée cette clé la première fois que vous lancez un cluster chiffré dans une AWS région et que vous choisissiez la clé par défaut.

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 déchiffrée 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, veuillez consulter [Création d'un cluster](#) et [Gestion des clusters à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift](#).

Copier AWS KMS des instantanés chiffrés vers une autre région AWS

AWS KMS les clés sont spécifiques à une AWS région. Si vous activez la copie des instantanés Amazon Redshift vers une autre AWS région et que le cluster source et ses instantanés sont chiffrés à l'aide d'une clé racine provenant de AWS KMS, vous devez configurer une autorisation pour qu'Amazon Redshift utilise une clé racine dans la région de destination. AWS Cette subvention permet à Amazon Redshift de chiffrer les instantanés dans la région de destination. AWS Pour de plus amples informations sur la copie d'instantanés entre régions, veuillez consulter [Copie d'instantanés sur une autre région AWS](#).

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 KMS à l'aide de la console, veuillez consulter [Configuration d'une copie instantanée entre régions pour un cluster AWS KMS 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

Pour plus d'informations sur la configuration des autorisations de copie instantanée pour les AWS KMS clusters chiffrés, consultez [Configuration d'Amazon Redshift pour utiliser les clés de chiffrement AWS KMS à l'aide de l'API Amazon Redshift et AWS CLI](#).

Chiffrement pour Amazon Redshift 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 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 service AWS CloudHSM .

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 doublement chiffré stocké en interne à l'aide de la clé racine interne pour ramener le DEK stocké en interne à l'état chiffré CEK. Le DEK chiffré par CEK est ensuite transmis au HSM pour être déchiffré et renvoyé à Amazon Redshift, où il peut être rechargé 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

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 à l'aide de la console Amazon Redshift](#) et [Rotation des clés de chiffrement à l'aide de l'API Amazon Redshift et de l'AWS CLI](#).

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 gérée ou d'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. Vous pouvez également migrer un cluster non chiffré vers un cluster chiffré en modifiant le cluster.

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 [Copie d'instantanés sur une autre région AWS](#) et [Configuration d'une copie instantanée entre régions pour un cluster AWS KMS chiffré](#). Vous ne pouvez pas activer le chiffrement HSM (module de sécurité matérielle) en modifiant le cluster. À la place, créez un nouveau cluster chiffré avec HSM et migrez vos données vers le nouveau cluster. Pour plus d'informations, consultez [Migration vers un cluster chiffré avec HSM](#).

Pour modifier le chiffrement de base de données sur un cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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.

Pour modifier le chiffrement du cluster à l'aide de l'interface de ligne de commande

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-identifiant <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-identifiant <value> --no-encrypted
```

Migration vers un cluster chiffré avec HSM

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 cluster chiffré par HSM en modifiant le cluster.

Pour migrer d'un cluster non chiffré vers un cluster chiffré avec HSM, vous devez d'abord télécharger 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 faire appel à l'utilitaire de [déchargement/copie Amazon Redshift](#) pour vous aider à effectuer la migration des données entre les deux 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 [AdminViews](#) les 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.

Configuration du chiffrement de base de données à l'aide de la console

Vous pouvez utiliser la console Amazon Redshift pour configurer Amazon Redshift afin d'utiliser un module de sécurité matérielle (HSM) et pour appliquer une rotation aux clés de chiffrement. Pour plus d'informations sur la création de clusters à l'aide de clés de AWS KMS chiffrement, reportez-vous [Création d'un cluster](#) aux sections et [Gestion des clusters à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift](#).

Pour modifier le chiffrement de base de données sur un cluster

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`](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 Modifier pour afficher la page de configuration.
4. Dans la section Configuration de la base de données, choisissez un paramètre pour Chiffrement, puis choisissez Modifier le cluster.

Rotation des clés de chiffrement à l'aide de la console Amazon Redshift

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 AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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).

Configuration du chiffrement de la base de données à l'aide de l'API Amazon Redshift et l'AWS CLI

Utilisez l'API Amazon Redshift et AWS Command Line Interface (AWS CLI) pour configurer les options de clés de chiffrement pour les bases de données Amazon Redshift. Pour plus d'informations sur le chiffrement de la base de données, consultez [Chiffrement de base de données Amazon Redshift](#).

Configuration d'Amazon Redshift pour utiliser les clés de chiffrement AWS KMS à l'aide de l'API Amazon Redshift et AWS CLI

Vous pouvez utiliser les actions suivantes de l'API Amazon Redshift pour configurer Amazon Redshift afin qu'il utilise les clés de chiffrement AWS KMS.

- [CreateCluster](#)
- [CreateSnapshotCopyGrant](#)

- [DescribeSnapshotCopyGrants](#)
- [DeleteSnapshotCopyGrant](#)
- [DisableSnapshotCopy](#)
- [EnableSnapshotCopy](#)

Vous pouvez utiliser les opérations CLI Amazon Redshift suivantes pour configurer Amazon Redshift afin d'utiliser les clés de chiffrement AWS KMS.

- [create-cluster](#)
- [create-snapshot-copy-grant](#)
- [describe-snapshot-copy-grants](#)
- [delete-snapshot-copy-grant](#)
- [disable-snapshot-copy](#)
- [enable-snapshot-copy](#)

Configuration d'Amazon Redshift pour utiliser un HSM à l'aide de l'API Amazon Redshift et AWS CLI

Vous pouvez utiliser des actions d'API Amazon Redshift suivantes pour gérer les modules de sécurité matérielle.

- [CreateHsmClientCertificate](#)
- [CreateHsmConfiguration](#)
- [DeleteHsmClientCertificate](#)
- [DeleteHsmConfiguration](#)
- [DescribeHsmClientCertificates](#)
- [DescribeHsmConfigurations](#)

Vous pouvez utiliser les opérations de l'AWS CLI suivantes pour gérer les modules de sécurité matérielle.

- [create-hsm-client-certificate](#)
- [create-hsm-configuration](#)
- [delete-hsm-client-certificate](#)
- [delete-hsm-configuration](#)

- [describe-hsm-client-certificates](#)
- [describe-hsm-configurations](#)

Rotation des clés de chiffrement à l'aide de l'API Amazon Redshift et de l'AWS CLI

Vous pouvez utiliser les actions d'API Amazon Redshift suivantes pour effectuer une rotation des clés de chiffrement.

- [RotateEncryptionKey](#)

Vous pouvez utiliser les opérations de l'AWS CLI suivantes pour effectuer une rotation des clés de chiffrement.

- [rotate-encryption-key](#)

Chiffrement en transit

Vous pouvez configurer votre environnement pour protéger la confidentialité et l'intégrité des données en transit.

Chiffrement de données en transit entre un cluster Amazon Redshift et des clients SQL sur 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 des certificats émis par AWS Certificate Manager (ACM) sur chaque cluster. Pour plus d'informations, consultez [Transition vers les certificats ACM pour les connexions SSL](#).
- Pour protéger vos données en transit au sein du cloudAWS, Amazon Redshift utilise l'accélération matérielle SSL afin de communiquer avec Amazon S3 ou Amazon DynamoDB pour les opérations de copie (COPY), de déchargement (UNLOAD), de sauvegarde et de restauration.

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) d'Amazon S3 en utilisant la clé par défaut de votre compte gérée par AWS Key Management Service (KMS).
- Chiffrement des 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](#).

Chiffrement et signature de données en transit entre des clients de AWS CLI, de kit SDK ou d'API et des 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 certificat X.509 ou par la clé d'accès secrète AWS du client, conformément au processus de signature de la version 4 (Sigv4). Pour plus d'informations, consultez [Processus de signature Signature Version 4](#) dans le Références générales AWS.
- Utilisez AWS CLI ou un des kits SDK AWS pour formuler des demandes à AWS. Ces outils signent automatiquement les demandes avec la clé d'accès que vous spécifiez lors de leur configuration.

Chiffrement de données en transit entre les clusters Amazon Redshift et l'éditeur de requête Amazon Redshift v2

- Les données sont transmises entre l'éditeur de requête v2 et les clusters Amazon Redshift sur un canal chiffré TLS.

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) à des fins de gestion des clés. AWS KMS utilise le chiffrement d'enveloppe. 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 de clés pour le chiffrement. Cette architecture se compose de clés de

chiffrement des données AES-256 générées de manière aléatoire, d'une clé de base de données, d'une clé de cluster et d'une clé root. Pour plus d'informations, consultez [Comment Amazon Redshift utilise AWS KMS](#).

- Vous pouvez créer votre propre clé gérée par le client dans AWS KMS. Pour plus d'informations, consultez [Création de clés](#).
- Vous pouvez également importer vos propres éléments de clé pour les nouvelles AWS KMS keys. Pour plus d'informations, consultez [Importation d'un article 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 ne prend en charge que AWS CloudHSM Classic pour la gestion des clés. Pour plus d'informations, consultez [Chiffrement pour Amazon Redshift à l'aide de modules de sécurité matérielle](#). Pour plus d'informations sur AWS CloudHSM, consultez [Qu'est-ce que 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 dans Amazon Redshift](#).

Création de jetons de données

La création de jetons (tokenisation) est le processus de remplacement des valeurs réelles par des valeurs opaques à des fins de sécurité des données. Les applications sensibles à la sécurité utilisent la création de jetons 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.

Confidentialité du trafic inter-réseau

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 soit une connexion VPN IPsec sur Internet, soit une connexion physique privée en utilisant la connexion AWS Direct Connect. AWS Direct Connect vous permet d'établir une interface virtuelle privée depuis votre réseau sur site directement vers votre VPC Amazon, vous fournissant ainsi une connexion réseau privée à large bande passante 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 que le Site-to-Site VPN AWS ?](#) et [Qu'est-ce que AWS 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 [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 être autorisées à accéder à AWS des ressources, telles qu'un cluster Amazon Redshift. Les sections suivantes fournissent des détails sur la façon dont vous pouvez utiliser [AWS Identity and Access Management \(IAM\)](#) 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'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la

section [Comment vous connecter à votre compte Compte AWS dans](#) le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d'AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section [Signature des demandes AWS d'API](#) dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez [Authentification multifactorielle](#) dans le Guide de l'utilisateur AWS IAM Identity Center et [Utilisation de l'authentification multifactorielle \(MFA\) dans l'interface AWS](#) dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez [Tâches nécessitant 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 au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez [Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification](#) dans le Guide de l'utilisateur IAM.

Un [groupe IAM](#) est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez [Quand créer un utilisateur IAM \(au lieu d'un rôle\)](#) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un [rôle IAM](#) est une identité au sein de votre Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console [changeant de rôle](#). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez [Utilisation de rôles IAM](#) dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique [Jeux d'autorisations](#) dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme

proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux [ressources entre comptes dans IAM dans le guide de l'utilisateur IAM](#).

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez [Sessions de transmission d'accès](#).
- Rôle de service : il s'agit d'un [rôle IAM](#) attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez [Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2](#) dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez [Quand créer un rôle IAM \(au lieu d'un utilisateur\)](#) dans le Guide de l'utilisateur IAM.

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'autorisation. 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) prennent également en charge l'attachement de 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, consultez [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, ainsi que 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 base de données, votre AWS compte est le propriétaire de la ressource Amazon Redshift.
- Si vous créez un rôle IAM dans votre AWS compte avec les autorisations nécessaires pour 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 accordez l'autorisation de créer des ressources Amazon Redshift à cet utilisateur, celui-ci peut créer des ressources Amazon Redshift. Toutefois, votre AWS compte, auquel appartient l'utilisateur, possède les 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'autorisation.

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).

Politiques basées sur une identité (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 contenant des autorisations permettant de créer, de supprimer, de modifier et de redémarrer des clusters Amazon Redshift pour votre AWS compte.

```
{
  "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.

Politiques basées sur les ressources

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 (voir [Ressources 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
<code>aws:RequestTag</code>	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.
<code>aws:ResourceTag</code>	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.
<code>aws:TagKeys</code>	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 [Présentation du balisage](#).

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'action Amazon Redshift `GetClusterCredentials`.

Clé de condition	Description
<code>redshift:DurationSeconds</code>	Limite le nombre de secondes qui peut être spécifié pour la durée.
<code>redshift:DbName</code>	Limite les noms de base de données qui peuvent être spécifiés.
<code>redshift:DbUser</code>	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 compte AWS spécifique de `us-west-2` la région avec une balise `environment` nommée avec une valeur de balise de `test`

```
{
  "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.

```
{
  "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 du cluster commence par `production` in Région AWS `us-west-2` et Compte AWS `123456789012`.

```
{
  "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. La déclaration spécifie un caractère générique (*) comme `Resource` valeur afin que la politique s'applique à toutes les ressources Amazon Redshift détenues par le AWS compte racine.

- 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 racine dont l'identifiant du cluster commence par `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.

AmazonRedshiftReadOnlyAccès

Accorde un accès en lecture seule à toutes les ressources Amazon Redshift d'un compte. AWS

Vous trouverez la politique [AmazonRedshiftReadOnly'accès](#) sur la console IAM et [AmazonRedshiftReadOnlyAccess](#) dans le Guide de référence des politiques AWS gérées.

AmazonRedshiftFullAccess

Accorde un accès complet à toutes les ressources Amazon Redshift pour un AWS compte. De plus, cette politique accorde un accès complet à toutes les ressources Amazon Redshift sans serveur.

Vous pouvez trouver 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 pouvez trouver la [AmazonRedshiftQueryEditor](#) politique sur la console IAM et [AmazonRedshiftQueryEditor](#) dans le AWS Managed Policy Reference Guide.

AmazonRedshiftDataFullAccès

Accorde un accès complet aux opérations et aux ressources de l'API Amazon Redshift Data pour un AWS compte.

Vous trouverez la politique [AmazonRedshiftDataFulld'accès](#) sur la console IAM et [AmazonRedshiftDataFullAccess](#) dans le Guide de référence des politiques AWS gérées.

AmazonRedshiftQueryEditorV2 FullAccess

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 FullAccess politique [AmazonRedshiftQueryEditorV2](#) sur la console IAM et la [AmazonRedshiftQueryEditorV2 FullAccess](#) dans le AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorV2 NoSharing

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 NoSharing politique [AmazonRedshiftQueryEditorV2](#) sur la console IAM et la [AmazonRedshiftQueryEditorV2 NoSharing](#) dans le AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorV2 ReadSharing

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 ReadSharing politique [AmazonRedshiftQueryEditorV2](#) sur la console IAM et la [AmazonRedshiftQueryEditorV2 ReadSharing](#) dans le AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorReadWritePartage V2

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 politique de [ReadWritepartage AmazonRedshift QueryEditor V2](#) sur la console IAM et le [ReadWritepartage AmazonRedshift QueryEditor V2](#) dans le Guide de référence des politiques AWS gérées.

AmazonRedshiftServiceLinkedRolePolicy

Vous ne pouvez pas vous associer 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 pouvez trouver 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 des autorisations pour exécuter des instructions SELECT pour des services connexes, tels qu'Amazon S3, CloudWatch Logs SageMaker, Amazon ou AWS Glue.

Vous pouvez trouver la [AmazonRedshiftAllCommandsFullAccess](#) politique sur la console IAM et [AmazonRedshiftAllCommandsFullAccess](#) 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.

Amazon Redshift met à jour les politiques gérées AWS

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.

Modification	Description	Date
AmazonRedshiftQueryEditorV2 FullAccess – Mise à jour d'une stratégie existante	Les autorisations pour les actions <code>redshift-serverless:ListNamespaces</code> et <code>redshift-serverless:ListWorkgroups</code> 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
AmazonRedshiftQueryEditorV2 NoSharing – Mise à jour d'une politique existante	Les autorisations pour les actions <code>redshift-serverless:ListNamespaces</code> et <code>redshift-serverless:ListWorkgroups</code> 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
AmazonRedshiftQueryEditorV2 ReadSharing – Mise à jour d'une politique existante	Les autorisations pour les actions <code>redshift-serverless:ListNamespaces</code> et <code>redshift-serverless:ListWorkgroups</code> sont ajoutées à la politique gérée. Leur ajout donne l'autorisation de répertorier les espaces de	21 février 2024

Modification	Description	Date
	noms et les groupes de travail sans serveur dans l'entrepôt de données Amazon Redshift.	
AmazonRedshiftQueryEditorReadWritePartage V2 – Mise à jour d'une politique existante	Les autorisations pour les actions <code>redshift-serverless:ListNamespaces</code> et <code>redshift-serverless:ListWorkgroups</code> 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 <code>redshift:ListRecommendations</code> 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 <code>ec2:AssignIpv6Addresses</code> et <code>ec2:UnassignIpv6Addresses</code> sont ajoutées à la politique gérée. Leur ajout donne l'autorisation d'attribuer des adresses IP ou d'annuler leur attribution.	31 octobre 2023

Modification	Description	Date
AmazonRedshiftQueryEditorV2 NoSharing – Mise à jour d'une politique existante	Les autorisations pour les actions <code>sqlworkbench:GetAutocompletionMetadata</code> et <code>sqlworkbench:GetAutocompletionResource</code> 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
AmazonRedshiftQueryEditorV2 ReadSharing – Mise à jour d'une politique existante	Les autorisations pour les actions <code>sqlworkbench:GetAutocompletionMetadata</code> et <code>sqlworkbench:GetAutocompletionResource</code> 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

Modification	Description	Date
AmazonRedshiftQueryEditorReadWritePartage V2 – Mise à jour d'une politique existante	Les autorisations pour les actions <code>sqlworkbench:GetAutocompletionMetadata</code> et <code>sqlworkbench:GetAutocompletionResource</code> 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

Modification	Description	Date
AmazonRedshiftServiceLinkedRolePolicy – Mise à jour d'une politique existante	<p>Les autorisations relatives aux actions visant AWS Secrets Manager à créer et à gérer des secrets sont ajoutées à la politique gérée. Les autorisations ajoutées sont les suivantes :</p> <ul style="list-style-type: none">• <code>secretsmanager:GetRandomPassword</code>• <code>secretsmanager:DescribeSecret</code>• <code>secretsmanager:PutSecretValue</code>• <code>secretsmanager:UpdateSecret</code>• <code>secretsmanager:UpdateSecretVersionStage</code>• <code>secretsmanager:RotateSecret</code>• <code>secretsmanager>DeleteSecret</code>	14 août 2023

Modification	Description	Date
AmazonRedshiftServiceLinkedRolePolicy – Mise à jour d'une politique existante	<p>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 :</p> <ul style="list-style-type: none">• <code>ec2:AuthorizeSecurityGroupEgress</code>• <code>ec2:AuthorizeSecurityGroupIngress</code>• <code>ec2:UpdateSecurityGroupRuleDescriptionsEgress</code>• <code>ec2:ReplaceRouteTableAssociation</code>• <code>ec2:CreateRouteTable</code>• <code>ec2:AttachInternetGateway</code>• <code>ec2:UpdateSecurityGroupRuleDescriptionsIngress</code>• <code>ec2:AssociateRouteTable</code>• <code>ec2:RevokeSecurityGroupIngress</code>• <code>ec2:CreateRoute</code>	8 mai 2023

Modification	Description	Date
	<ul style="list-style-type: none">• ec2:CreateSecurityGroup• ec2:RevokeSecurityGroupEgress• ec2:ModifyVpcAttribute• ec2:CreateSubnet• ec2:CreateInternetGateway• ec2:CreateVpc <p>Ils étaient associés à la balise Purpose : RedshiftMigrateToVpc resource. 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 ressource, consultez Contrôle de l'accès aux ressources AWS à l'aide de balises.</p>	

Modification	Description	Date
AmazonRedshiftData FullAccès – Mise à jour d'une politique existante	L'autorisation pour l'action <code>redshift:GetClusterCredentialsWithIAM</code> 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 <code>aws:RequestTag/Redshift</code> . Cela permet de limiter l'étendue des autorisations à des ressources Amazon Redshift spécifiques.	6 avril 2023

Modification	Description	Date
AmazonRedshiftQueryEditorV2 NoSharing – Mise à jour d'une politique existante	L'autorisation pour l'action <code>sqlworkbench:GetSchemaInference</code> 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
AmazonRedshiftQueryEditorV2 ReadSharing – Mise à jour d'une politique existante	L'autorisation pour l'action <code>sqlworkbench:GetSchemaInference</code> 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
AmazonRedshiftQueryEditorReadWritePartage V2 – Mise à jour d'une politique existante	L'autorisation pour l'action <code>sqlworkbench:GetSchemaInference</code> 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

Modification	Description	Date
AmazonRedshiftQueryEditorV2 NoSharing – Mise à jour d'une politique existante	L'autorisation pour l'action <code>sqlworkbench:AssociateNotebookWithTab</code> 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
AmazonRedshiftQueryEditorV2 ReadSharing – Mise à jour d'une politique existante	L'autorisation pour l'action <code>sqlworkbench:AssociateNotebookWithTab</code> 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
AmazonRedshiftQueryEditorReadWritePartage V2 – Mise à jour d'une politique existante	L'autorisation pour l'action <code>sqlworkbench:AssociateNotebookWithTab</code> 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

Modification	Description	Date
AmazonRedshiftQueryEditorV2 NoSharing – Mise à jour d'une politique existante	<p>Pour autoriser l'utilisation de blocs-notes, Amazon Redshift a ajouté l'autorisation pour les actions suivantes :</p> <ul style="list-style-type: none"> • <code>sqlworkbench:ListNotebooks</code> • <code>sqlworkbench:CreateNotebook</code> • <code>sqlworkbench:DuplicateNotebook</code> • <code>sqlworkbench:CreateNotebookFromVersion</code> • <code>sqlworkbench:ImportNotebook</code> • <code>sqlworkbench:GetNotebook</code> • <code>sqlworkbench:UpdateNotebook</code> • <code>sqlworkbench>DeleteNotebook</code> • <code>sqlworkbench:CreateNotebookCell</code> • <code>sqlworkbench>DeleteNotebookCell</code> • <code>sqlworkbench:UpdateNotebookCellContent</code> • <code>sqlworkbench:UpdateNotebookCellLayout</code> 	17 octobre 2022

Modification	Description	Date
	<ul style="list-style-type: none">• <code>sqlworkbench:BatchGetNotebookCell</code>• <code>sqlworkbench:ListNotebookVersions</code>• <code>sqlworkbench:CreateNotebookVersion</code>• <code>sqlworkbench:GetNotebookVersion</code>• <code>sqlworkbench>DeleteNotebookVersion</code>• <code>sqlworkbench:RestoreNotebookVersion</code>• <code>sqlworkbench:ExportNotebook</code>	

Modification	Description	Date
AmazonRedshiftQueryEditorV2 ReadSharing – Mise à jour d'une politique existante	<p>Pour autoriser l'utilisation de blocs-notes, Amazon Redshift a ajouté l'autorisation pour les actions suivantes :</p> <ul style="list-style-type: none">• <code>sqlworkbench:ListNotebooks</code>• <code>sqlworkbench:CreateNotebook</code>• <code>sqlworkbench:DuplicateNotebook</code>• <code>sqlworkbench:CreateNotebookFromVersion</code>• <code>sqlworkbench:ImportNotebook</code>• <code>sqlworkbench:GetNotebook</code>• <code>sqlworkbench:UpdateNotebook</code>• <code>sqlworkbench>DeleteNotebook</code>• <code>sqlworkbench:CreateNotebookCell</code>• <code>sqlworkbench>DeleteNotebookCell</code>• <code>sqlworkbench:UpdateNotebookCellContent</code>• <code>sqlworkbench:UpdateNotebookCellLayout</code>	17 octobre 2022

Modification	Description	Date
	<ul style="list-style-type: none">• <code>sqlworkbench:BatchGetNotebookCell</code>• <code>sqlworkbench:ListNotebookVersions</code>• <code>sqlworkbench:CreateNotebookVersion</code>• <code>sqlworkbench:GetNotebookVersion</code>• <code>sqlworkbench>DeleteNotebookVersion</code>• <code>sqlworkbench:RestoreNotebookVersion</code>• <code>sqlworkbench:ExportNotebook</code>	

Modification	Description	Date
<p>AmazonRedshiftQueryEditorReadWritePartage V2 – Mise à jour d'une politique existante</p>	<p>Pour autoriser l'utilisation de blocs-notes, Amazon Redshift a ajouté l'autorisation pour les actions suivantes :</p> <ul style="list-style-type: none"> • <code>sqlworkbench:ListNotebooks</code> • <code>sqlworkbench:CreateNotebook</code> • <code>sqlworkbench:DuplicateNotebook</code> • <code>sqlworkbench:CreateNotebookFromVersion</code> • <code>sqlworkbench:ImportNotebook</code> • <code>sqlworkbench:GetNotebook</code> • <code>sqlworkbench:UpdateNotebook</code> • <code>sqlworkbench>DeleteNotebook</code> • <code>sqlworkbench:CreateNotebookCell</code> • <code>sqlworkbench>DeleteNotebookCell</code> • <code>sqlworkbench:UpdateNotebookCellContent</code> • <code>sqlworkbench:UpdateNotebookCellLayout</code> 	<p>17 octobre 2022</p>

Modification	Description	Date
	<ul style="list-style-type: none"> • <code>sqlworkbench:BatchGetNotebookCell</code> • <code>sqlworkbench:ListNotebookVersions</code> • <code>sqlworkbench:CreateNotebookVersion</code> • <code>sqlworkbench:GetNotebookVersion</code> • <code>sqlworkbench>DeleteNotebookVersion</code> • <code>sqlworkbench:RestoreNotebookVersion</code> • <code>sqlworkbench:ExportNotebook</code> 	
AmazonRedshiftServiceLinkedRolePolicy – Mise à jour d'une politique existante	Amazon Redshift a ajouté l'espace de noms AWS/Redshift pour autoriser la publication de métriques sur CloudWatch	29 septembre 2022
AmazonRedshiftQueryEditorV2 NoSharing – Mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation aux actions <code>sqlworkbench:ListQueryExecutionHistory</code> et <code>sqlworkbench:GetQueryExecutionHistory</code> . Cela permet de consulter l'historique des requêtes.	30 août 2022

Modification	Description	Date
AmazonRedshiftQueryEditorV2 ReadSharing – Mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation aux actions <code>sqlworkbench:ListQueryExecutionHistory</code> et <code>sqlworkbench:GetQueryExecutionHistory</code> . Cela permet de consulter l'historique des requêtes.	30 août 2022
AmazonRedshiftQueryEditorReadWritePartage V2 – Mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation aux actions <code>sqlworkbench:ListQueryExecutionHistory</code> et <code>sqlworkbench:GetQueryExecutionHistory</code> . 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 gérée existante <code>AmazonRedshiftFullAccess</code> .	22 juillet 2022

Modification	Description	Date
AmazonRedshiftDataFullAccès – Mise à jour d'une politique existante	Amazon Redshift a mis à jour la condition de portée par défaut <code>redshift-serverless:GetCredentials</code> de l'autorisation de la balise <code>aws:ResourceTag/RedshiftDataFullAccess</code> passant de <code>StringEquals</code> à <code>StringLike</code> pour accorder l'accès aux ressources marquées avec une clé de balise <code>RedshiftDataFullAccess</code> et n'importe quelle valeur de balise.	11 juillet 2022
AmazonRedshiftDataFullAccès – Mise à jour d'une politique existante	Amazon Redshift a ajouté de nouvelles autorisations pour permettre à <code>redshift-serverless:GetCredentials</code> 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 <code>sqlworkbench:GetAccountSettings</code> . Ceci accorde l'autorisation d'obtenir les paramètres de compte.	15 juin 2022

Modification	Description	Date
AmazonRedshiftQueryEditorV2 ReadSharing – Mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation à l'action <code>sqlworkbench:GetAccountSettings</code> . Ceci accorde l'autorisation d'obtenir les paramètres de compte.	15 juin 2022
AmazonRedshiftQueryEditorReadWritePartage V2 – Mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation à l'action <code>sqlworkbench:GetAccountSettings</code> . 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

Modification	Description	Date
AmazonRedshiftQueryEditorV2 FullAccess – Mise à jour d'une politique existante	Autorisations pour l'action <code>sqlworkbench:ListTaggedResources</code> . 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 <code>tag:GetResources</code> uniquement via l'éditeur de requête v2.	22 février 2022
AmazonRedshiftQueryEditorV2 NoSharing – Mise à jour d'une politique existante	Autorisations pour l'action <code>sqlworkbench:ListTaggedResources</code> . 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 <code>tag:GetResources</code> uniquement via l'éditeur de requête v2.	22 février 2022
AmazonRedshiftQueryEditorV2 ReadSharing – Mise à jour d'une politique existante	Autorisations pour l'action <code>sqlworkbench:ListTaggedResources</code> . 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 <code>tag:GetResources</code> uniquement via l'éditeur de requête v2.	22 février 2022

Modification	Description	Date
AmazonRedshiftQueryEditorReadWritePartage V2 – Mise à jour d'une politique existante	Autorisations pour l'action <code>sqlworkbench:ListTaggedResources</code> . 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 <code>tag:GetResources</code> uniquement via l'éditeur de requête v2.	22 février 2022
AmazonRedshiftQueryEditorV2 ReadSharing – Mise à jour d'une politique existante	L'autorisation pour l'action <code>sqlworkbench:AssociateQueryWithTab</code> 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

Modification	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 les nouvelles actions afin de permettre la gestion des groupes de journaux et des flux de journaux Amazon CloudWatch 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

Modification	Description	Date
AmazonRedshiftQueryEditorV2 FullAccess – Nouvelle politique	Amazon Redshift a ajouté une nouvelle politique permettant un accès complet à l'éditeur de requête Amazon Redshift v2.	24 septembre 2021
AmazonRedshiftQueryEditorV2 NoSharing – 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
AmazonRedshiftQueryEditorV2 ReadSharing – 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
AmazonRedshiftQueryEditorReadWritePartage V2 – 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
AmazonRedshiftDataFullAccès – Mise à jour d'une politique existante	Amazon Redshift a ajouté de nouvelles autorisations pour autoriser Authorize DataShare .	12 août 2021

Modification	Description	Date
AmazonRedshiftData FullAccès – 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

Autorisations requises pour utiliser Redshift Spectrum

Amazon Redshift Spectrum a besoin d'autorisations pour accéder aux AWS ressources à d'autres services. 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 minimal d'autorisations lui permettant de décrire les ressources Amazon Redshift associées à son compte. Ces autorisations doivent également permettre à l'utilisateur de décrire d'autres informations connexes, notamment les informations relatives à la sécurité Amazon EC2 CloudWatch, Amazon, Amazon SNS et au 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 politiques `AmazonRedshiftReadOnlyAccess` AWS gérées `AmazonRedshiftQueryEditor` et les politiques. La politique `AmazonRedshiftQueryEditor` accorde l'autorisation à l'utilisateur de récupérer les résultats de ses propres instructions SQL uniquement. Il s'agit des déclarations soumises par celui-ci, `aws:user-id` comme indiqué dans cette section de la politique `AmazonRedshiftQueryEditor` AWS gérée.

```
{
  "Sid": "DataAPIIAMSessionPermissionsRestriction",
  "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:user-id}"
    }
  }
}
```

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 minimum d'autorisations pour accéder à Amazon Redshift, aux opérations de l'éditeur de requêtes v2 et à AWS d'autres services AWS Key Management Service tels que 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 des conditions permettant de 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 acteurs Compte AWS ayant la même valeur de balise (par exemple, `accounting-team`) font partie de la même équipe dans l'éditeur de requêtes 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 modifiée 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 la balise **accounting-team** pour un rôle IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation de la console, choisissez Rôles (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.

```
{
  "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.

```
{
```

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

Pour connaître les étapes de création d'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**) afin de permettre au planificateur d'assumer les autorisations en votre nom. Vous associez également une politique (autorisations) au rôle pour les opérations d'API Amazon Redshift Data que vous souhaitez planifier, ainsi qu'une politique pour les opérations Amazon EventBridge .

Vous utilisez le EventBridge planificateur lorsque vous créez des requêtes planifiées avec 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.

```
{
  "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 connaître les étapes de création d'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 Events.
- 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, 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 le SageMaker pilote automatique avec les explications du modèle fournies par Amazon Redshift.

```
{
  "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.

```

{
  "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",
            ]
        }
    }
}

```



```
]
}
```

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 êtes autorisé à appeler des opérations SageMaker d'API. 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.

```
{
```

```

"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](#) dans le manuel Amazon SageMaker Developer Guide.

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.

```

{
  "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": "*"
}
]
```

Pour plus d'informations sur Amazon Redshift ML, consultez [Utilisation du machine learning dans Amazon Redshift](#) ou [CREATE 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 unités 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 en matière de 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 par programmation l'action `GetClusterCredentials`, vous devez disposer d'un ensemble minimal d'autorisations. Au minimum, vous avez besoin de l'autorisation d'appeler l'action `redshift:GetClusterCredentials` 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.

GetClusterCredentials paramètre	Action	Ressource
Autocreate	redshift:CreateClusterUser	dbuser

GetClusterCredentials paramètre	Action	Ressource
DbGroups	redshift:JoinGroups	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

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, AWS les 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.

```
{
```



```

"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`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUSWest2Region",
      "Action": [
        "redshift:*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:redshift:us-west-2:*"
    },
    {
      "Sid": "DenyDeleteUSWest2Region",
      "Action": [
        "redshift>Delete*"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:redshift:us-west-2:*"
    }
  ]
}

```

}

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`.

```
{
  "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`.

```
{
  "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`.

```
{
  "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`.

```

{
  "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 : Accorder à un utilisateur l'accès à Amazon Redshift, ainsi qu'à des actions et ressources communes pour les services AWS connexes

L'exemple de politique suivant autorise l'accès 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

Les autorisations au niveau des ressources ne sont pas prises en charge pour les actions Amazon EC2 qui sont spécifiées dans cet exemple de politique.

```

{
  "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 AWS Resource Groups. 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 [Étiquetage des ressources Amazon Redshift](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Tagging permissions",
      "Effect": "Allow",
      "Action": [
        "redshift:DeleteTags",
        "redshift:CreateTags",
        "redshift:DescribeTags",
        "tag:UntagResources",
        "tag:TagResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemple de politique d'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 `"AIDIO4R4TAW7CSEXAMPLE:${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"`.

```
{
  "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"
    ]
}
]

```


}

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.

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 : : < GroupName sur Azure <Namespace>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.

Fonctionnement de la connexion avec la fédération de fournisseurs d'identités 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.

Utilisation d'outils client de bureau pour se connecter à Amazon Redshift

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). Il décrit une step-by-step implémentation de la configuration IdP native d'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 apprendre comment intégrer la fédération IdP native d'Amazon Redshift avec Azure AD, à l'aide de Power BI Desktop et de JDBC Client-SQL Workbench/J, regardez la vidéo suivante :

Pour obtenir des instructions sur l'utilisation de la fédération de fournisseurs d'identités natifs pour se connecter à Amazon Redshift avec un client SQL, en particulier DBeaver ou SQL Workbench/J, consultez le billet de blog [Integrate Amazon Redshift native IdP federation with Microsoft Azure AD using a SQL client](#) (Intégrer la fédération d'identités natives Amazon Redshift à Microsoft Azure AD à l'aide d'un client SQL).

Connexion de Redshift à IAM Identity Center pour offrir aux utilisateurs 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. Cela fonctionne grâce à une connexion entre Redshift et AWS IAM Identity Center, qui offre à vos utilisateurs une expérience d'authentification unique. Vous pouvez ainsi introduire des utilisateurs et des groupes depuis votre annuaire et leur attribuer des autorisations directement. Par la suite, cette connexion permet de lier des outils et services supplémentaires. Pour illustrer un end-to-end cas, vous pouvez utiliser un Amazon QuickSight 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 IAM Identity Center. Redshift peut déterminer l'identité d'un utilisateur et son appartenance aux groupes. IAM Identity Center permet également de connecter et de gérer les identités par le biais d'un fournisseur d'identité tiers (IdP) tel qu'Okta ou PingOne

Une fois que votre administrateur a configuré la connexion entre Redshift et 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.

Les avantages de l'intégration de Redshift à AWS IAM Identity Center

L'utilisation d'IAM Identity Center avec Redshift peut profiter à votre organisation des manières suivantes :

- Les auteurs de tableaux de bord Amazon QuickSight peuvent se connecter aux sources de données Redshift sans avoir à saisir à nouveau les mots de passe ou à demander à un administrateur de configurer des rôles IAM avec des autorisations complexes.
- IAM Identity Center fournit un emplacement central pour les utilisateurs de votre personnel dans AWS. Vous pouvez créer des utilisateurs et des groupes directement dans IAM Identity Center ou connecter des utilisateurs et des groupes existants que vous gérez dans un fournisseur d'identité normalisé tel qu'Okta PingOne ou Microsoft Entra ID (Azure AD). IAM Identity Center dirige l'authentification vers la source de vérité que vous avez choisie pour les utilisateurs et les groupes, et il gère un annuaire des utilisateurs et des groupes auquel 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 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 IAM Identity Center pour chacun d'entre eux, et cela garantit que tous les clusters et groupes de travail disposent d'une vue cohérente des utilisateurs, de leurs attributs et des groupes. Notez que l'instance IAM Identity Center de votre organisation doit se trouver dans la même région que toutes les unités de partage des données Redshift auxquelles 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.

Configuration de l'intégration d'IAM Identity Center à Amazon Redshift

Votre administrateur de cluster Amazon Redshift ou administrateur Amazon Redshift sans serveur doit effectuer plusieurs étapes pour configurer Redshift en tant qu'application compatible avec IAM Identity Center. Redshift peut ainsi découvrir et se connecter automatiquement à IAM Identity Center pour recevoir les services de connexion et d'annuaire d'utilisateurs. Après cela, lorsque votre administrateur Redshift crée un cluster ou un groupe de travail, il peut permettre au nouvel entrepôt des données d'utiliser IAM Identity Center pour gérer l'accès aux bases de données.

L'objectif de l'activation de Redshift en tant qu'application gérée par IAM Identity Center est de vous permettre de contrôler les autorisations des utilisateurs et des groupes depuis IAM Identity Center ou depuis un fournisseur d'identité tiers qui y est intégré. Lorsque des utilisateurs de base de données se connectent à une base de données Redshift, par exemple un analyste ou un scientifique des données, leurs groupes sont vérifiés dans IAM Identity Center et mis en correspondance avec les

noms de rôles 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.

Prérequis

Voici les conditions préalables à l'intégration d'IAM Identity Center à Amazon Redshift :

- Configuration du compte : vous devez configurer IAM Identity Center dans le compte de gestion de votre AWS organisation si vous prévoyez d'avoir des cas d'utilisation entre comptes ou si vous utilisez des clusters Redshift dans différents comptes avec la même instance d'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 d'avoir créé des utilisateurs ou des groupes dans IAM Identity Center, ou d'avoir synchronisé des utilisateurs et des groupes à partir de votre source d'identité avant de pouvoir les attribuer à des données dans Redshift.

Note

Vous avez la possibilité d'utiliser une instance de compte d'IAM Identity Center, à condition que Redshift et IAM Identity Center soient dans le 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 chargé de configurer l'intégration d'IAM Identity Center puisse sélectionner l'émetteur de jetons approuvé et ajouter les attributs nécessaires pour terminer la configuration. Cela peut inclure la configuration d'un fournisseur d'identité externe pour qu'il serve d'émetteur de jetons approuvé et l'ajout de ses attributs dans la console IAM Identity Center. Pour effectuer ces étapes, consultez la section [Utilisation d'applications avec un émetteur de jetons fiable](#).

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.

Pour plus d'informations, consultez [Bien démarrer avec IAM Identity Center](#).

Configuration de votre fournisseur d'identité pour qu'il fonctionne avec IAM Identity Center

La première étape du contrôle de la gestion des identités des utilisateurs et des groupes consiste à vous connecter à IAM Identity Center et à configurer votre fournisseur d'identité. Vous pouvez utiliser IAM Identity Center lui-même comme fournisseur d'identité ou vous pouvez connecter un magasin d'identité tiers, tel 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 IAM Identity Center. À la fin de ce processus, assurez-vous qu'un petit ensemble d'utilisateurs et de groupes a été ajouté à IAM Identity Center, à des fins de test.

Autorisations administratives

Autorisations requises pour la gestion du cycle de vie des applications RedShift/IAM Identity Center

Vous devez créer une identité IAM, qu'un administrateur Redshift utilise pour configurer Redshift afin de l'utiliser avec 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/IAM Identity Center

- `sso:PutApplicationAssignmentConfiguration` : pour la sécurité.
- `sso:CreateApplication` : sert à créer une application 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 IAM Identity Center. Cela inclut les [subventions d'accès pour AWS Lake Formation et pour Amazon S3](#).
- `redshift:CreateRedshiftIdcApplication` : sert à créer l'application Redshift IDC.

Décrire l'application RedShift/IAM Identity Center

- `sso:GetApplicationGrant` : sert à répertorier les informations relatives à l'émetteur de jetons approuvé.
- `sso:ListApplicationAccessScopes`— Pour configurer l'application Redshift IAM Identity Center afin de répertorier les intégrations en aval, telles que for AWS Lake Formation et S3 Access Grants.
- `redshift:DescribeRedshiftIdcApplications`— Utilisé pour décrire les applications IAM Identity Center existantes.

Modification de l'application RedShift/IAM Identity Center

- `redshift:ModifyRedshiftIdcApplication` : sert à modifier une application Redshift existante.
- `sso:UpdateApplication` : sert à mettre à jour une application IAM Identity Center.
- `sso:GetApplicationGrant`— Récupère les informations sur l'émetteur du jeton de confiance.
- `sso:ListApplicationAccessScopes` : pour la configuration de l'application Redshift 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 IAM Identity Center. Cela inclut les [subventions d'accès pour AWS Lake Formation et pour Amazon S3](#).
- `sso>DeleteApplicationAccessScope`— Pour supprimer la configuration de l'application Redshift IAM Identity Center. Cela inclut les [subventions d'accès pour AWS Lake Formation et pour Amazon S3](#).

Suppression de l'application RedShift/IAM Identity Center

- `sso>DeleteApplication` : sert à supprimer une application IAM Identity Center.
- `redshift>DeleteRedshiftIdcApplication` : permet de supprimer une application Redshift IDC existante.

Autorisations requises pour la gestion du cycle de vie des applications RedShift/Query Editor v2

Vous devez créer une identité IAM, qu'un administrateur Redshift utilise pour configurer Redshift afin de l'utiliser avec 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 Query Editor v2

- `redshift:CreateQev2IdcApplication`— Utilisé pour créer l'application QEV2.
- `sso:CreateApplication`— Permet de créer une application 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 IAM Identity Center. Cela inclut l'éditeur de requêtes v2.
- `sso:PutApplicationAssignmentConfiguration` : pour la sécurité.

Décrire l'application de l'éditeur de requêtes v2

- `redshift:DescribeQev2IdcApplications`— Utilisé pour décrire l'application IAM Identity Center QEV2.

Modifier l'application de l'éditeur de requêtes v2

- `redshift:ModifyQev2IdcApplication`— Utilisé pour modifier l'application IAM Identity Center QEV2.
- `sso:UpdateApplication`— Utilisé pour modifier l'application IAM Identity Center QEV2.

Supprimer l'application de l'éditeur de requêtes v2

- `redshift>DeleteQev2IdcApplication`— Utilisé pour supprimer l'application QEV2.
- `sso>DeleteApplication`— Utilisé pour supprimer l'application QEV2.

Note

Dans le SDK Amazon Redshift, les API suivantes ne sont pas disponibles :

- CreateQev2 IdcApplication
- DescribeQev2 IdcApplications
- ModifyQev2 IdcApplication
- DeleteQev2 IdcApplication

Ces actions sont spécifiques à l'intégration d'IAM Identity Center à Redshift QEV2 dans la console. AWS Pour plus d'informations, consultez la section [Actions définies par Amazon Redshift](#).

Autorisations requises pour que l'administrateur de base de données puisse connecter 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 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 qu'application AWS gérée avec IAM Identity Center

Avant qu'IAM Identity Center puisse gérer les identités pour un cluster provisionné par Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur, l'administrateur Redshift doit suivre les étapes nécessaires pour faire de Redshift une application gérée par IAM Identity Center :

1. Sélectionnez Intégration à IAM Identity Center dans le menu de la console Amazon Redshift ou Amazon Redshift sans serveur, puis sélectionnez Se connecter à IAM Identity Center. À partir de là, vous devez effectuer une série de sélections pour renseigner les propriétés nécessaires à l'intégration d'IAM Identity Center.
2. Choisissez un nom d'affichage et un nom unique pour l'application gérée par IDC 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 utilisateurs et rôles gérés par IDC 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 [Fonctionnement de la propagation d'identité approuvée](#). Reportez-vous également à la documentation bêta d'IAM Identity Center, qui accompagne cette documentation.

Une fois que l'administrateur Redshift a terminé les étapes et enregistré la configuration, les propriétés d'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 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'IAM Identity Center peut être activée sur chaque nouveau cluster.

Après la configuration, vous pouvez inclure les utilisateurs et les groupes d'IAM Identity Center dans Redshift en choisissant l'onglet Utilisateurs ou Groupes, puis en choisissant Attribuer.

Activation de l'intégration d'IAM Identity Center pour un nouveau cluster Amazon Redshift ou groupe de travail Amazon Redshift sans serveur

Votre administrateur de base de données configure les nouvelles ressources Redshift pour qu'elles fonctionnent en harmonie avec 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 dotée d'autorisations pour créer des ressources Redshift peut effectuer ces tâches d'intégration d'IAM Identity Center. Lorsque vous créez un cluster provisionné, vous commencez par choisir Créer un cluster dans la console Amazon Redshift. La procédure suivante montre comment activer la gestion d'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 d'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 IAM Identity Center et Redshift.
- Nom du rôle : ce rôle de base de données Redshift doit correspondre au nom du groupe dans IAM Identity Center.

Redshift se connecte à IAM Identity Center et récupère les informations nécessaires pour créer et mapper le rôle de base de données au groupe IAM Identity Center.

Notez que lorsqu'un nouvel entrepôt des données est créé, le rôle IAM spécifié pour l'intégration IDC est automatiquement associé au cluster provisionné ou au groupe de travail Amazon Redshift sans serveur. Après avoir saisi les métadonnées de cluster requises et créé la ressource, vous pouvez vérifier le statut de l'intégration d'IAM Identity Center dans les propriétés. Si les noms de vos groupes dans IAM Identity Center comportent des espaces, vous devez utiliser des guillemets dans le code 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 QuickSight. 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 renseignez un élément `RedshiftIdcApplication`, qui représente l'application Redshift dans IAM Identity Center.

1. Pour commencer, vous pouvez créer des utilisateurs et les ajouter à des groupes dans IAM Identity Center. Vous pouvez le faire dans la AWS console d'IAM Identity Center (IDC).
2. Appelez `create-redshift-idc-application` pour créer une application IDC 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 IDC. L'ARN du

rôle IAM est un ARN doté d'autorisations pour accéder à 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 utiliser `create-application-assignment` pour attribuer des groupes particuliers ou des utilisateurs individuels à l'application gérée dans IAM Identity Center. Ce faisant, vous pouvez spécifier les groupes à gérer via IAM Identity Center. Si l'administrateur de base de données crée des rôles de base de données dans Redshift, les noms des groupes dans IAM Identity Center correspondent aux noms des rôles dans Redshift. Les rôles contrôlent les autorisations dans la base de données. Pour plus d'informations, consultez [Attribution d'un accès utilisateur aux applications dans la console IAM Identity Center](#).

- Après avoir activé l'application, appelez `create-cluster` et incluez l'ARN de l'application gérée par Redshift depuis IAM Identity Center. Cela permet d'associer le cluster à l'application gérée dans IAM Identity Center.

Association d'une application IAM Identity Center à un cluster ou à un groupe de travail existant

Si vous avez un cluster ou un groupe de travail existant que vous souhaitez activer pour l'intégration d'IAM Identity Center, vous pouvez le faire en exécutant une commande SQL. Exécutez la commande suivante pour activer l'intégration. Il est nécessaire qu'un administrateur de base de données exécute cette requête et que la connexion entre Redshift et IAM Identity Center soit déjà configurée. Lorsque vous définissez `ENABLE`, cela permet à IAM Identity Center de fournir une gestion des identités pour le cluster ou le groupe de travail.

```
ALTER IDENTITY PROVIDER
<idp_name> | NAMESPACE <namespace> | IAM_ROLE default | 'arn:aws:iam::<AWS account-
id-1>:role/<role-name>' | [DISABLE | ENABLE]
```

Vous pouvez 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 d'accès à différentes ressources, en fonction des attributs d'identité des utilisateurs et de leur appartenance aux groupes, au sein de leur fournisseur d'identité ou directement au sein d'IAM Identity Center. Par exemple, l'administrateur de 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.

Personas d'administrateur pour la connexion des applications

Les personas suivants sont essentiels pour connecter les applications analytiques à l'application gérée par 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 dans IAM Identity Center peuvent correspondre à des autorisations spécifiques.

Connexion à Amazon Redshift avec IAM Identity Center via Amazon QuickSight

Voici comment utiliser Amazon pour s'authentifier QuickSight auprès de Redshift lorsqu'il est connecté à IAM Identity Center et que l'accès est géré via celui-ci : [Autoriser les connexions entre QuickSight Amazon et les clusters Amazon Redshift](#). Ces étapes s'appliquent également à Amazon Redshift sans serveur.

Connexion à Amazon Redshift avec IAM Identity Center via l'éditeur de requêtes Amazon Redshift v2

Après avoir terminé la procédure de configuration d'une connexion IAM Identity Center avec Redshift, l'utilisateur peut accéder à la base de données et aux objets appropriés figurant dans la base de données via son identité basée sur IAM Identity Center et préfixée par l'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 [Utilisation de l'éditeur de requêtes v2](#).

Interrogation de 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 d'identité vers Lake Formation via 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 IAM Identity Center. Cette section explique comment configurer deux cas d'utilisation, l'interrogation depuis un lac de données et l'interrogation depuis un partage de données, qui montrent comment tirer parti d'IAM Identity Center avec Redshift pour se connecter aux ressources gouvernées par Lake Formation.

Utilisation d'une connexion IAM Identity Center et Redshift pour interroger un lac de données

Ces étapes couvrent un cas d'utilisation dans lequel vous utilisez IAM Identity Center connecté à Redshift pour interroger un lac de données régi par Lake Formation.

Prérequis

Cette procédure exige plusieurs étapes préalables :

1. IAM Identity Center doit être configuré pour prendre en charge l'authentification et la gestion des identités avec Redshift. Vous pouvez activer IAM Identity Center depuis la console et sélectionner une source de fournisseur d'identité (IdP). Synchronisez ensuite un ensemble de vos utilisateurs IdP avec IAM Identity Center. Vous devez également configurer une connexion entre 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 IAM Identity Center dans la procédure de configuration.
3. Créez une application IAM Identity Center gérée pour Lake Formation et configurez-la. Cela fait suite à la configuration de la connexion entre IAM Identity Center et Redshift. La procédure est la suivante :
 - a. Dans AWS CLI, utilisez la commande `modify-redshift-idc-application` pour activer l'intégration du service Lake Formation à l'application gérée par 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 IAM Identity Center pour Lake Formation, qui est visible sur le portail 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 d'ARN de l'instance IAM Identity Center.

Une fois que l'administrateur a terminé la configuration prérequis, 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 que la spécification d'un rôle IAM n'est pas requise dans ce cas, car l'accès est géré via IAM Identity Center.

2. L'administrateur accorde des autorisations : l'administrateur accorde l'autorisation d'utilisation à un groupe 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 "MYC0:sales";
```

Par la suite, l'administrateur accorde à Lake Formation des autorisations sur les objets, en fonction des exigences de l'organisation, à l'aide de la AWS CLI :

```
aws lakeformation grant-permissions ...
```

3. Les utilisateurs exécutent des requêtes : à ce stade, un utilisateur 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;
```

Utilisation d'une connexion IAM Identity Center et Redshift pour se connecter à une unité de partage des données

Vous pouvez accéder à une unité de partage des données depuis un autre entrepôt des données Redshift lorsque l'accès est géré via 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 que vous avez établi une connexion entre Redshift et 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 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'autorisation d'utilisation à un groupe IAM Identity Center. Cela accorde des autorisations sur les ressources Redshift :

```
GRANT USAGE ON DATABASE "my_external_db" to "MYC0:sales";
```

L'administrateur accorde également à Lake Formation des autorisations sur les objets, à l'aide de la AWS CLI :

```
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 par le biais de la connexion IAM Identity Center. Si vous avez déjà configuré l'intégration de Redshift à IAM Identity Center, utilisez les propriétés détaillées dans cette section pour configurer une connexion.

Plug-in d'authentification pour la connexion à Redshift à l'aide d'IAM Identity Center

`IdpTokenAuthPlugin` fournit des propriétés de connexion et facilite l'authentification avec IAM Identity Center. Il accepte un jeton Web JSON (JWT) OpenID Connect (OIDC) provenant de n'importe quel fournisseur d'identité Web connecté à IAM Identity Center.

Si vous utilisez un pilote Amazon Redshift, vous pouvez l'utiliser `IdpTokenAuthPlugin` pour vous authentifier auprès de Redshift avec IAM Identity Center. Ce plugin accepte un JWT OIDC de tout fournisseur d'identité Web connecté à IAM Identity Center. Le tableau suivant détaille les options de connexion à utiliser pour une authentification réussie.

Pilote	Clé d'option de connexion	Valeur	Remarques
JDBC	<code>plugin_name</code>	<code>com.amazon.redshift.plugin.IdpTokenAuthPlugin</code>	Vous devez saisir le nom de classe complet du plugin lorsque vous vous connectez.
ODBC	<code>plugin_name</code>	<code>IdpTokenAuthPlugin</code>	
Python	<code>credentials_provider</code>	<code>IdpTokenAuthPlugin</code>	Aucune <code>plugin_name</code> option n'est disponible pour le pilote Python. Utilisez à la place <code>credentials_provider</code> .

Le plugin dispose des options de connexion supplémentaires suivantes :

- `jeton` — Un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web connecté à IAM Identity Center. Votre application doit générer ce jeton en authentifiant l'utilisateur de votre application auprès d'un fournisseur d'identité connecté à IAM Identity Center.
- `token_type` — Le type de jeton utilisé pour. `IdpTokenAuthPlugin` Vous pouvez spécifier des valeurs pour l'option suivante :
 - `EXT_JWT` — Fournissez-le si vous utilisez un jeton Web (JWT) OpenID Connect (OIDC) JSON fourni par un fournisseur d'identité Web connecté à IAM Identity Center.

Vous devez entrer ces valeurs dans les propriétés de connexion de l'outil que vous créez et avec lequel vous vous connectez. Pour plus d'informations, consultez la documentation des options de connexion pour chaque pilote respectif :

- [Options de configuration du pilote JDBC version 2.1](#)
- [Configuration des options du pilote ODBC](#)
- [Options de configuration pour le connecteur Amazon Redshift Python](#)

Résolution des problèmes de connexion depuis l'éditeur de requêtes Amazon Redshift v2

Cette liste détaille les erreurs les plus fréquentes et peut vous aider à vous connecter à votre base de données Redshift avec l'éditeur de requêtes v2, en utilisant une identité IAM Identity Center.

- Erreur : problème de connexion : aucune information de session du centre d'identité n'est disponible. — 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 l'éditeur de requêtes Amazon Redshift 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 vous ne voyiez pas l'icône en forme d'œil dans la barre d'adresse.
 - Safari — Sur un Mac, ouvrez l'application Safari. Choisissez Réglages, puis Options avancées. Activez pour désactiver : bloquez 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 le message d'erreur Problème de connexion persiste : aucune information de session du centre d'identité n'est disponible, nous vous recommandons d'actualiser votre connexion avec IAM Identity Center. Pour ce faire, cliquez avec le bouton droit sur votre instance de base de données Redshift et choisissez Refresh. Une nouvelle fenêtre apparaît, dans laquelle vous pouvez vous authentifier.

- Erreur : problème de connexion : la session Identity Center a expiré ou n'est pas valide. — Suite à l'intégration d'un cluster provisionné par Redshift ou d'un groupe de travail sans serveur à 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 Refresh. Une nouvelle fenêtre apparaît, dans laquelle vous pouvez vous authentifier.

- Erreur : étendue non valide. Les informations d'identification de l'utilisateur ne sont pas autorisées à se connecter à Redshift. — Suite à l'intégration d'un cluster provisionné par Redshift ou d'un groupe de travail sans serveur à 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 à partir de l'éditeur de requêtes v2. Dans ce cas, pour que l'éditeur de requêtes v2 puisse correctement connecter et authentifier un utilisateur via IAM Identity Center afin d'accéder aux ressources appropriées, un administrateur doit affecter l'utilisateur à l'application Redshift 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 est la limite de mise en cache de session IAM Identity Center.
- Erreur : les bases de données n'ont pas pu être répertoriées. FATAL : échec de la requête lorsque le cluster est mis en pause automatiquement. — Lorsqu'une base de données Amazon Redshift Serverless est inactive et ne traite aucune charge de travail, elle peut rester suspendue lorsque vous vous connectez à une identité IAM Identity Center. Pour y remédier, connectez-vous à l'aide d'une autre méthode d'authentification afin de reprendre le groupe de travail Serverless. Connectez-vous ensuite à la base de données avec votre identité IAM Identity Center.
- Erreur : une erreur s'est produite lors de la tentative de fédération avec IAM Identity Center. Un administrateur Amazon Redshift doit supprimer et recréer l'application IAM Identity Center QEV2 à l'aide de la console Redshift. — Cette erreur se produit généralement lorsque l'instance d'application 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 IAM Identity Center. Cela peut être effectué sur la console Redshift ou à l'aide de la commande <https://docs.aws.amazon.com/cli/latest/reference/redshift/delete-redshift-idc-application.html> CLI.

Limites

Les limitations suivantes s'appliquent :

- Utilisation d'IAM Identity Center avec des pilotes Redshift : lorsque vous utilisez `IdpTokenAuthPlugin` le, disponible via les pilotes Redshift actuels, il est nécessaire que

l'application cliente génère le jeton d'authentification. Notez toutefois qu' AWS IAM Identity Center ne prend actuellement pas en charge la génération d'un jeton d'accès pour Redshift. L'utilisation d'un jeton d'accès IAM Identity Center n'est donc pas prise en charge. Il est actuellement possible de l'utiliser `IdpTokenAuthPlugin` pour se connecter à une base de données Amazon Redshift via un fournisseur d'identité Web externe, tel qu'Okta, PingOne ou Microsoft Entra ID (Azure AD), intégré à IAM Identity Center. Dans ce cas, le client est chargé de générer un jeton Web JSON (JWT) OpenID Connect (OIDC) à partir du fournisseur d'identité Web et de le fournir en tant qu'entrée au pilote. `IdpTokenAuthPlugin` Le plugin est décrit dans la section précédente. Vous pouvez également vous connecter à l'aide de l'éditeur de requêtes v2 si vous souhaitez utiliser directement l'autorisation et l'authentification IAM Identity Center.

- Aucune prise en charge du VPC amélioré : le VPC amélioré n'est pas pris en charge lorsque vous configurez la propagation d'identité sécurisée Redshift avec IAM Identity Center. Pour plus d'informations sur le VPC amélioré, consultez la section Routage [VPC amélioré dans Amazon Redshift](#).
- Mise en cache du centre d'identité IAM : le centre d'identité IAM 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 Redshift v2. Cela est dû au fait que la session IAM Identity Center associée dans l'éditeur de requêtes v2 reste valide, même dans le cas où 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.

Utilisation des rôles liés à un service pour Amazon Redshift

[Amazon Redshift utilise des rôles liés à un AWS Identity and Access Management service \(IAM\)](#). Un rôle lié à un service est un type unique de rôle IAM lié directement à Amazon Redshift. Les rôles liés aux services sont prédéfinis par Amazon Redshift et incluent toutes les autorisations requises par le service pour AWS appeler 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 géré par Redshift. Vous ne pouvez supprimer le rôle lié au service qu'après avoir supprimé tous les clusters Amazon Redshift ou les points de terminaison VPC gérés par Redshift 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 [Services AWS fonctionnant avec IAM](#) et recherchez les services avec un Yes (Oui) dans la colonne Service-Linked Role (Rôle lié à un service). Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations du rôle lié à un service 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`

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": "*"
  }
]
```

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 plus d'informations, consultez [Arrêt et suppression de clusters](#).

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 [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 AWS Identity and Access Management (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.

Pour plus d'informations, veuillez consulter la rubrique [Fournisseurs d'identité et fédération](#) dans le Guide de l'utilisateur IAM.

Rubriques

- [Présentation](#)
- [Création d'informations d'identification temporaires IAM](#)
- [Options visant à fournir des informations d'identification IAM](#)

Présentation

Amazon Redshift fournit l'opération d'[GetClusterCredentials](#) API 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) compatible avec le 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'opération `GetClusterCredentials` ou de la commande parallèle `get-cluster-credentials` CLI, reportez-vous [GetClusterCredentials](#) aux sections 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 d'utilisateur préexistantes provenant d'AWS Directory Service, de l'annuaire d'utilisateurs de votre entreprise ou d'un fournisseur d'identité web. Ils sont appelés 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.

Création d'informations d'identification temporaires IAM

Dans cette section, vous trouverez les étapes de configuration de votre système pour générer des informations temporaires d'identification de l'utilisateur de base de données basées sur IAM et vous connecter à votre base de données à l'aide de ces 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 des autorisations d'appel 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'identité (IdP) SAML-2.0 tiers.

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 IdP Amazon Redshift, créez un AWS fournisseur d'identité SAML. Vous créez un IdP dans la console IAM pour fournir des informations sur AWS l'IdP et sa configuration. Cela permet d'établir un lien 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 en matière de 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 de politique d'utilisation GetClusterCredentials](#).

Pour configurer votre IdP pour définir les paramètres `DbUser`, `AutoCreate` et `DbGroups`, incluez les éléments `Attribute` suivants :

- Un `Attribute` élément dont l'`Nameattribut` 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 `Attribute` 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 aucun. Définissez la valeur `AttributeValue` sur `false` pour spécifier que l'utilisateur de 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'attribut `Name` 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 des autorisations d'appel `GetClusterCredentials`

Votre client SQL a besoin d'une autorisation pour appeler l'opération `GetClusterCredentials` en votre nom. Pour fournir cette autorisation, vous créez un utilisateur ou un rôle et vous attachez une politique qui accorde les autorisations nécessaires.

Pour créer un rôle IAM autorisé à appeler `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'opération `redshift:DescribeClusters` 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 en matière de ressources pour GetClusterCredentials](#).

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`.

```
{
  "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.

```
{
  "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.

```
{
  "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](#).

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 AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	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.	<p>Suivez les instructions de l'interface que vous souhaitez utiliser.</p> <ul style="list-style-type: none"> • Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur. • Pour les AWS SDK, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des SDK et des outils.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	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 d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.
IAM	(Non recommandé) Utilisez des informations d'identification à long terme 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. <ul style="list-style-type: none"> • Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS SDK et les outils, voir Authentification à l'aide d'informations d'identification à long terme dans le Guide de l'AWS référence des SDK 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 Amazon Redshift JDBC et ODBC comprennent des plugins pour les fournisseurs d'identité basés sur SAML suivants :

- 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 avec Microsoft Azure AD](#).

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 le pilote JDBC version 2.1 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'opération `redshift:DescribeClusters`, 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 plus de détails, consultez [Options JDBC et ODBC pour la création d'informations d'identification de l'utilisateur de base de données](#).

L'URL suivante indique l' `AccessKeyId` 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 ODBC](#).

1. Installez et configurez le dernier pilote ODBC Amazon Redshift pour votre système d'exploitation. Pour plus d'informations, consultez [Configuration d'une connexion ODBC](#).

 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.

Pour plus d'informations, consultez les étapes suivantes :

- [Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows](#)
- [Utilisez un gestionnaire de pilotes ODBC pour configurer le pilote sur les systèmes d'exploitation Linux et macOS X](#)

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)
- Database (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` d'une région pour obtenir le serveur et le port en appelant l'opération `DescribeCluster`.

Si votre utilisateur ou rôle n'a pas l'autorisation d'appeler l'opération `redshift:DescribeClusters`, spécifiez `Serveur` et `Port`.

- b. Sous Authentication (Authentication), 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 plus d'informations, consultez [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 plus d'informations, consultez [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

SessionToken est requis 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 plus d'informations, consultez [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 [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 plus d'informations, consultez [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 [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 plus d'informations, consultez [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 [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 plus d'informations, consultez [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 plus d'informations, consultez [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 l' `AccessKeyId` et `SecretAccessKey`, éventuellement, `SessionToken` sous la forme de paramètres JDBC ou ODBC. `SessionToken` est requis uniquement pour un rôle IAM doté d'informations d'identification temporaires. Pour plus d'informations, consultez [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 plus d'informations, consultez [Utilisation d'un plugin de fournisseur d'informations d'identification](#).

Les pilotes Amazon Redshift JDBC et ODBC incluent des plugins pour les fournisseurs d'informations d'identification de fédération d'identité basées sur SAML 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 2.1](#) et [Configurer les options du pilote ODBC](#).

Pour plus d'informations, consultez [Configurer une connexion JDBC ou ODBC pour utiliser des informations d'identification IAM](#).

Utilisation d'un profil de configuration

Vous pouvez fournir les options d'identification IAM et les `GetClusterCredentials` options 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 plugin de fournisseur d'informations d'identification basé sur SAML inclus dans un pilote JDBC ou ODBC d'Amazon Redshift, vous pouvez utiliser les paramètres décrits précédemment dans [Utilisation d'un plugin de fournisseur d'informations d'identification](#). Si `plugin_name` n'est pas utilisé, les autres options sont ignorées.

L'exemple suivant montre le fichier `~/.aws/credentials` 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//////////
wEXAMPLEtc764bNrC9SAPBSM22wD0k4x4HIZ8j4FZTwdQWLWskWHGBuFqwaEMicRXmxfpSPfIeoIYRqTf1fKD8YUuwthAx7
qkPpKPi/kMcGd
QImGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5VSXDvp75YU
9HFv1Rd8Tx6q6fE8YQcHNvXAKiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fP0Ln9FX9KSYvKTr4rvx3iS1lTJabIQwj2ICCR/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 [Configuration de l'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.
AccessKey ID	ID de clé d'accès et clé d'accès secrète pour le rôle IAM ou l'utilisateur configuré pour l'authentification de base de données IAM. <code>SessionToken</code> est requis uniquement pour un rôle IAM doté d'informations d'identification temporaires.
SecretAccessKey	<code>SessionToken</code> n'est pas utilisé pour un utilisateur. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires .
SessionToken	
plugin_name	Nom complet d'une classe qui implémente un fournisseur d'informations d'identification. Le pilote Amazon Redshift JDBC inclut des plugins de fournisseurs d'informations d'identification basées sur SAML. Si vous fournissez <code>plugin_name</code> , vous pouvez également fournir d'autres options connexes. Pour plus d'informations, consultez Utilisation d'un plugin de fournisseur d'informations d'identification .
Profile	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 plus d'informations, consultez Utilisation d'un profil de configuration .

Utilisation d'un plugin de fournisseur d'informations d'identification

Amazon Redshift utilise des plugins de fournisseur d'informations d'identification pour l'authentification unique.

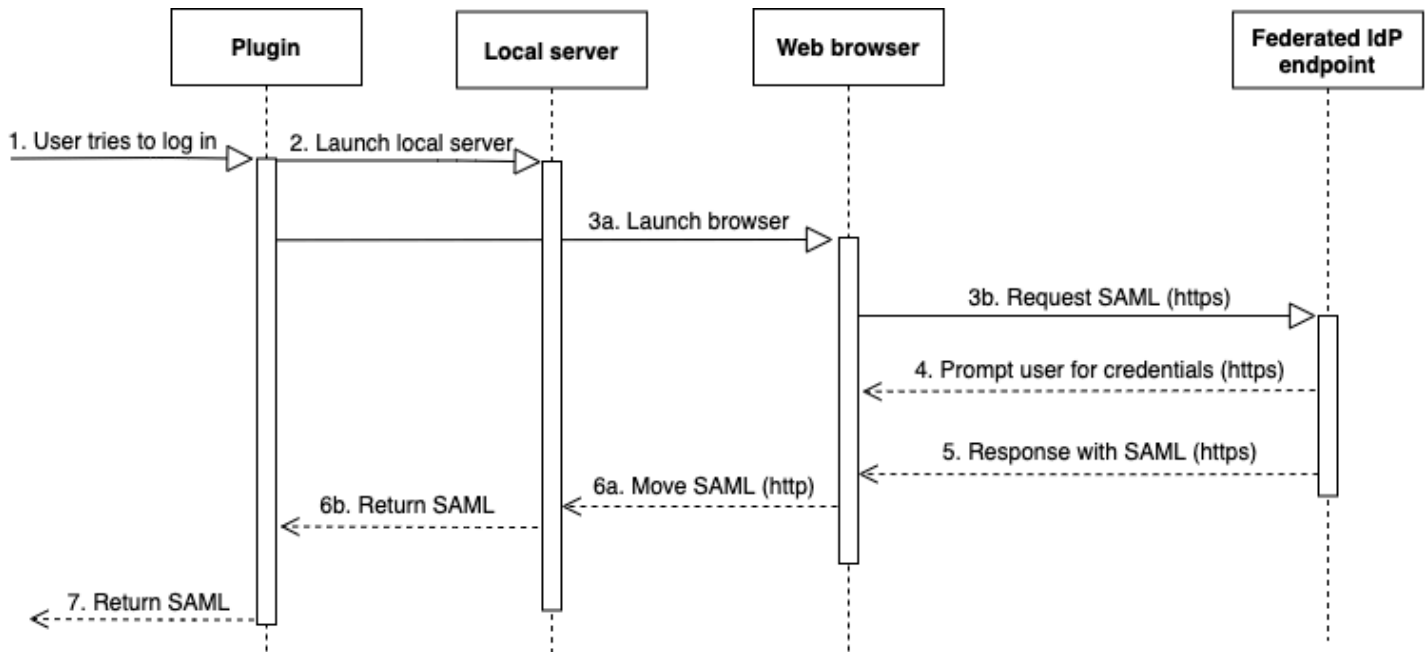
Pour prendre en charge l'authentification unique, Amazon Redshift fournit le plugin Azure AD pour Microsoft Azure Active Directory. Pour plus d'informations sur la configuration de ce plugin, consultez [Configuration de l'authentification unique JDBC ou ODBC avec Microsoft Azure AD](#).

Configuration de l'authentification multifacteur

Configuration de l'authentification multifacteur

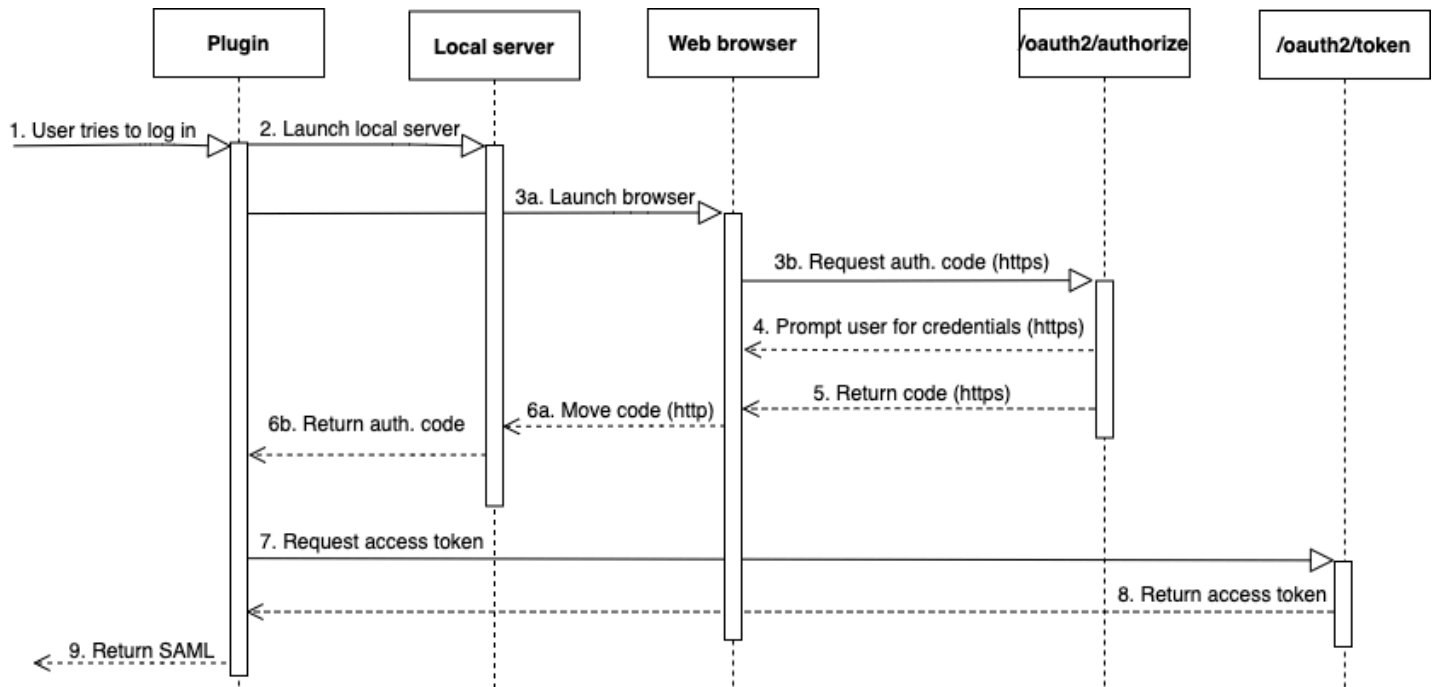
Pour prendre en charge l'authentification multifacteur (MFA), Amazon Redshift fournit des plugins basés sur un navigateur. Utilisez le plug-in SAML du navigateur pour Okta et PingOne le plug-in Azure AD du navigateur pour Microsoft Azure Active Directory.

Avec le plugin SAML du navigateur, l'authentification SAML 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 plus d'informations, consultez [Configuration de l'authentification unique JDBC ou ODBC avec AD FS](#).

- PingOne (Ping)

Le ping n'est pris en charge qu'avec l'adaptateur PingOne IdP prédéterminé utilisant l'authentification par formulaire.

Pour plus d'informations, consultez [Configuration de l'authentification unique JDBC ou ODBC avec Ping Identity](#).

- Okta

Okta est pris en charge uniquement pour l'application fournie par Okta utilisée avec le AWS Management Console.

Pour plus d'informations, consultez [Configuration de l'authentification unique JDBC ou ODBC avec Okta](#).

- Microsoft Azure Active Directory (Azure AD)

Pour plus d'informations, consultez [Configuration de l'authentification unique JDBC ou ODBC avec Microsoft Azure AD](#).

Configuration des options du plugin

Configuration des options du plugin

Pour utiliser un plugin de fournisseur d'informations d'identification basées sur SAML, 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
<code>plugin_name</code>	<p>Pour JDBC, nom de classe qui implémente un fournisseur d'informations d'identification. Spécifiez l'un des éléments suivants :</p> <ul style="list-style-type: none"> • Pour Active Directory Federation Services <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin-top: 10px;"> <code>com.amazon.redshift.plugin.AdfsCredentialsProvider</code> </div>

Option	Description
	<ul style="list-style-type: none"> • Pour Okta <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"> <code>com.amazon.redshift.plugin.OktaCredentialsProvider</code> </div> • Pour PingFederate <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"> <code>com.amazon.redshift.plugin.PingCredentialsProvider</code> </div> • Pour Microsoft Azure Active Directory <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"> <code>com.amazon.redshift.plugin.AzureCredentialsProvider</code> </div> • Pour SAML MFA <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"> <code>com.amazon.redshift.plugin.BrowserSamlCredentialsProvider</code> </div> • Pour une authentification unique Microsoft Azure Active Directory avec MFA <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"> <code>com.amazon.redshift.plugin.BrowserAzureCredentialsProvider</code> </div> <p>Pour ODBC, spécifiez l'un des éléments suivants :</p> <ul style="list-style-type: none"> • Pour Active Directory Federation Services : <code>adfs</code> • Pour Okta : <code>okta</code> • Pour PingFederate : <code>ping</code> • Pour Microsoft Azure Active Directory : <code>azure</code> • Pour MFA SAML : <code>browser saml</code> • Pour une authentification unique Microsoft Azure Active Directory avec MFA : <code>browser azure ad</code>
<code>idp_host</code>	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 <code>idp_host</code> doit se terminer par <code>.okta.com</code> .
<code>idp_port</code>	Port utilisé par le fournisseur d'identité. La valeur par défaut est 443. Ce port est ignoré pour Okta.

Option	Description
<code>preferred_role</code>	Amazon Resource Name (ARN) du rôle provenant des éléments <code>Attribute Value</code> pour l'attribut <code>Role</code> dans l'assertion SAML. Collaborez avec votre administrateur IdP pour rechercher la valeur appropriée pour le rôle préféré. Pour plus d'informations, consultez Configurer des assertions SAML pour votre IdP .
<code>user</code>	nom d'utilisateur d'entreprise, incluant le domaine, le cas échéant. Par exemple, pour Active Directory, le nom de domaine au format <code>domaine\nom d'utilisateur</code> 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.
<code>app_id</code>	ID d'une application Okta. Utilisé uniquement avec Okta. La valeur de <code>app_id</code> suit <code>amazon_aws</code> 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 : <code>https://example.okta.com/home/amazon_aws/0oa2hylw1rpM8UGehd1t7/272</code>
<code>idp_tenant</code>	Locataire utilisé pour Azure AD. Utilisé uniquement avec Azure.
<code>client_id</code>	ID client de l'application métier Amazon Redshift dans Azure AD. Utilisé uniquement avec Azure.

Configuration de l'authentification unique JDBC ou ODBC avec Microsoft Azure AD

Vous pouvez utiliser Microsoft Azure AD en tant que fournisseur d'identité (IdP) pour accéder à votre cluster Amazon Redshift. Vous trouverez ci-dessous une procédure qui décrit comment configurer une relation d'approbation à cet effet. Pour plus d'informations sur la configuration AWS en tant que fournisseur de services pour l'IdP, consultez les sections [Configuration de votre IdP SAML 2.0 en toute confiance et ajout de réclamations dans le](#) guide de l'utilisateur IAM.

 Note

Pour utiliser Azure AD avec JDBC, le pilote JDBC d'Amazon Redshift doit être de la version 1.2.37.1061 ou ultérieure. Pour utiliser Azure AD avec ODBC, le pilote ODBC d'Amazon Redshift doit être de la version 1.4.10.1000 ou ultérieure.

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](#).

Pour configurer Azure AD et votre AWS compte afin qu'ils se fassent mutuellement 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 plus d'informations, consultez [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' AWS application.
7. Sous Gérer, choisissez Single Sign-On.
8. Choisissez SAML. La page d'authentification basée sur Amazon Web Services (AWS) | SAML apparaît.
9. Choisissez Oui pour passer à la page Configurer l'authentification unique 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 Name (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 Name (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	Valeur
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:: <i>123456789012</i> :role/ <i>AzureSSO</i> ,arn:aws:iam:: <i>123456789012</i> :saml-provider/ <i>AzureADProvider</i>
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.userprincipalname

Nom de la demande	Valeur
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 sous la forme 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-identifiant***.
- Remplacez votre base de données (ou * pour toutes les bases de données) par ***dev***.
- Remplacez ***AROAJ2UCCR6DPCEXAMPLE*** 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-identifiant/dev",
        "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-identifiant/${redshift:DbUser}",
        "arn:aws:redshift:us-west-1:123456789012:cluster:cluster-identifiant"
      ],
      "Condition": {
        "StringEquals": {
          "aws:userid": "AROAJ2UCCR6DPCEXAMPLE:${redshift:DbUser}@example.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "redshift:CreateClusterUser",
      "Resource": "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-identifiant/${redshift:DbUser}"
    },
    {
      "Effect": "Allow",
      "Action": "redshift:JoinGroup",
      "Resource": "arn:aws:redshift:us-west-1:123456789012:dbgroup:cluster-identifiant/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 `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.

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 le pilote JDBC version 2.1 pour Amazon Redshift](#).

Par exemple, vous pouvez utiliser SQLWorkBench/J comme client. Lorsque vous configurez SQLWorkbench/J, l'URL de votre base de données utilise le format suivant.

```
jdbc:redshift:iam://cluster-identifiant:us-west-1/dev
```

Si vous utilisez SQLWorkBench/J comme client, procédez comme suit :

- a. Démarrez SQL Workbench/J. Sur 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-identifiant: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 spécifie au pilote d'utiliser l'authentification unique Azure AD 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 créé lors de la définition de votre configuration d'authentification unique Azure. Cela ne s'applique qu'au `com.amazon.redshift.plugin.AzureCredentialsProvider` plugin.
- Pour `client_id`, entrez **`your-azure-redshift-application-client-id`**. Utilisé uniquement pour 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.

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.

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.

Installez et configurez également le dernier pilote ODBC Amazon Redshift pour votre système d'exploitation comme suit :


- Pour Windows, consultez [Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows](#).
- Pour macOS, consultez [Installer le pilote ODBC d'Amazon Redshift sur macOS X](#).
- Pour Linux, consultez [Installer le pilote ODBC Amazon Redshift sous Linux](#).

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-identifiant***.
- 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 spécifie au pilote d'utiliser l'authentification unique Azure comme méthode d'authentification.
- Pour `plugin_name` de la configuration d'authentification unique Azure AD avec MFA, entrez ***BrowserAzureAD***. Cela spécifie au pilote d'utiliser l'authentification unique Azure 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
```

Pour résoudre les problèmes liés au plugin Browser Azure AD

1. 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 l'authentification unique avec SAML sur le portail Microsoft Azure. Ensuite, vérifiez que l'URL de réponse est définie sur `http://localhost/redshift/`.

2. 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.

3. 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.

4. 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 pour utiliser `http://localhost/redshift/` comme URI de redirection.

Configuration de l'authentification unique JDBC ou ODBC avec AD FS

Vous pouvez utiliser AD FS en tant que fournisseur d'identité (IdP) pour accéder à votre cluster Amazon Redshift. Vous trouverez ci-dessous une procédure qui décrit comment configurer une relation d'approbation à cet effet. Pour plus d'informations sur la configuration AWS en tant que fournisseur de services pour AD FS, consultez les sections [Configuration de votre IdP SAML 2.0 avec la confiance des parties et ajout](#) de réclamations dans le guide de l'utilisateur IAM.

Pour configurer AD FS et votre AWS compte de manière à ce qu'ils se fassent mutuellement confiance

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 page Modifier la règle, procédez comme suit :
 - Dans Nom de la règle de réclamation, entrez Nameld.
 - 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 pour configurer la relation de confiance 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 avec Microsoft Azure AD](#).

Pour configurer JDBC pour l'authentification auprès des services 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 le pilote JDBC version 2.1 pour Amazon Redshift](#).

Par exemple, vous pouvez utiliser SQLWorkBench/J comme client. Lorsque vous configurez SQLWorkbench/J, l'URL de votre base de données utilise le format suivant.

```
jdbc:redshift:iam://cluster-identifiant:us-west-1/dev
```

Si vous utilisez SQLWorkBench/J comme 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-identifiant*:*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.

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.

Installez et configurez également le dernier pilote ODBC Amazon Redshift pour votre système d'exploitation comme suit :


- Pour Windows, consultez [Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows](#).
- Pour macOS, consultez [Installer le pilote ODBC d'Amazon Redshift sur macOS X](#).
- Pour Linux, consultez [Installer le pilote ODBC Amazon Redshift sous Linux](#).

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
```

Configuration de l'authentification unique JDBC ou ODBC avec Ping Identity

Vous pouvez utiliser Ping Identity comme fournisseur d'identité (IdP) pour accéder à votre cluster Amazon Redshift. Vous trouverez ci-dessous une procédure qui décrit comment établir une relation de confiance à cette fin à l'aide du PingOne portail. Pour plus d'informations sur la configuration AWS en tant que fournisseur de services pour Ping Identity, consultez les [sections Configuration de votre IdP SAML 2.0 avec la confiance des parties et ajout](#) de réclamations dans le guide de l'utilisateur IAM.

Pour configurer Ping Identity et votre AWS compte afin qu'ils se fassent mutuellement 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 plus d'informations, consultez [Création d'un cluster](#).
2. Ajoutez Amazon Redshift en tant que nouvelle application SAML sur le portail. PingOne 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
<code>https://aws.amazon.com/SAML/Attributes/Role</code>	<i>arn:aws:iam : 123456789012:role/ Ping, arn:aws:iam : 123456789012:saml-provider/ PingProvider</i>
<code>https://aws.amazon.com/SAML/Attributes/RoleSessionName</code>	e-mail
<code>https://redshift.amazon.com/SAML/Attributes/AutoCreate</code>	"true"
<code>https://redshift.amazon.com/SAML/Attributes/ DbUser</code>	e-mail
<code>https://redshift.amazon.com/SAML/Attributes/ DbGroups</code>	Les groupes figurant dans les attributs « DbGroups » contiennent le préfixe @directory. Pour supprimer cela, dans Identity Bridge (Pont d'identité), saisissez memberOf. Dans Fonction, sélectionnez ExtractByRegularExpression. Dans Expression, saisissez <code>(.*)[\@](?:.*)</code> .

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 Lancer l'URL d'authentification unique (SSO) comme URL de connexion pour le plugin du navigateur SAML.
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 avec Microsoft Azure AD](#).

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 le pilote JDBC version 2.1 pour Amazon Redshift](#).

Par exemple, vous pouvez utiliser SQLWorkBench/J comme client. Lorsque vous configurez SQLWorkbench/J, l'URL de votre base de données utilise le format suivant.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Si vous utilisez SQLWorkBench/J comme 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 Utilisateur, entrez votre nom PingOne d'utilisateur. 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.
 - Dans 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-identifiant:your-cluster-region/your-database-name***.
- e. Choisissez Propriétés étendues et effectuez l'une des opérations suivantes :
 - Pour login_url, entrez ***your-ping-ss0-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 authentification unique comme méthode d'authentification.

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.

Installez et configurez également le dernier pilote ODBC Amazon Redshift pour votre système d'exploitation comme suit :


- Pour Windows, consultez [Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows](#).
- Pour macOS, consultez [Installer le pilote ODBC d'Amazon Redshift sur macOS X](#).
- Pour Linux, consultez [Installer le pilote ODBC Amazon Redshift sous Linux](#).

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 qui est autorisé à accéder au cluster à l'aide duquel vous essayez de vous authentifier. À utiliser uniquement pour le type d'authentification est le fournisseur d'identité : PingFederate.

- Pour Mot de passe, entrez ***your-ping-password***. À utiliser uniquement pour le type d'authentification est le fournisseur d'identité : 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-identifiant***. 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 du délai spécifié 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
```

Configuration de l'authentification unique JDBC ou ODBC avec Okta

Vous pouvez utiliser Okta comme fournisseur d'identité (IdP) pour accéder à votre cluster Amazon Redshift. Vous trouverez ci-dessous une procédure qui décrit comment configurer une relation d'approbation à cet effet. Pour plus d'informations sur la configuration AWS en tant que fournisseur de services pour Okta, consultez les sections [Configuration de votre idP SAML 2.0 en toute confiance et ajout de réclamations](#) dans le guide de l'utilisateur IAM.

Pour configurer Okta et votre AWS compte de manière à ce qu'ils se fassent mutuellement 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-ss-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 Advanced Settings (Paramètres avancés), pour SAML Issuer ID (ID d'émetteur SAML), saisissez ***your-Identity-Provider-Issuer-ID***, que vous pouvez trouver dans la section View Setup Instructions (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	Valeur
<code>https://aws.amazon.com/SAML/Attributes/Role</code>	<code>arn:aws:iam::<i>123456789012</i> :role/<i>Okta</i>,arn:aws:iam::<i>123456789012</i> :saml-provider/<i>Okta</i></code>
<code>https://aws.amazon.com/SAML/Attributes/RoleSessionName</code>	<code>user.email</code>

Nom de la demande	Valeur
<code>https://redshift.amazon.com/SAML/Attributes/AutoCreate</code>	<code>"true"</code>
<code>https://redshift.amazon.com/SAML/Attributes/DbUser</code>	<code>user.email</code>

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 avec Microsoft Azure AD](#).

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 le pilote JDBC version 2.1 pour Amazon Redshift](#).

Par exemple, vous pouvez utiliser SQLWorkBench/J comme client. Lorsque vous configurez SQLWorkbench/J, l'URL de votre base de données utilise le format suivant.

```
jdbc:redshift:iam://cluster-identifiant:us-west-1/dev
```

Si vous utilisez SQLWorkBench/J comme 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-identifiant:your-cluster-region/your-database-name**.
- e. Choisissez Propriétés étendues et effectuez l'une des opérations suivantes :
 - Pour login_url, entrez ***your-okta-ssologin-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.

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.


Installez et configurez également le dernier pilote ODBC Amazon Redshift pour votre système d'exploitation comme suit :

- Pour Windows, consultez [Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows](#).
- Pour macOS, consultez [Installer le pilote ODBC d'Amazon Redshift sur macOS X](#).
- Pour Linux, consultez [Installer le pilote ODBC Amazon Redshift sous Linux](#).

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 du délai spécifié 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
```

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 [Configurer des assertions SAML pour votre IdP](#).

Note

Si vous utilisez la variable de politique IAM `${redshift:DbUser}`, comme décrit dans [Politiques en matière de 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 de politique d'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
<code>DbUser</code>	Nom d'un utilisateur de la base de données. Si un utilisateur nommé <code>DbUser</code> existe dans la base de données, les informations d'identification de l'utilisateur temporaire ont les mêmes autorisations que l'utilisateur existant. S'il <code>DbUser</code> n'existe pas dans la base de données et <code>AutoCreate</code> s'il est vrai, un nouveau nom d'utilisateur <code>DbUser</code> est créé. Vous pouvez aussi désactiver le mot de passe d'un utilisateur existant. Pour plus d'informations, consultez ALTER_USER
<code>AutoCreate</code>	Spécifiez <code>true</code> pour créer un utilisateur de base de données portant le nom indiqué <code>DbUser</code> s'il n'en existe pas un. La valeur par défaut est <code>false</code> .
<code>DbGroups</code>	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 <code>PUBLIC</code> .

Génération d'informations d'identification de base de données pour une identité IAM à l'aide de la CLI ou de l'API Amazon Redshift

Pour générer par programmation des informations d'identification utilisateur temporaires de base de données, Amazon Redshift fournit [get-cluster-credentials](#) la commande pour le AWS CLI() et AWS Command Line Interface [GetClusterCredentials](#) l'opération API. 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 les étapes permettant d'appeler l'opération `GetClusterCredentials` ou la `get-cluster-credentials` commande par programme, de récupérer les informations d'identification de l'utilisateur de la base de données et de se connecter 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 [Création d'un rôle IAM avec des autorisations d'appel `GetClusterCredentials`](#).
2. En tant qu'utilisateur ou rôle que vous avez autorisé à l'étape précédente, exécutez la commande `get-cluster-credentials` CLI ou appelez l'opération `GetClusterCredentials` API et 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` qu'il est vrai, un nouvel utilisateur est créé avec le MOT DE PASSE désactivé.
 - Si l'utilisateur n'existe pas et qu' `AutoCreate` 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-identifiant 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": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM80yxpDHwXVPyJYBDm/
ggX2Eeaq6P3DgTzgPg=="
}
```

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-identifiant 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": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM80yxpDHwXVPyJYBDm/
ggX2Eeaq6P3DgTzgPg=="
}
```

- 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](#).

- Si la connexion n'utilise pas SSL, la tentative de connexion échoue.
- Le cluster envoie une demande d'authentification au client SQL.
- Le client SQL envoie le mot de passe temporaire au cluster.
- Si le mot de passe est valide et n'a pas expiré, le cluster établit la connexion.

Autoriser Amazon Redshift à accéder à d' AWS autres services en votre nom

Certaines fonctionnalités d'Amazon Redshift nécessitent qu'Amazon Redshift accède à AWS d'autres services en votre nom. Par exemple, les commandes [COPY](#) et [UNLOAD](#) peuvent charger ou télécharger les données de votre cluster Amazon Redshift à l'aide d'un compartiment Amazon S3. La commande [CREATE EXTERNAL FUNCTION](#) peut appeler 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 AWS Glue Athena ou. 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 AWS Identity and Access Management (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 AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
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. <ul style="list-style-type: none"> • Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur. • Pour les AWS SDK, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des SDK 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 d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	<p>Suivez les instructions de l'interface que vous souhaitez utiliser.</p> <ul style="list-style-type: none"> • Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS SDK et les outils, voir Authentifier à l'aide d'informations d'identification à long terme dans le Guide de AWS référence des SDK 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 doté des 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 aux services AWS

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 afin de permettre à Amazon Redshift d'accéder aux services AWS

1. Ouvrez la [console IAM](#).
2. Dans le panneau de navigation, choisissez Roles (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:workgroup-name/user-name`

2. Ouvrez la [console IAM](#).
3. Dans le panneau de navigation, choisissez Roles (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 AWS d'accéder à d'autres services en votre nom repose sur une relation de confiance comme suit :

```
{
  "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.

```
{
  "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.

Restriction d'un rôle IAM à une région AWS

Vous pouvez restreindre l'accès à un rôle IAM uniquement dans une certaine AWS région. 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](https://console.aws.amazon.com/) à l'adresse <https://console.aws.amazon.com/>.
2. Dans le panneau de navigation, choisissez Roles (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 AWS d'accéder à d'autres services en votre nom repose sur une relation de confiance comme suit :

```
{
  "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.

```
{
  "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 du cluster permettant à Amazon Redshift AWS d'accéder à d'autres services » dans [Quotas pour les objets Amazon Redshift](#)

Supposons, par exemple, que l'entreprise A souhaite accéder aux données d'un compartiment Amazon S3 appartenant à l'entreprise B. L'entreprise A crée un rôle de AWS service pour Amazon Redshift nommé `RoleA` et l'attache 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1487639602000",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::210987654321:role/RoleB"
    }
  ]
}
```

Un rôle transféré 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::role/RoleA"
      }
    }
  ]
}
```

La politique de confiance suivante établit une relation de confiance avec le propriétaire du RoleA AWS compte123456789012.

```
{
  "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 crée une chaîne avec `RoleA` et `RoleB` pour décharger des 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';
```

Informations supplémentaires

Pour en savoir plus, veuillez également consulter [Autorisation des opérations COPY, UNLOAD, CREATE EXTERNAL FUNCTION et CREATE EXTERNAL SCHEMA à l'aide des rôles IAM](#).

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 appeler des fonctions Lambda depuis AWS Lambda. La méthode préférée pour fournir des informations d'identification de sécurité consiste à spécifier un rôle AWS Identity and Access Management (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 [Autoriser Amazon Redshift à accéder à d' AWS autres services en votre nom](#).

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS l'extérieur de l'AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
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.	<p>Suivez les instructions de l'interface que vous souhaitez utiliser.</p> <ul style="list-style-type: none"> • Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur. • Pour les AWS SDK, les outils et les AWS API,

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
		<p>consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des SDK et des outils.</p>
IAM	<p>Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.</p>	<p>Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.</p>
IAM	<p>(Non recommandé) Utilisez des informations d'identification à long terme pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.</p>	<p>Suivez les instructions de l'interface que vous souhaitez utiliser.</p> <ul style="list-style-type: none"> • Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS SDK et les outils, voir Authentifier à l'aide d'informations d'identification à long terme dans le Guide de AWS référence des SDK 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.

Dans cette rubrique, vous apprenez à associer un rôle IAM à un cluster Amazon Redshift.

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 télécharger 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.

```
{
  "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 ne peut être associé à un cluster Amazon Redshift que si le rôle IAM et le cluster appartiennent au même compte. AWS

Utilisation de la console pour gérer les associations de rôle IAM

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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
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.

Utilisation du AWS CLI pour gérer les associations de rôles IAM

Vous pouvez gérer les associations de rôles IAM pour un cluster à AWS CLI l'aide des approches suivantes.

Associer un rôle IAM à un cluster à l'aide du AWS CLI

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-identifiant "my-redshift-cluster" \  
  --node-type "ra3.4xlarge" \  
  --number-of-nodes 16 \  
  --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftRole1" \  
  --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftRole2"
```

```
--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-identifiant "my-redshift-cluster" \  
  --add-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Dissociation d'un rôle IAM d'un cluster à l'aide du AWS CLI

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`. 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 pour un rôle IAM pour le 123456789012 AWS compte d'un cluster nommé `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifiant "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 les crée par programmation dans Compte AWS votre console 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.

Présentation des 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.

Utilisation des rôles IAM créés dans la console

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, télécharger, interroger et analyser les données relatives AWS aux 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 des autorisations pour exécuter des instructions SELECT pour AWS des services connexes, tels qu'Amazon S3, Amazon CloudWatch Logs SageMaker, Amazon 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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.
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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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.
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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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.
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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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.
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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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.
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 par défaut pour le cluster, utilisez la commande `aws redshift create-cluster` AWS CLI

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 \  
  --iam-roles 'arn:aws:iam::012345678910:role/myrole3'  
'arn:aws:iam::012345678910:role/myrole4'
```

```
--cluster-identifrier 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 permet de supprimer `myrole3` et `myrole4` de quitter le cluster.

```
aws redshift modify-cluster-iam-roles \  
--cluster-identifrier mycluster \  
--iam-roles 'arn:aws:iam::012345678910:role/myrole3'  
'arn:aws:iam::012345678910:role/myrole4'
```

```
--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:aws:iam::012345678910:role/myrole2
```

```
--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 le 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 commande `aws redshift restore-from-cluster-snapshot` AWS CLI

La AWS CLI commande suivante restaure le cluster à partir d'un instantané et le définit `myrole2` comme valeur par défaut pour le cluster.

```
aws redshift restore-from-cluster-snapshot \
  --cluster-identifiant mycluster-clone \
  --snapshot-identifiant 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'identité AWS avec les informations d'identification fournies par `GetDatabaseCredentials` peut simplifier l'autorisation et l'accès aux données locales et aux données externes. 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. Dans cette rubrique, nous expliquons comment fournir un accès aux ressources grâce à la fédération des AWS identités, au lieu d'utiliser un rôle IAM spécifique. La fédération d'identité, avec les informations d'identification fournies par `GetDatabaseCredentials`, peut fournir un accès aux ressources Redshift Spectrum AWS Glue et les rendre accessibles via des règles IAM granulaires qui sont 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 politique gérée est requise si vous l'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. Vous pouvez notamment utiliser le client SQL Workbench/J. Définissez les propriétés étendues de connexion client suivantes :
 - `AccessKeyID` — L'identifiant de votre clé d'accès.
 - `SecretAccessClé` : 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`— 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 des AWS Glue travaux 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'
```

Dans ce cas, `catalog_id` la valeur est votre numéro 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, `table1` peut être, par exemple, de données au format JSON 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 2.1.](#)

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 [Autoriser Amazon Redshift à accéder à d' AWS autres 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 n'avez plus besoin de gérer les rôles IAM attachés à un cluster pour que Redshift Spectrum puisse interroger les données enregistrées auprès de ce dernier. AWS Lake Formation Pour plus d'informations, consultez [Utilisation 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 :

- Création d'un cluster provisionné ou d'un espace de noms sans serveur
- Restauration d'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 fournie par AWS Secrets Manager .

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 provisionné ou à un espace de noms sans serveur avec des informations d'identification gérées par secret, vous pouvez récupérer le secret à partir d' AWS Secrets Manager à l'aide de la console Secrets Manager ou de l'appel d'API Secrets Manager `GetSecretValue`. 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 l'intégration

Les utilisateurs doivent disposer des autorisations requises pour effectuer les opérations liées à AWS Secrets Manager l'intégration. 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 plus d'informations, consultez [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 du secret de mot de passe d'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, il 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, voir [Rotation AWS Secrets Manager des secrets](#) dans le guide de l'utilisateur AWS Secrets Manager.

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 AWS Management Console 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 AWS Management Console 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 de connexion à la base de données

Vous pouvez créer un secret Secrets Manager pour stocker les informations d'identification utilisées pour vous connecter à un cluster provisionné par Amazon Redshift ou à un espace de noms et à un groupe de travail Redshift Serverless. Vous pouvez également utiliser ce secret lors de la planification d'une requête dans l'éditeur de requêtes Amazon Redshift v2.

Pour créer un secret pour une base de données dans un cluster provisionné par 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 Credentials for Amazon Redshift Data Warehouse. 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 l'entrepôt de données, choisissez le cluster provisionné Amazon Redshift qui contient vos données.
 - Dans Nom du secret, entrez le nom du secret.
 - Dans Description, entrez une description du secret.
 - Pour les 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 l'éditeur de requêtes Amazon Redshift 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.
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 du tag `Redshift`.

Pour créer un secret pour une base de données dans un espace de noms Redshift Serverless à l'aide de la console Redshift Serverless

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
2. Choisissez Redshift serverless et accédez à la 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, modifiez les informations d'identification de l'administrateur.

5. Pour le 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.

Vérifiez qu'un message s'affiche 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 avoir une clé de balise commençant par la chaîne « Redshift » pour qu'il 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 Redshift Serverless 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 Credentials for Amazon Redshift Data Warehouse. 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 l'entrepôt de données, choisissez l'espace de noms Redshift Serverless qui contient vos données.
 - Dans Nom du secret, entrez le nom du secret.
 - Dans Description, entrez une description du secret.
 - Pour les 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 l'éditeur de requêtes Amazon Redshift 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.

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 du tag `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 à utiliser AWS CloudShell à exécuter la commande AWS CLI Secrets Manager comme suit. Vous devez disposer des autorisations appropriées pour exécuter les commandes AWS CLI indiquées dans la procédure suivante.

1. Sur la console AWS, ouvrez l'invite de commande AWS CloudShell. Pour plus d'informations sur AWS CloudShell, voir [Contenu](#) du guide AWS CloudShell de l'utilisateur AWS CloudShell.
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 Amazon Redshift Query Editor v2. Remplacez les valeurs suivantes dans la commande par des valeurs correspondant à votre environnement :
 - `admin` est le nom d'utilisateur de l'administrateur de l'entrepôt de données.
 - `password` est le mot de passe de l'administrateur.
 - `dev` est le nom initial de la base de données dans l'entrepôt de données.
 - `la région` est celle 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 pouvez trouver cet identifiant sur la page de 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\":\"password\",\"dbname\":\n\"dev\",\"engine\":\"redshift\"} \" \n--tags "[{\"Key\":\"redshift-serverless:namespaceArn\",\"Value\":\n\"arn:aws:redshift-serverless:region:123456789012:namespace/namespace-id\"}]\"
```

Considérations relatives à 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 le programme de rotation automatique à l'aide de l'appel `secretsmanager:RotateSecret` d'API pour continuer à faire AWS Secrets Manager automatiquement pivoter 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 le programme de rotation automatique à l'aide de l'appel `secretsmanager:RotateSecret` d'API pour continuer à faire AWS Secrets Manager automatiquement pivoter votre secret.

Journalisation et surveillance dans Amazon Redshift

La surveillance est un enjeu important pour assurer la fiabilité, la disponibilité et les performances d'Amazon Redshift et de vos solutions AWS. Vous pouvez recueillir les données de surveillance de toutes les parties de votre solution AWS de telle sorte que vous puissiez déboguer plus facilement une éventuelle défaillance à plusieurs points. AWS fournit plusieurs outils pour surveiller vos ressources Amazon Redshift et répondre aux incidents potentiels :

Alarmes Amazon CloudWatch

À l'aide d'alarmes Amazon CloudWatch, vous surveillez une métrique unique sur une période donnée que vous spécifiez. Si la métrique dépasse un seuil donné, une notification est envoyée à une rubrique Amazon SNS ou à une stratégie AWS Auto Scaling. Les alarmes CloudWatch n'appellent pas une action uniquement parce qu'elles se trouvent dans un état particulier. L'état doit avoir changé et avoir été conservé pendant un nombre de périodes spécifié. Pour de plus amples informations, veuillez consulter [Gérer les alarmes](#). Pour connaître la liste des métriques, consultez [Surveillance d'Amazon Redshift à l'aide de métriques CloudWatch](#).

Journaux AWS CloudTrail

CloudTrail fournit un enregistrement des opérations API effectuées par un utilisateur, un rôle IAM ou un service AWS dans Amazon Redshift. Avec les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à Amazon Redshift, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres détails. 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](#)
- [Activation de la journalisation](#)
- [Envoi de journaux d'audit à Amazon CloudWatch](#)
- [Gestion des fichiers journaux dans Simple Storage Service \(Amazon S3\)](#)
- [Dépannage de la journalisation des audits Amazon Redshift dans Amazon S3](#)
- [Journalisation des appels d'API Amazon Redshift avec AWS CloudTrail](#)
- [Configuration d'audit à l'aide de la console](#)
- [Configuration de la journalisation à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift](#)

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).
sslcipher	Chiffrement SSL.
mtu	Unité de transmission maximale (MTU).
sslcompression	Type de compression SSL.
sslexpansion	Type d'extension SSL.
iamauthguid	L'ID d'authentification AWS Identity and Access Management (IAM) pour la AWS CloudTrail demande. Il s'agit de l'identifiant de l'appel d' GetClusterCredentials API 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.

Nom de la colonne	Description
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.

Nom de la colonne	Description
action	Action qui s'est produite. Valeurs valides : <ul style="list-style-type: none"> • Alter • Création • 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.

Nom de la colonne	Description
utilisateur	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.

Activation de la journalisation

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'AWS Management Console 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 plus d'informations, consultez [Groupes de paramètres Amazon Redshift](#).

Envoi de journaux d'audit à Amazon CloudWatch

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.

Gestion des fichiers journaux dans Simple Storage Service (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 pouvez seulement utiliser le chiffrement des clés gérées par Amazon S3 (SSE-S3) (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 cas Régions AWS, vous ajoutez le nom principal du service Redshift, `redshift.amazonaws.com`.*

La politique de compartiment 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.

```
{
  "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.

```
{
  "Version": "2008-10-17",
  "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 « opt-in », nécessitent un nom de principal du service spécifique à une région. 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 du principal du service spécifique à la région correspond à la région où 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 politiques de compartiments, veuillez consulter la rubrique [Création d'un compartiment](#) et [Modification des autorisations de compartiment](#) 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

Dépannage de la journalisation des audits Amazon Redshift dans 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.

Journalisation des appels d'API Amazon Redshift 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](#).

Configuration d'audit à l'aide de la console

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 AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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).

Configuration de la journalisation à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift

Vous pouvez utiliser les opérations de CLI Amazon Redshift suivantes pour configurer la journalisation d'audit :

- [describe-logging-status](#)
- [disable-logging](#)
- [enable-logging](#)

Vous pouvez utiliser les opérations de l'API Amazon Redshift suivantes pour configurer la journalisation d'audit :

- [DescribeLoggingStatus](#)
- [DisableLogging](#)
- [EnableLogging](#)

Se connecter avec CloudTrail

Journalisation des appels avec AWS 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](#).

Utilisation des informations contenues 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 afficher, rechercher et télécharger les événements récents dans votre compte AWS. 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 d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de

votre choix. 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 des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la demande a été effectuée par un autre service AWS.

Pour plus d'informations, consultez la section [CloudTrail UserIdentity Element](#) dans le guide de l'utilisateur AWS CloudTrail.

Présentation des entrées des fichiers journaux

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 individuelle émise à partir d'une source quelconque et comprend 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'AuthorizeDataShareopération.

```
{
  "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 boto3/1.17.41",
  "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'CreateNamespaceaction.

```

{
  "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 boto3/1.17.41",
  "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'ExecuteStatementaction 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 boto3/1.17.41",
  "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 l'éditeur de requêtes v2 Amazon Redshift.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'CreateConnectionaction.

```
{
  "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",
        "updatedAt": "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 les journaux AWS CloudTrail

Lorsqu'Amazon Redshift appelle un autre service AWS pour vous, l'appel est journalisé avec un ID de compte qui appartient à Amazon Redshift. Il n'est pas consigné avec votre ID de compte. Par exemple, supposons qu'Amazon Redshift appelle des opérations AWS Key Management Service (AWS KMS) telles que `CreateGrant`, `Decrypt`, `Encrypt` et `RetireGrant` pour gérer le

chiffrement sur votre cluster. Dans ce cas, les appels sont journalisés par AWS CloudTrail en utilisant un ID 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 US East (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 (Melbourne)	ap-southeast-4	945512339897
Région Asie-Pacifique (Mumbai)	ap-south-1	408097707231
Région Asie-Pacifique (Osaka)	ap-northeast-3	398671365691
Région Asia Pacific (Seoul)	ap-northeast-2	713597048934
Région Asie-Pacifique (Singapour)	ap-southeast-1	960118270566
Région Asie-Pacifique (Sydney)	ap-southeast-2	485979073181
Région Asie-Pacifique (Tokyo)	ap-northeast-1	615915377779

Région	Région	ID de compte
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
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": "AR0AI5QPCMKLTL4VHFCYY: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": "AR0AI5QPCMKLTL4VHFCYY",
        "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"  
}
```

Validation de la conformité pour Amazon Redshift

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon Redshift dans le cadre de plusieurs programmes de conformité AWS. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et autres.

Pour obtenir la liste des services AWS concernés par des programmes de conformité spécifiques, consultez [Services AWS concernés par les programmes de conformité](#). Pour obtenir des informations générales, veuillez consulter [Programmes de conformité AWS](#).

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour plus d'informations, consultez [Téléchargement des 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, AWS fournit des ressources pour vous aider :

- Les [Guides de démarrage rapide de la sécurité et de la conformité](#) proposent des considérations architecturales et fournissent des étapes pour déployer des environnements de référence centrés 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 utiliser AWS pour créer des applications conformes à la loi HIPAA.
- [Ressources de conformité AWS](#), manuels et guides susceptibles de s'appliquer à votre secteur et à votre emplacement.
- [AWS Config](#), un service AWS qui permet d'évaluer comment les configurations de vos ressources se conforment aux pratiques internes, aux normes et aux directives industrielles.
- [AWS Security Hub](#), un service AWS qui fournit une vue complète de votre état de sécurité au sein d'AWS et vous permet de vérifier votre conformité aux normes du secteur et aux bonnes pratiques de sécurité. Security Hub utilise des contrôles de sécurité pour évaluer les configurations des ressources et les normes de sécurité afin de vous aider à respecter divers cadres de conformité.

Pour plus d'informations sur l'utilisation de Security Hub pour évaluer les ressources Amazon Redshift, consultez [Contrôles Amazon Redshift](#) dans le Guide de l'utilisateur AWS Security Hub.

Les documents suivants liés à la sécurité et à la conformité couvrent Amazon Redshift et sont disponibles à la demande via 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 mondiale d'AWS repose sur des régions AWS et des zones de disponibilité AWS. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. 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 régions AWS ont 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 [Déplacement de votre cluster](#).

En cas de panne lorsqu'un événement inattendu se produit dans une zone de disponibilité, vous pouvez définir un déploiement avec plusieurs zones de disponibilité (multi-AZ) afin que votre entrepôt des 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 déploiements Multi-AZ, consultez [Configuration d'un déploiement multi-AZ](#).

Pour plus d'informations sur les régions et les zones de disponibilité AWS, consultez [Infrastructure mondiale AWS](#).

Sécurité de l'infrastructure dans Amazon Redshift

En tant que service géré, Amazon Redshift est protégé par la sécurité du réseau mondial AWS. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez la section [Sécurité du cloud AWS](#). Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section [Protection de l'infrastructure](#) dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous pouvez utiliser les appels d'API publiés par AWS 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 nous recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser [AWS Security Token Service](#)

(AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Isolement de réseau

Un réseau privé virtuel (VPC) basé sur le service Amazon VPC constitue votre réseau privé isolé logiquement dans le Cloud AWS. Vous pouvez déployer un cluster Amazon Redshift dans un VPC en procédant comme suit :

- Créez un VPC dans une région AWS. 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. Pour de plus amples informations, veuillez consulter [Groupes de sous-réseaux du cluster Amazon Redshift](#).

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 de plus amples informations, veuillez consulter [Groupes de sous-réseaux du cluster Amazon 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'entreprise.

Lors de la configuration des listes de contrôle d'accès réseau associées au(x) sous-réseau(x) avec lequel/lesquels votre cluster Amazon Redshift est balisé, assurez-vous que les plages CIDR S3 de la région AWS sont ajoutées à la liste approuvée pour les règles d'entrée et de sortie. Cela vous permet d'exécuter des opérations basées sur S3 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 du cluster 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 êtes sur la plateforme EC2-VPC, vous pouvez utiliser un groupe de sécurité Amazon VPC existant ou en définir un nouveau et l'associer ensuite à un cluster. Pour plus d'informations sur la gestion d'un cluster sur la plateforme EC2-VPC, consultez la section [Gestion des clusters dans un VPC](#).

Connexion à Amazon Redshift à l'aide d'un point de terminaison de VPC d'interface

Vous pouvez vous connecter directement à Amazon Redshift 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 à ce sujet AWS PrivateLink, consultez la section [Interface VPC endpoints \(AWS PrivateLink\)](#) dans le guide de l'utilisateur Amazon VPC. Notez que la connexion JDBC/ODBC au cluster ne fait pas partie du service API Amazon Redshift.

Lorsque vous utilisez un point de terminaison VPC d'interface, la communication entre votre VPC et Amazon Redshift s'effectue entièrement au sein du AWS réseau, ce qui peut renforcer la sécurité. 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 AWS 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 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 AWS VPN option ou. AWS Direct Connect Pour plus d'informations sur AWS VPN les options, consultez la section [Connexions VPN](#) dans le guide de l'utilisateur Amazon VPC. Pour obtenir des informations sur AWS Direct Connect, consultez [Création d'une connexion](#) dans le Guide de l'utilisateur AWS Direct Connect .

Vous pouvez créer un point de terminaison VPC d'interface pour vous connecter à Amazon Redshift à AWS Management Console 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. Lorsque vous le faites, la résolution du point de terminaison Amazon Redshift par défaut (<https://redshift.Region.amazonaws.com>) est faite par votre point de terminaison de VPC.

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.

```
VPC_endpoint_ID.redshift.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 prend en charge les appels à toutes ses [fonctions API](#) à l'intérieur 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 AWS Identity and Access Management (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 en savoir plus, consultez [Contrôle de l'accès aux services avec des points de terminaison d'un VPC](#) dans le guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison de 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.

Rubriques

- [Exemple : politique de point de terminaison VPC visant à refuser tout accès à partir d'un compte spécifié AWS](#)
- [Exemple : politique de point de terminaison d'un VPC pour autoriser l'accès VPC uniquement à un rôle IAM spécifié](#)
- [Exemple : politique de point de terminaison de VPC pour autoriser l'accès VPC uniquement à un principal IAM spécifié \(utilisateur\)](#)
- [Exemple : politique de point de terminaison VPC pour autoriser les opérations Amazon Redshift en lecture seule](#)
- [Exemple : politique de point de terminaison de VPC refusant l'accès à un cluster spécifié](#)

Exemple : politique de point de terminaison VPC visant à refuser tout accès à partir d'un compte spécifié AWS

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 redshiftrole dans AWS le compte 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 IAM du compte 123456789012 redshiftadmin. AWS 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"
        ]
      }
    }
  ]
}
```

Configuration et analyse des vulnérabilités dans Amazon Redshift

AWS gère les tâches de sécurité de base comme les correctifs du système d'exploitation invité et de base de données, la configuration du pare-feu, et la reprise après sinistre. 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 requête Amazon Redshift v2 est une application gérée par AWS. Tous les correctifs et mises à jour sont appliqués par AWS si nécessaire.

Tâches de réseau

Vous pouvez effectuer des tâches réseau, telles que la personnalisation de votre connexion à une base de données Redshift. Vous pouvez également effectuer des tâches liées au DNS, telles que la configuration d'un nom de domaine personnalisé. Ces tâches de configuration sont disponibles si vous disposez d'un cluster provisionné par Amazon Redshift ou d'un groupe de travail Amazon Redshift Serverless.

Rubriques

- [Utilisation d'un nom de domaine personnalisé pour les connexions client](#)
- [Utilisation des points de terminaison de VPC gérés par RedShift](#)
- [Amélioration du routage VPC dans Amazon Redshift](#)

Utilisation d'un nom 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 easy-to-read DNS qui achemine les connexions des clients 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. Pour en savoir plus, consultez [Configuration d'un nom de domaine personnalisé](#).

Sécurité pour un nom de domaine personnalisé

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).

Renouvellement d'un certificat

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.

Configuration d'un nom de domaine personnalisé

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 Les étapes sont détaillées dans les sections suivantes.

Enregistrement d'un nom de domaine et sélection d'un certificat

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 [Déplacement de votre 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 :

Demande de certificat auprès d'ACM pour un nom de domaine

1. Connectez-vous à la console ACM AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/acm/>.
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 qu'ACM 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.

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](#).

Création du nom de 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 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.

Changement de nom d'un cluster auquel un domaine personnalisé a été attribué à l'aide de la console

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 personnalisés à l'aide de commandes CLI

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 personnalisées, 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 d'y parvenir. 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 du 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 plus d'informations, consultez [DeleteCustomDomainAssociation](#).

Connexion à votre cluster ou groupe de travail avec un nom de domaine personnalisé, à l'aide d'un client SQL

Pour vous connecter à un nom de domaine personnalisé, les autorisations IAM suivantes sont requises pour un cluster provisionné : `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 et Python. Les connexions ODBC ne sont pas prises en charge.

Utilisation des points de terminaison de VPC gérés par RedShift

Par défaut, un cluster Amazon Redshift ou un groupe de travail Amazon Redshift Serverless est provisionné dans un cloud privé virtuel (VPC). Le VPC est accessible depuis un autre VPC ou sous-réseau lorsque vous autorisez l'accès public ou que vous configurez une passerelle Internet, un périphérique NAT ou une AWS Direct Connect connexion pour acheminer le trafic vers celui-ci. Vous pouvez également accéder à un cluster ou à un groupe de travail en configurant un point de terminaison VPC géré par Redshift (alimenté par). AWS PrivateLink

Vous pouvez configurer un point de terminaison VPC géré par Redshift 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 dans un autre compte, le titulaire du compte (concedant) doit accorder l'accès au compte de connexion (bénéficiaire). Grâce à cette approche, vous pouvez accéder à l'entrepôt de données sans utiliser d'adresse IP publique ni acheminer le trafic via Internet.

Voici les raisons les plus courantes pour autoriser l'accès à l'aide d'un point de terminaison VPC géré par Redshift :

- 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 pour configurer un point de terminaison VPC géré par Redshift 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 AWS compte et l'identifiant VPC (ou tous les VPC) du bénéficiaire.
2. Le compte bénéficiaire est informé qu'il est autorisé à créer un point de terminaison de VPC géré par Redshift.
3. Le compte bénéficiaire crée un point de terminaison de VPC géré par Redshift.
4. Le compte bénéficiaire accède au cluster ou au groupe de travail du compte propriétaire via le point de terminaison VPC géré par Redshift.

Pour ce faire, vous pouvez utiliser la console Amazon Redshift AWS CLI, ou l'API Amazon Redshift.

Considérations lors de l'utilisation de points de terminaison de VPC gérés par Redshift

Note

Pour créer ou modifier des points de terminaison VPC gérés par Redshift, vous avez besoin d'une `ec2:CreateVpcEndpoint` autorisation `ec2:ModifyVpcEndpoint` ou d'une autorisation figurant dans votre politique IAM, en plus des autres autorisations spécifiées dans la politique gérée. `AWS AmazonRedshiftFullAccess`

Lorsque vous utilisez des points de terminaison de VPC gérés par Redshift, gardez à l'esprit les points suivants :

- Assurez-vous que le cluster auquel accéder est un type de nœud RA3. Un groupe de travail Amazon Redshift Serverless fonctionne également pour cela.
- Pour les clusters provisionnés, assurez-vous que le cluster est activé pour la relocalisation du cluster ou pour le multi-AZ. Pour plus d'informations sur les conditions requises pour activer la relocalisation du cluster, consultez [Déplacement de votre cluster](#). Pour plus d'informations sur l'activation de Multi-AZ, consultez [Configuration de Multi-AZ lors de la création d'un cluster](#).
- Assurez-vous que le cluster ou le groupe de travail auquel accéder via son groupe de sécurité est disponible dans les plages de ports valides 5431 à 5455 et 8191 à 8215. La valeur par défaut est 5439.
- Vous pouvez modifier les groupes de sécurité VPC associés à un point de terminaison de VPC géré par Redshift existant. Pour modifier d'autres paramètres, supprimez le point de terminaison de VPC géré par Redshift actuel et créez-en un nouveau.
- Le nombre de points de terminaison de VPC gérés par Redshift que vous pouvez créer est limité à votre quota de points de terminaison de VPC.
- Les points de terminaison de VPC gérés par Redshift ne sont pas accessibles depuis Internet. Un point de terminaison VPC géré par Redshift n'est accessible qu'au sein du VPC où le point de terminaison est provisionné ou à partir de tout VPC apparié 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 de VPC gérés par Redshift.

- Lorsque vous créez un point de terminaison VPC géré par Redshift pour un cluster provisionné, le VPC que vous choisissez doit avoir un groupe de sous-réseaux. Pour créer un groupe de sous-réseaux, consultez [Gestion des groupes de sous-réseaux du cluster à l'aide de la console](#).
- Si une zone de disponibilité est hors service, Amazon Redshift ne crée pas de nouvelle interface Elastic network dans une autre zone de disponibilité. Dans ce cas, vous devrez peut-être créer un nouveau 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](#).

Gestion des points de terminaison VPC gérés par Redshift à l'aide de la console

Vous pouvez configurer l'utilisation des points de terminaison de VPC gérés par Redshift à l'aide de la console Amazon Redshift.

Octroi de l'accès à

Si le VPC auquel vous souhaitez accéder à votre cluster ou groupe de travail se trouve sur un autre AWS compte, assurez-vous de l'autoriser depuis le compte du propriétaire (du concédant).

Pour autoriser un VPC d'un autre AWS compte à accéder à votre cluster ou groupe de travail

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`](https://console.aws.amazon.com/redshiftv2/).
2. Dans le menu de navigation, choisissez Clusters. Pour Amazon Redshift Serverless, choisissez le tableau de bord sans serveur.
3. Pour un cluster auquel vous souhaitez autoriser l'accès, consultez les détails 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 Serverless, 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 terminaison de VPC géré par Redshift

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 VPC géré par Redshift pour celui-ci.

Pour créer un point de terminaison de VPC géré par Redshift

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dans le menu de navigation, choisissez Configurations.

La page Configurations affiche les points de terminaison de VPC gérés par Redshift qui ont été créés. Pour afficher les détails d'un point de terminaison, choisissez son nom. Pour Amazon Redshift Serverless, les points de terminaison 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 AWS compte 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 dans Subnet définit les sous-réseaux et les adresses IP sur lesquels 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.

Les règles du groupe de sécurité du groupe de sécurité VPC définissent les ports, les protocoles et les sources du trafic entrant que vous autorisez pour votre point de terminaison. Vous autorisez l'accès au port sélectionné via le groupe de sécurité ou la plage CIDR sur laquelle s'exécutent vos charges de travail.

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 VPC géré par Redshift.

Gestion des points de terminaison VPC gérés par Redshift à l'aide du AWS CLI

Vous pouvez utiliser les opérations de la CLI d'Amazon Redshift suivantes pour utiliser les points de terminaison de VPC gérés par Redshift. Pour plus d'informations, consultez la référence de la commande AWS CLI .

- [authorize-endpoint-access](#)
- [revoke-endpoint-access](#)
- [create-endpoint-access](#)
- [modify-endpoint-access](#)
- [delete-endpoint-access](#)
- [describe-endpoint-access](#)
- [describe-endpoint-authorization](#)

Gestion des points de terminaison de VPC gérés par Redshift à l'aide des opérations d'API Amazon Redshift

Vous pouvez utiliser les opérations de l'API d'Amazon Redshift suivantes pour utiliser les points de terminaison de VPC gérés par Redshift. Pour plus d'informations, consultez la référence d'API Amazon Redshift.

- [AuthorizeEndpointAccess](#)
- [RevokeEndpointAccess](#)
- [CreateEndpointAccess](#)
- [ModifyEndpointAccess](#)
- [DeleteEndpointAccess](#)
- [DescribeEndpointAccess](#)
- [DescribeEndpointAuthorization](#)

Gestion des points de terminaison VPC gérés par Redshift à l'aide de AWS CloudFormation

Pour plus d'informations sur le type de AWS CloudFormation ressource à AWS CloudFormation utiliser pour créer un point de terminaison VPC géré par Redshift, [AWS::Redshift::EndpointAccess](#) consultez le guide de l'utilisateur AWS CloudFormation

Amélioration du routage VPC dans Amazon 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 gérer de près 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 [Redshift Spectrum et le 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, 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 [Utilisation des 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 Amazon S3 VPC Gateway, 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, le cluster doit avoir une adresse IP publique 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.

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

- [Utilisation des points de terminaison d'un VPC](#)
- [Routage VPC amélioré](#)
- [Redshift Spectrum et le routage VPC amélioré](#)

Utilisation des points de terminaison d'un VPC

Vous pouvez utiliser un point de terminaison VPC pour créer une connexion gérée entre votre cluster Amazon Redshift 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 téléchargement 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. Imaginons par exemple que vous avez un acheminement existant dans votre table de routage pour tout le trafic Internet (0.0.0.0/0) ; cet acheminement 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 puisque 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 end-to-end du réseau 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](#).

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 pour un cluster, votre cluster doit répondre aux exigences et aux contraintes suivantes :

- Votre cluster doit se trouver dans un VPC.

Si vous attachez un point de terminaison Amazon S3 VPC, votre cluster utilise le point de terminaison VPC uniquement pour accéder aux compartiments Amazon S3 de 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 accessible au public ou utilisez [une passerelle de traduction d'adresses réseau \(NAT\)](#). Pour plus d'informations, consultez [Création d'un cluster 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 créer un cluster avec un routage VPC amélioré

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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 créer un groupe de travail Amazon Redshift sans serveur avec un routage VPC amélioré

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

Redshift Spectrum et le routage VPC amélioré

Amazon Redshift Spectrum ne prend pas en charge le routage VPC amélioré avec des clusters provisionnés. Le routage VPC amélioré Amazon Redshift achemine un trafic spécifique via votre VPC. L'ensemble du trafic entre votre cluster et vos compartiments Amazon S3 est contraint de passer par votre VPC Amazon. Redshift Spectrum s'exécute sur des ressources AWS gérées détenues par Amazon Redshift. Puisque ces ressources se trouvent en dehors de votre VPC, Redshift Spectrum n'utilise pas le routage VPC amélioré.

Le trafic entre Redshift Spectrum et Amazon S3 est acheminé de manière sécurisée via le réseau AWS privé, en dehors de votre VPC. Le trafic en transit est signé par le protocole Amazon Signature Version 4 (SIGv4) et chiffré via 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. Vous devrez peut-être également configurer votre VPC pour autoriser votre cluster à accéder à AWS Glue Athena, comme indiqué ci-dessous.

Étant donné que le routage VPC amélioré affecte la manière dont Amazon Redshift accède aux autres ressources, les requêtes peuvent échouer si vous ne configurez pas votre VPC correctement. Pour obtenir plus d'informations, consultez la rubrique [Amélioration du routage VPC dans Amazon Redshift](#) qui traite en détail de la création d'un point de terminaison VPC, d'une passerelle NAT et d'autres ressources de réseaux pour diriger le trafic vers vos compartiments Amazon S3.

Note

Amazon Redshift sans serveur prend en charge le routage VPC amélioré pour les requêtes vers des tables externes sur Amazon S3.

Considérations relatives à l'utilisation d'Amazon Redshift Spectrum

Vous trouverez ci-après les considérations relatives à l'utilisation de Redshift Spectrum :

- [Politiques d'accès au compartiment](#)
- [Rôle IAM du cluster](#)
- [Audit et journalisation des accès Amazon S3](#)
- [Accès à AWS Glue ou Amazon Athena](#)

Politiques d'accès au compartiment

Vous pouvez contrôler l'accès aux données de vos compartiments Amazon S3 en utilisant d'une part une politique de compartiment associée au compartiment correspondant et d'autre part un rôle IAM associé au cluster.

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.

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 politique IAM bloquant l'utilisation des URL présignées Amazon S3 ne peut être mise en place. 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 politiques de compartiment qui incluent une `s3:signatureAge` action, veuillez à définir la valeur sur au moins 3 600 000 millisecondes.

L'exemple de politique de compartiment suivant autorise l'accès au compartiment spécifié uniquement à partir du trafic provenant de Redshift Spectrum détenu par AWS le compte. 123456789012

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "BucketPolicyForSpectrum",
    "Effect": "Allow",
    "Principal": {
      "AWS": ["arn:aws:iam::123456789012:role/redshift"]
    },
    "Action": ["s3:GetObject", "s3:List*"],
    "Resource": ["arn:aws:s3:::examplebucket/*"],
    "Condition": {
      "StringEquals": {
        "aws:UserAgent": "AWS Redshift/Spectrum"
      }
    }
  }]
}
```

Rôle IAM du cluster

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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```
}
```

Vous pouvez ajouter une politique au rôle du cluster afin d'empêcher l'accès de COPY et UNLOAD à un compartiment spécifique. La politique suivante autorise le trafic vers le compartiment défini uniquement à partir de Redshift Spectrum.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["s3:Get*", "s3:List*"],
    "Resource": "arn:aws:s3:::myBucket/*",
    "Condition": {"StringEquals": {"aws:UserAgent": "AWS Redshift/
Spectrum"}}
  ]
}
```

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 de blog sur la AWS 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 accède 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.

Pour activer l'accès à AWS Glue ou Athena, configurez votre VPC avec une passerelle Internet ou une passerelle NAT. Configurez vos groupes de sécurité VPC pour autoriser le trafic sortant vers les points de terminaison publics pour et Athena. AWS Glue Vous pouvez également configurer un point de terminaison VPC d'interface pour accéder AWS Glue à votre. AWS Glue Data Catalog Lorsque vous utilisez un point de terminaison d'interface VPC, la communication entre votre VPC et celui-ci AWS Glue s'effectue au sein du réseau. AWS Pour plus d'informations, consultez [Création d'un point de terminaison d'interface](#).

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, le cluster 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 .

Pour plus d'informations, consultez [Amélioration du routage VPC dans Amazon Redshift](#).

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.

Rubriques

- [Présentation](#)
- [Surveillance d'Amazon Redshift à l'aide de métriques CloudWatch](#)
- [Utilisation des données de performance dans la console Amazon Redshift](#)

Présentation

Les données de performance que vous pouvez utiliser dans la console Amazon Redshift se divisent en deux catégories :

- **CloudWatch Métriques Amazon** : CloudWatch les métriques Amazon vous aident 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 avec les métriques, par exemple avec le AWS CLI ou l'un des AWS SDK.
- **Données de performances de requête/de chargement** – 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 corréliser facilement ce que vous voyez dans les CloudWatch métriques avec des événements de requête et de chargement de base de données 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. Il n'est pas publié en tant que CloudWatch métrique.

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.
- Certains indicateurs de performance sont affichés dans des unités mieux dimensionnées dans la console Amazon Redshift par rapport à CloudWatch. Par exemple `WriteThroughput`, est affiché en Gbit/s (par rapport aux octets/s en entrée 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 performance (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 performance Amazon Redshift présentées sous forme de CloudWatch métriques, consultez [Qu'est-ce que c'est ? CloudWatch](#) dans le guide de CloudWatch l'utilisateur Amazon.

Surveillance d'Amazon Redshift à l'aide de métriques CloudWatch

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 du nœud. 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 métriques 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.

Title

Métrique	Description
<code>CommitQueueLength</code>	<p>Nombre de transactions en attente de validation à un moment donné dans le temps.</p> <p>Unités : nombre</p> <p>Dimensions : <code>ClusterIdentifier</code></p>
<code>ConcurrencyScalingActiveClusters</code>	<p>Nombre de clusters de mise à l'échelle de la simultanéité qui traitent activement des requêtes à un instant donné.</p>

Métrique	Description
	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	<p>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.</p> <div data-bbox="592 640 1507 1333" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Sur Amazon CloudWatch, cette métrique est signalée sous la forme 1 ou 0, tandis que dans la console Amazon Redshift, elle est affichée avec les mots HEALTHY ou UNHEALTHY pour des raisons de commodité. 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).</p></div> <p>Unités : nombre (1/0) (HEALTHY/UNHEALTHY dans la console Amazon Redshift)</p> <p>Dimensions : ClusterIdentifier</p>

Métrique	Description
MaintenanceMode	<p>Indique si le cluster est en mode maintenance.</p> <div data-bbox="591 302 1508 953" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Sur Amazon CloudWatch, cette métrique est signalée sous la forme 1 ou 0, tandis que dans la console Amazon Redshift, elle est affichée avec les mots ON ou OFF pour des raisons de commodité. 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).</p></div> <p>Unités : nombre (1/0) (ON/OFF dans la console Amazon Redshift).</p> <p>Dimensions : ClusterIdentifier</p>
MaxConfiguredConcurrencyScalingClusters	<p>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.</p> <p>Unités : nombre</p> <p>Dimensions : ClusterIdentifier</p>

Métrique	Description
NetworkReceiveThroughput	Débit auquel le nœud ou cluster reçoit des données. Unités : octets/seconde (Mo/s dans la console Amazon Redshift) Dimensions: ClusterIdentifier , NodeID Dimensions : ClusterIdentifier
NetworkTransmitThroughput	Débit auquel le nœud ou cluster écrit des données. Unités : octets/seconde (Mo/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 nœud unique. Unités : nombre/seconde Dimensions: ClusterIdentifier , latency Dimensions: ClusterIdentifier , wlmid

Métrique	Description
QueryDuration	<p>Durée moyenne pour exécuter une requête. Communiqué par intervalles de 5 minutes. Cette métrique n'est pas prise en charge sur les clusters à nœud unique.</p> <p>Unités : microsecondes</p> <p>Dimensions : ClusterIdentifier , NodeID, latency</p> <p>Dimensions: ClusterIdentifier , latency</p> <p>Dimensions : ClusterIdentifier , NodeID, wlmid</p>
QueryRuntimeBreakdown	<p>Durée totale des requêtes exécutées par étape de requête. Communiqué par intervalles de 5 minutes.</p> <p>Unités : millisecondes</p> <p>Dimensions : ClusterIdentifier, NodeID, scène</p> <p>Dimensions : ClusterIdentifier scène</p>
ReadIOPS	<p>Nombre moyen d'opérations de lecture de disque par seconde.</p> <p>Unités : nombre/seconde</p> <p>Dimensions: ClusterIdentifier , NodeID</p> <p>Dimensions : ClusterIdentifier</p>
ReadLatency	<p>Temps moyen nécessaire pour les opérations d'I/O de lecture de disque.</p> <p>Unités : secondes</p> <p>Dimensions: ClusterIdentifier , NodeID</p> <p>Dimensions : ClusterIdentifier</p>

Métrique	Description
ReadThroughput	<p>Nombre moyen d'octets lus sur le disque par seconde.</p> <p>Unités : octets (Go/s dans la console Amazon Redshift)</p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>NodeID</code></p> <p>Dimensions : <code>ClusterIdentifier</code></p>
RedshiftManagedStorageTotalCapacity	<p>Capacité de stockage géré totale.</p> <p>Unités : mégaoctets</p> <p>Dimensions : <code>ClusterIdentifier</code></p>
TotalTableCount	<p>Nombre de tables utilisateur créées à un moment spécifique. Ce total n'inclut pas les tables Amazon Redshift Spectrum.</p> <p>Unités : nombre</p> <p>Dimensions : <code>ClusterIdentifier</code></p>
WLMQueueLength	<p>Nombre de requêtes en attente d'entrée dans la file d'attente de gestion de la charge de travail (WLM).</p> <p>Unités : nombre</p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>service class</code></p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>QueueName</code></p>

Métrique	Description
WLMQueueWaitTime	<p>Temps total pendant lequel les requêtes attendent dans la file d'attente de gestion des charges de travail. Communiqué par intervalles de 5 minutes.</p> <p>Unités : millisecondes.</p> <p>Dimensions: ClusterIdentifiant , QueryPriority</p> <p>Dimensions: ClusterIdentifiant , wlmid</p> <p>Dimensions: ClusterIdentifiant , QueueName</p>
WLMQueriesCompletedPerSecond	<p>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 nœud unique.</p> <p>Unités : nombre/seconde</p> <p>Dimensions: ClusterIdentifiant , wlmid</p> <p>Dimensions: ClusterIdentifiant , QueueName</p>
WLMQueryDuration	<p>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 nœud unique.</p> <p>Unités : microsecondes</p> <p>Dimensions: ClusterIdentifiant , wlmid</p> <p>Dimensions: ClusterIdentifiant , QueueName</p>

Métrique	Description
WLMRunningQueries	<p>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.</p> <p>Unités : nombre</p> <p>Dimensions: ClusterIdentifiant , wlmid</p> <p>Dimensions: ClusterIdentifiant , QueueName</p>
WriteIOPS	<p>Nombre moyen d'opérations d'écriture par seconde.</p> <p>Unités : nombre/seconde</p> <p>Dimensions: ClusterIdentifiant , NodeID</p> <p>Dimensions : ClusterIdentifiant</p>
WriteLatency	<p>Temps moyen nécessaire pour les opérations d'I/O d'écriture de disque.</p> <p>Unités : secondes</p> <p>Dimensions: ClusterIdentifiant , NodeID</p> <p>Dimensions : ClusterIdentifiant</p>
WriteThroughput	<p>Nombre moyen d'octets écrits sur le disque par seconde.</p> <p>Unités : octets (Go/s dans la console Amazon Redshift)</p> <p>Dimensions: ClusterIdentifiant , NodeID</p> <p>Dimensions : ClusterIdentifiant</p>

Métrique	Description
SchemaQuota	<p>Quota configuré pour un schéma.</p> <p>Unités : mégaoctets</p> <p>Dimensions : ClusterIdentifier , Database, Schema</p> <p>Périodique/Push : Periodic</p> <p>Fréquence : 5 minutes</p> <p>Critères d'arrêt : schéma abandonné ou quota supprimé</p>
NumExceededSchemaQuotas	<p>Nombre de schémas avec des quotas dépassés.</p> <p>Unités : nombre</p> <p>Dimensions : ClusterIdentifier</p> <p>Périodique/Push : Periodic</p> <p>Fréquence : 5 minutes</p> <p>Critères d'arrêt : N/A</p>
StorageUsed	<p>Espace disque ou de stockage utilisé par un schéma.</p> <p>Unités : mégaoctets</p> <p>Dimensions : ClusterIdentifier , Database, Schema</p> <p>Périodique/Push : Periodic</p> <p>Fréquence : 5 minutes</p> <p>Critères d'arrêt : schéma abandonné ou quota supprimé</p>

Métrique	Description
PercentageQuotaUsed	<p>Pourcentage d'espace disque ou de stockage utilisé par rapport au quota de schéma configuré.</p> <p>Unités : pourcentage</p> <p>Dimensions : ClusterIdentifier , Database, Schema</p> <p>Périodique/Push : Periodic</p> <p>Fréquence : 5 minutes</p> <p>Critères d'arrêt : schéma abandonné ou quota supprimé</p>
UsageLimitAvailable	<p>En fonction de FeatureType, UsageLimitAvailable renvoie ce qui suit :</p> <ul style="list-style-type: none"> • Si tel FeatureType est le casCONCURRENCY_SCALING , UsageLimitAvailable renvoie le temps total qui peut être utilisé par la mise à l'échelle simultanée par incréments d'une minute. • Si tel FeatureType est le casCROSS_REGION_DATAS HARING , UsageLimitAvailable renvoie la quantité totale de données pouvant être numérisées par incréments de 1 To. • Si tel FeatureType est le casSPECTRUM, UsageLimitAvailable renvoie la quantité totale de données pouvant être numérisées par incréments de 1 To. <p>Unités : minutes ou To</p> <p>Dimensions : ClusterIdentifier , FeatureType , UsageLimitId</p>

Métrique	Description
UsageLimitConsumed	<p>En fonction de FeatureType, UsageLimitConsumed renvoie ce qui suit :</p> <ul style="list-style-type: none"> • Si tel FeatureType est le casCONCURRENCY_SCALING , UsageLimitAvailable renvoie le temps total utilisé par la mise à l'échelle de la simultanéité par incréments d'une minute. • Si tel FeatureType est le casCROSS_REGION_DATAS HARING , UsageLimitAvailable renvoie la quantité totale de données numérisées par incréments de 1 To. • Si tel FeatureType est le casSPECTRUM, UsageLimitAvailabl e renvoie la quantité totale de données numérisées par incréments de 1 To. <p>Unités : minutes ou To</p> <p>Dimensions : ClusterIdentifier , FeatureType , UsageLimitId</p>

Dimensions des métriques Amazon Redshift

Les données Amazon Redshift peuvent être filtrées selon n'importe quelle dimension dans le tableau suivant.

Dimension	Description
latency	<p>Les valeurs possibles sont les suivantes :</p> <ul style="list-style-type: none"> • short – moins de 10 secondes • medium – entre 10 secondes et 10 minutes • long – plus de 10 minutes
NodeID	<p>Les filtres ont demandé des données spécifiques aux nœuds d'un cluster. NodeID a la valeur « Principal », « Partagé » ou « Calcul-N » où N est égal à 0, 1, ... pour le nombre de nœuds</p>

Dimension	Description
	<p>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.</p> <p>Les métriques pour <code>CPUUtilization</code> , <code>NetworkTransmitThroughput</code> et <code>ReadIOPS</code> sont communiquées uniquement pour le nœud principal et les nœuds de calcul. Les autres métriques qui utilisent la dimension <code>NodeId</code> sont communiquées uniquement pour les nœuds de calcul.</p>
<code>ClusterIdentifier</code>	<p>Les filtres ont demandé des données spécifiques au cluster. Les métriques spécifiques aux clusters incluent <code>HealthStatus</code> , <code>MaintenanceMode</code> et <code>DatabaseConnections</code> . Les métriques générales de cette dimension (par exemple <code>ReadIOPS</code>) 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.</p>
<code>service class</code>	Identifiant d'une classe de service WLM.

Dimension	Description
stage	<p>Étapes de l'exécution d'une requête. Les valeurs possibles sont les suivantes :</p> <ul style="list-style-type: none"> • 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 de la 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 CONCURRENTLY_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 des requêtes et des chargements. 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 performance des requêtes et des chargements ne sont pas publiées sous forme de CloudWatch métriques 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.

Données de chargement et de requête	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.

Données de chargement et de requête	Description
Détails de la requête	<p>Fournit des détails sur une requête donnée, notamment :</p> <ul style="list-style-type: none">• 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	<p>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.</p>
Détails de charge	<p>Fournit des détails sur une opération de charge particulière, notamment :</p> <ul style="list-style-type: none">• 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 chargement (pour de plus amples informations, consultez Affichage de l’historique des requêtes).

Utilisation des données de performance dans la console Amazon Redshift

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 performance (voir [Surveillance d'Amazon Redshift à l'aide de métriques CloudWatch](#)), vous pouvez également les utiliser CloudWatch pour personnaliser davantage vos graphiques de mesures. Par exemple, vous pouvez choisir des durées plus longues ou combiner des métriques de plusieurs clusters. Pour plus d'informations sur l'utilisation de la CloudWatch console, consultez [Utilisation des indicateurs 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 requêtes et des charges](#)
- [Affichage des métriques du cluster pendant les opérations de chargement](#)
- [Analyse des performances de la charge de travail](#)
- [Gérer les alarmes](#)
- [Utilisation des indicateurs de performance dans la CloudWatch console](#)

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

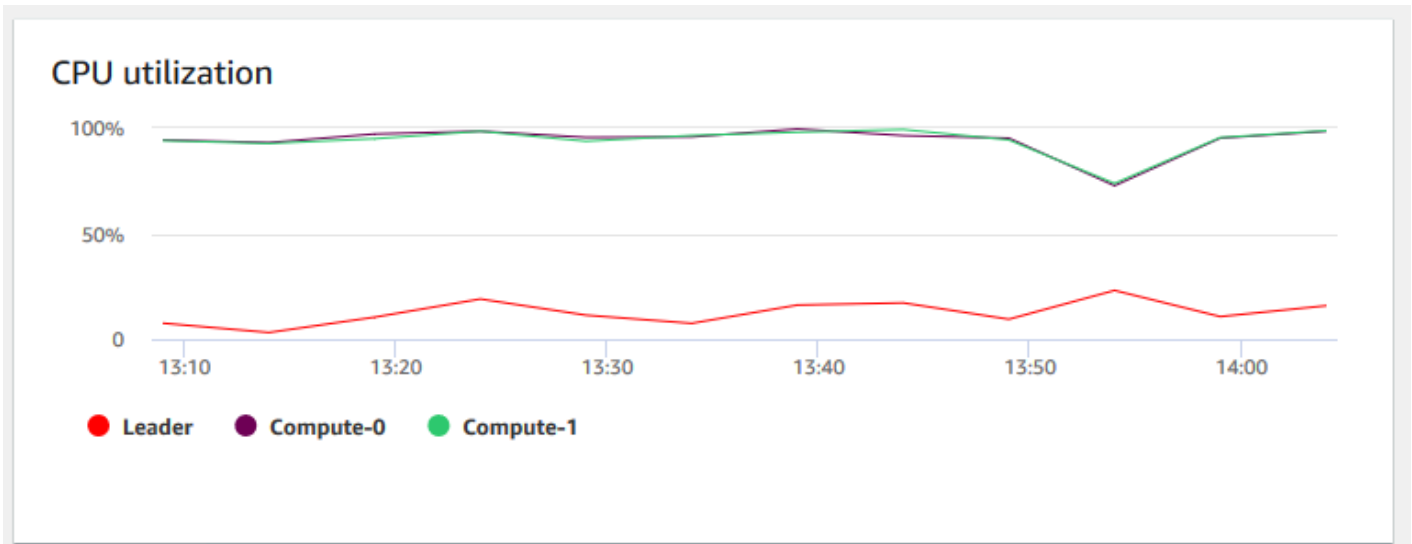
1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dans le menu de navigation, choisissez Clusters, puis choisissez le nom d'un cluster dans la liste pour ouvrir ses détails. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Datashares, 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.

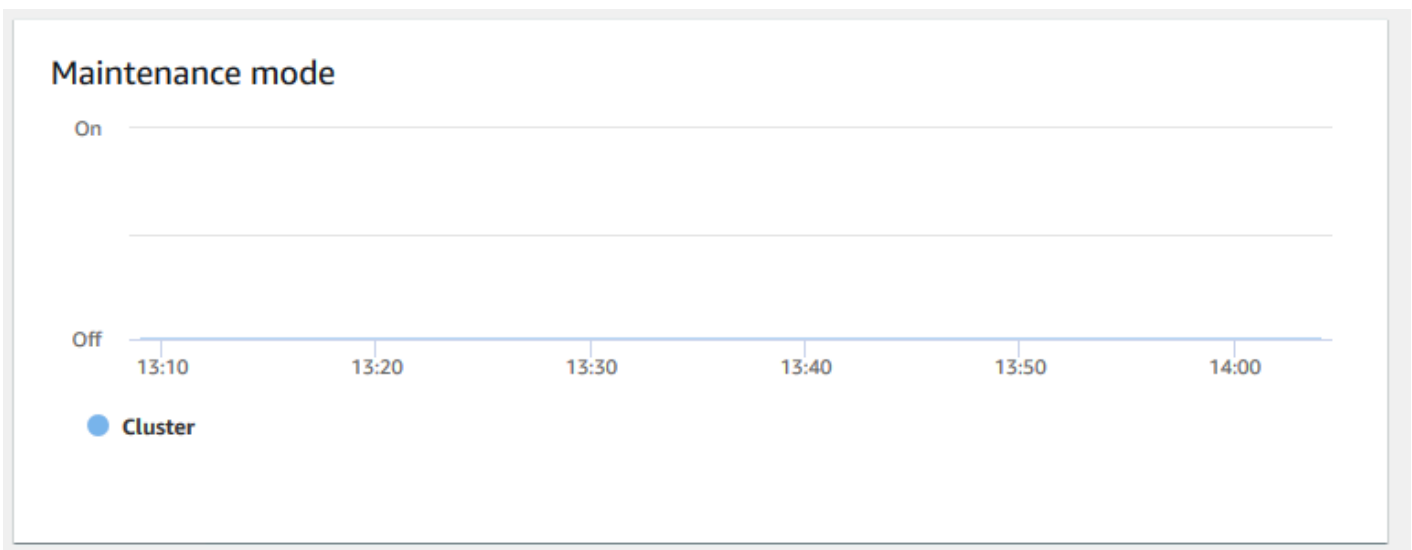
Graphiques de performances de cluster

Les exemples suivants illustrent certains des graphiques affichés dans la nouvelle console Amazon Redshift.

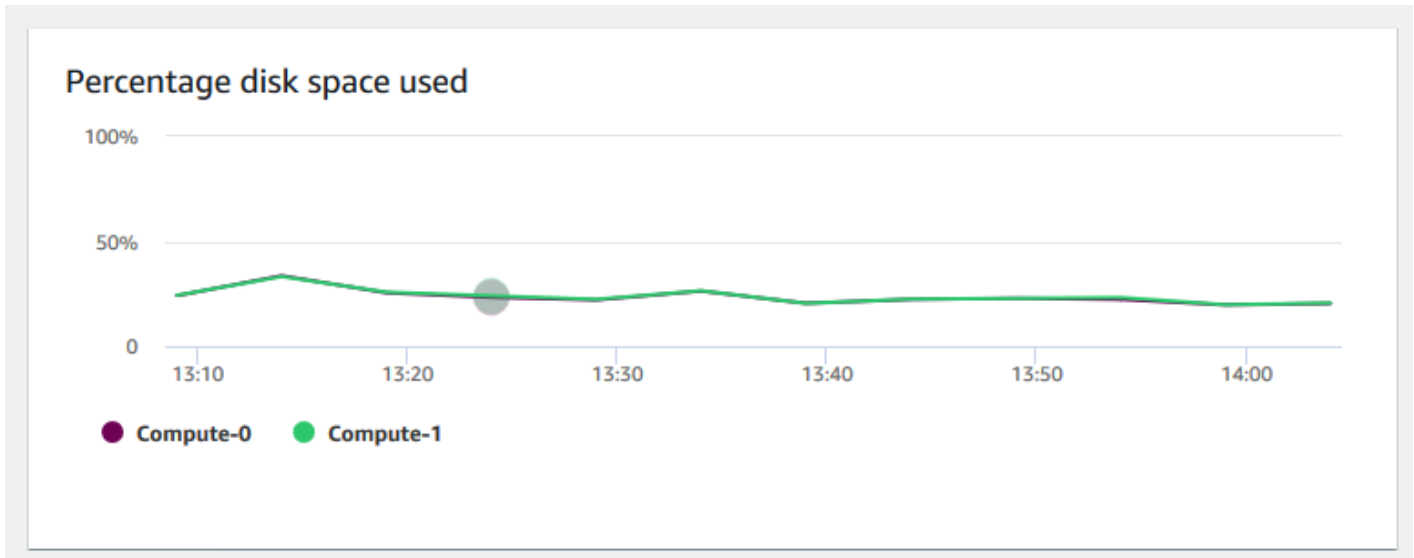
- **Utilisation du CPU** – Indique le pourcentage d'utilisation du CPU pour tous les nœuds (principal et calcul). Pour trouver une heure où l'utilisation du cluster est la plus faible avant de planifier la migration du cluster ou d'autres opérations consommant des ressources, surveillez ce graphique pour voir l'utilisation de l'UC par individu ou tous les nœuds.



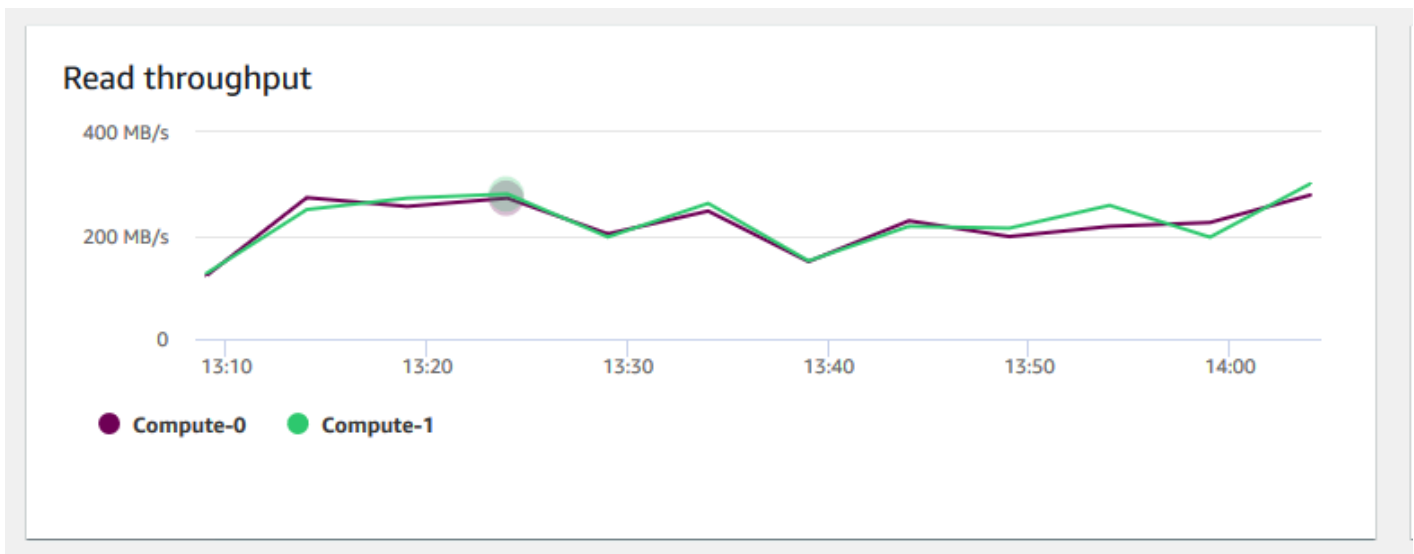
- **Mode maintenance** – Indique si le cluster est en mode maintenance à un moment donné à l'aide des indicateurs On et Off. Vous pouvez voir l'heure à laquelle le cluster est en cours de maintenance. Vous pouvez ensuite mettre en corrélation cette fois avec les opérations effectuées sur le cluster afin d'estimer ses temps d'arrêt futurs pour les événements récurrents.



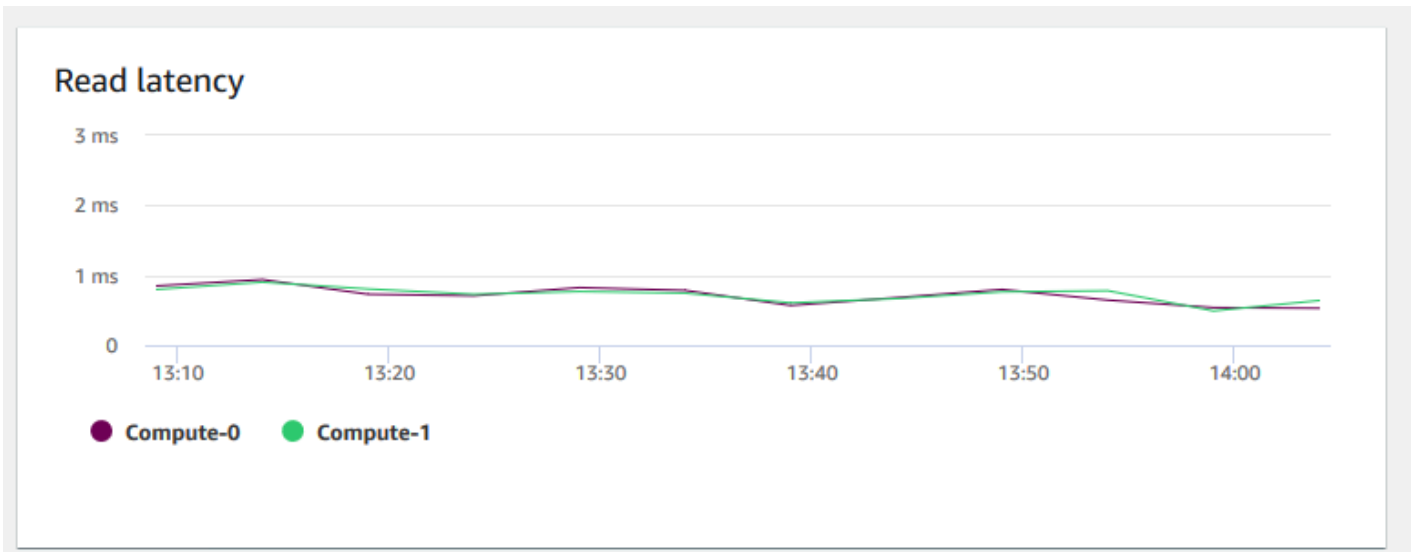
- **Pourcentage d'espace disque utilisé** – Indique le pourcentage d'utilisation de l'espace disque pour chaque nœud de calcul, et non pour le cluster dans son ensemble. Vous pouvez explorer ce graphique pour surveiller l'utilisation du disque. Les opérations de maintenance telles que VACUUM et COPY 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.



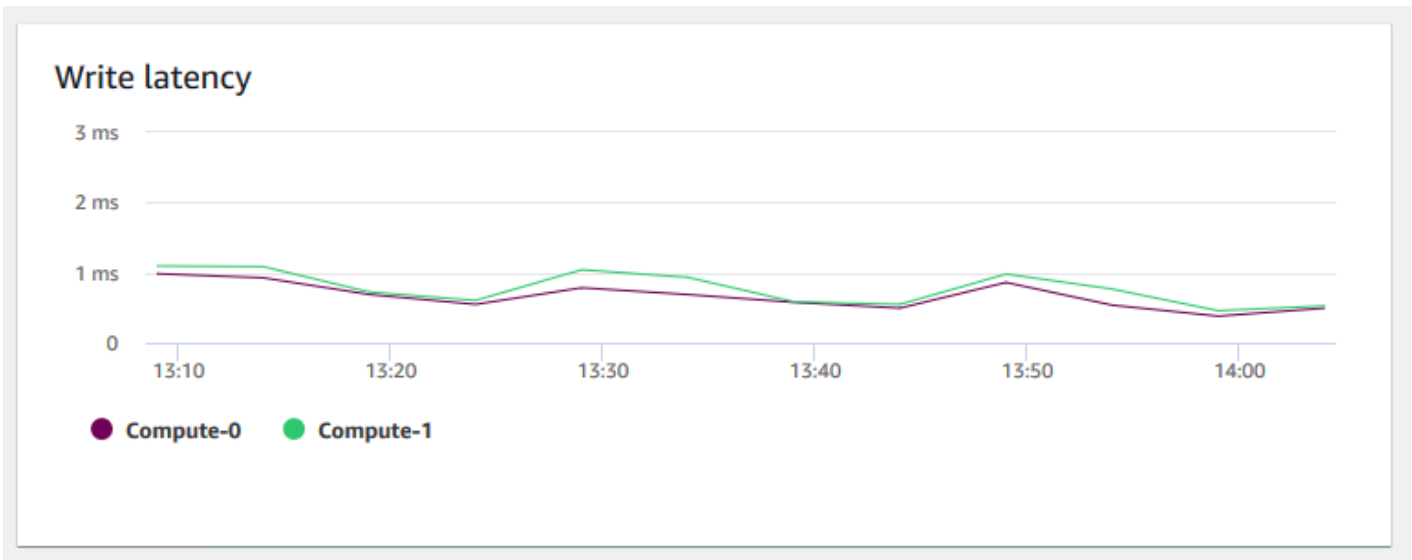
- **Latence de lecture** – Indique la durée moyenne des opérations d'I/O de lecture de disque par milliseconde. Vous pouvez afficher les temps de réponse pour que les données reviennent. Lorsque la latence est élevée, cela signifie que l'expéditeur passe plus de temps inactif (sans envoyer de nouveaux paquets), ce qui réduit la vitesse de croissance du débit.



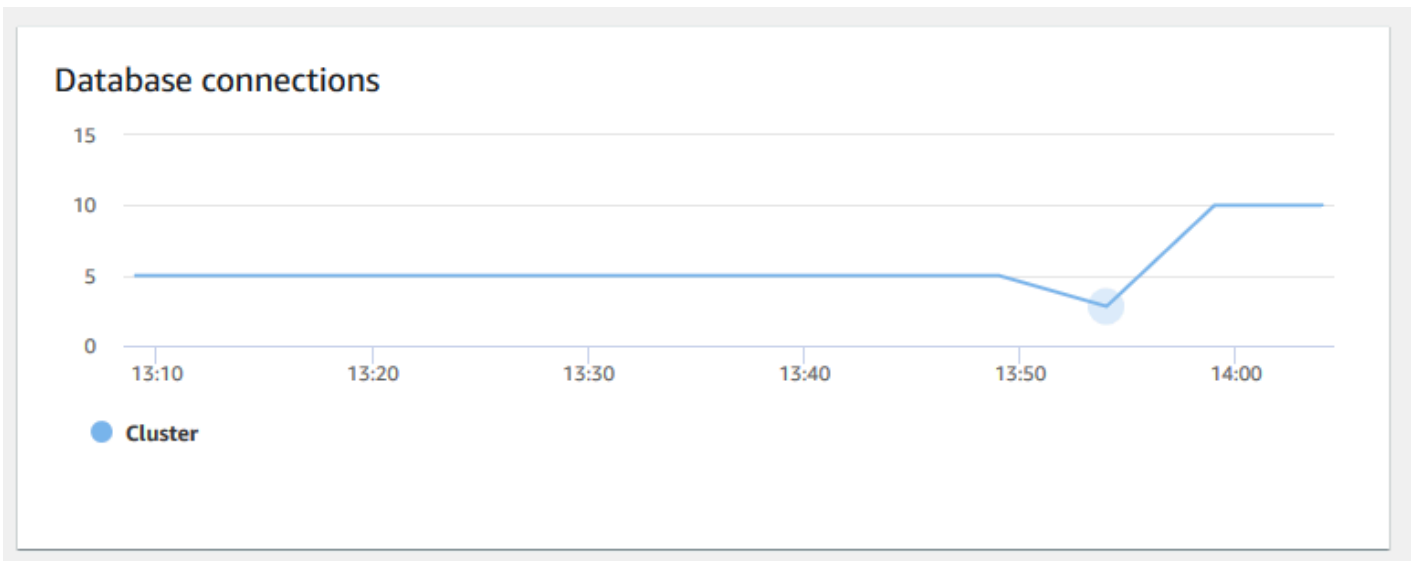
- Débit d'écriture – Indique le nombre moyen de mégaoctets écrits sur le disque par seconde. Vous pouvez évaluer cette métrique pour surveiller l'aspect physique correspondant du cluster. Ce débit n'inclut pas le trafic réseau entre les instances du cluster et le volume de cluster.



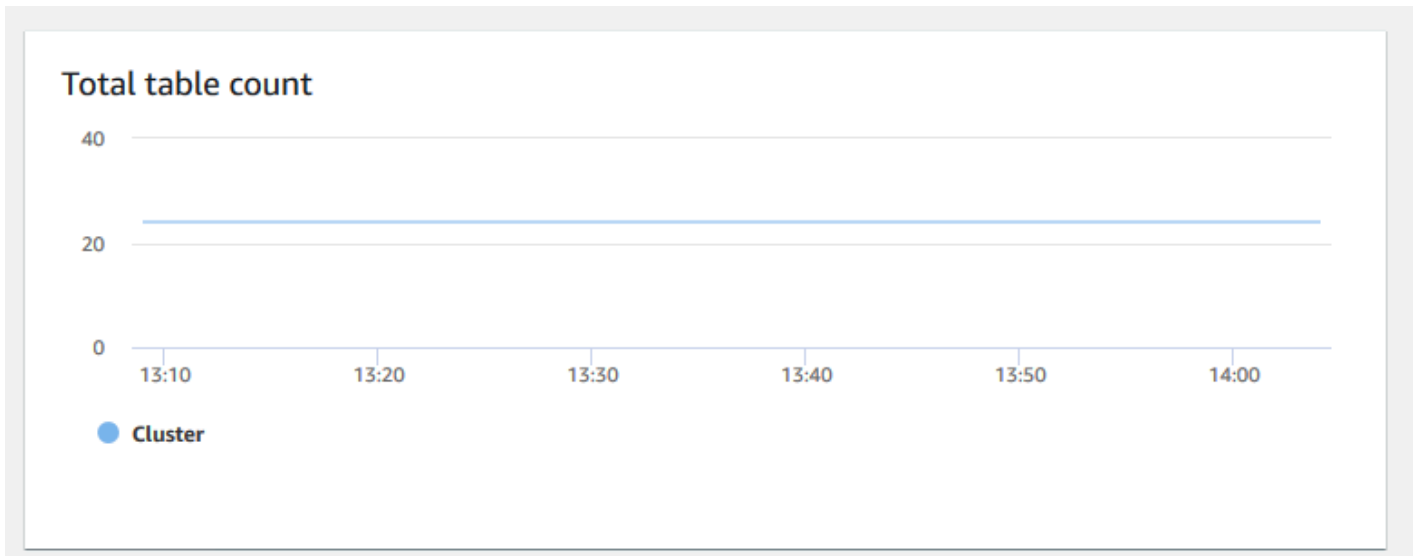
- Latence d'écriture – Indique la durée moyenne en millisecondes des opérations d'I/O d'écriture sur disque. Vous pouvez évaluer le temps de retour de l'accusé de réception d'écriture. Lorsque la latence est élevée, cela signifie que l'expéditeur passe plus de temps inactif (sans envoyer de nouveaux paquets), ce qui réduit la vitesse de croissance du débit.



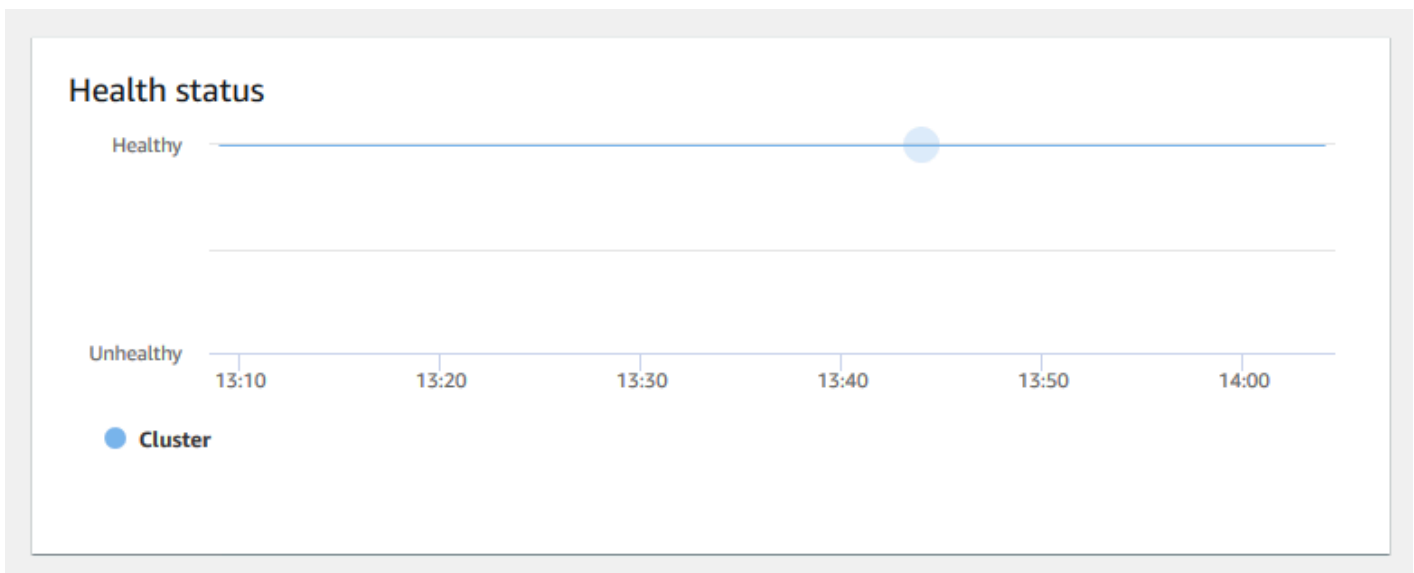
- **Connexions à la base de données** – Indique le nombre de connexions à la base de données d'un cluster. Vous pouvez utiliser ce graphique pour voir le nombre de connexions établies à la base de données et trouver une heure où l'utilisation du cluster est la plus faible.



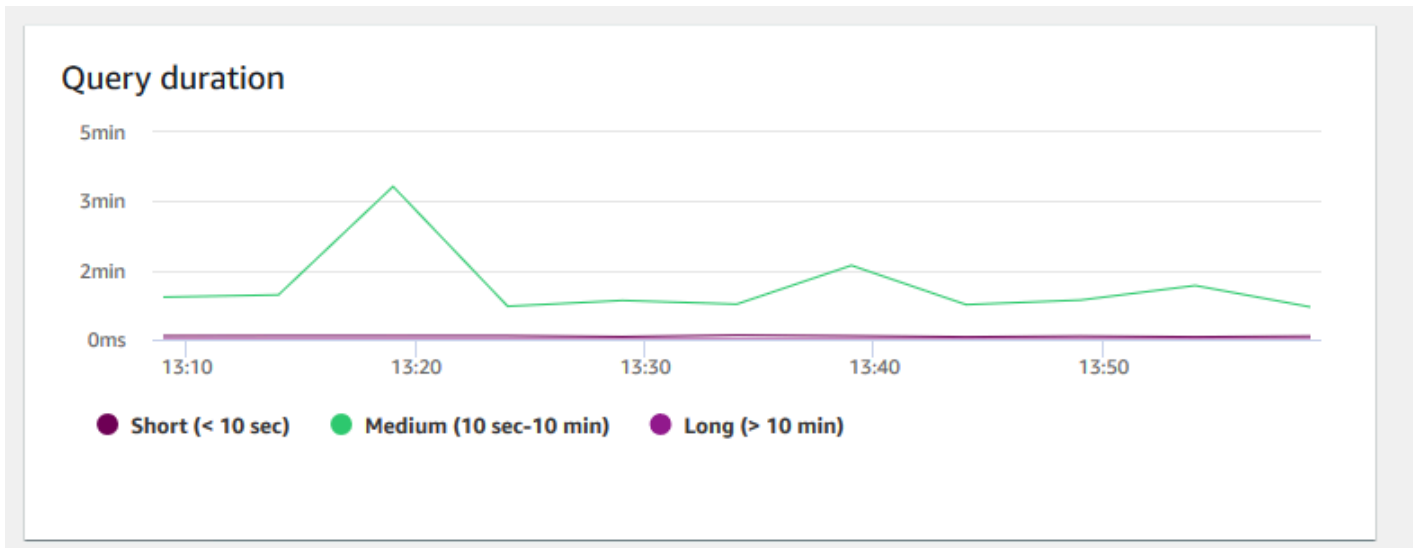
- **Nombre total de tables** – Indique le nombre de tables utilisateur ouvertes à un moment donné dans un cluster. Vous pouvez surveiller les performances du cluster lorsque le nombre de tables ouvertes est élevé.



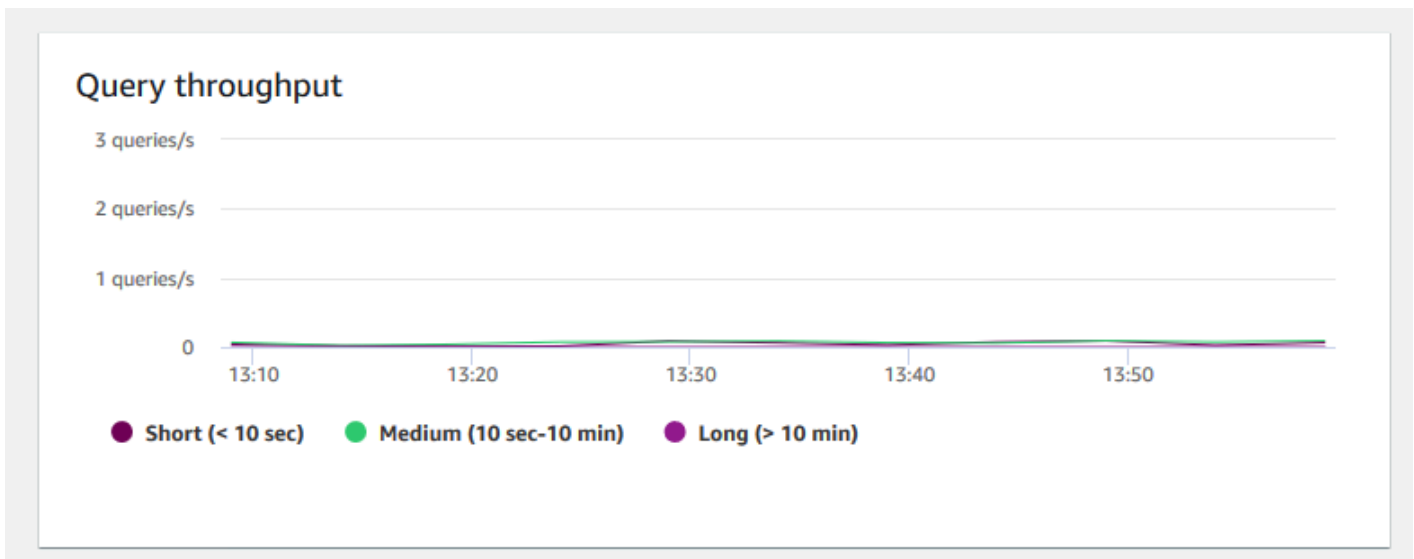
- **État d'intégrité** – Indique l'état d'intégrité du cluster comme Healthy ou Unhealthy. Si le cluster peut se connecter à sa base de données et exécuter une requête simple avec succès, le cluster est considéré comme sain. Sinon, le cluster est défectueux. Un état défectueux peut se produire lorsque 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.



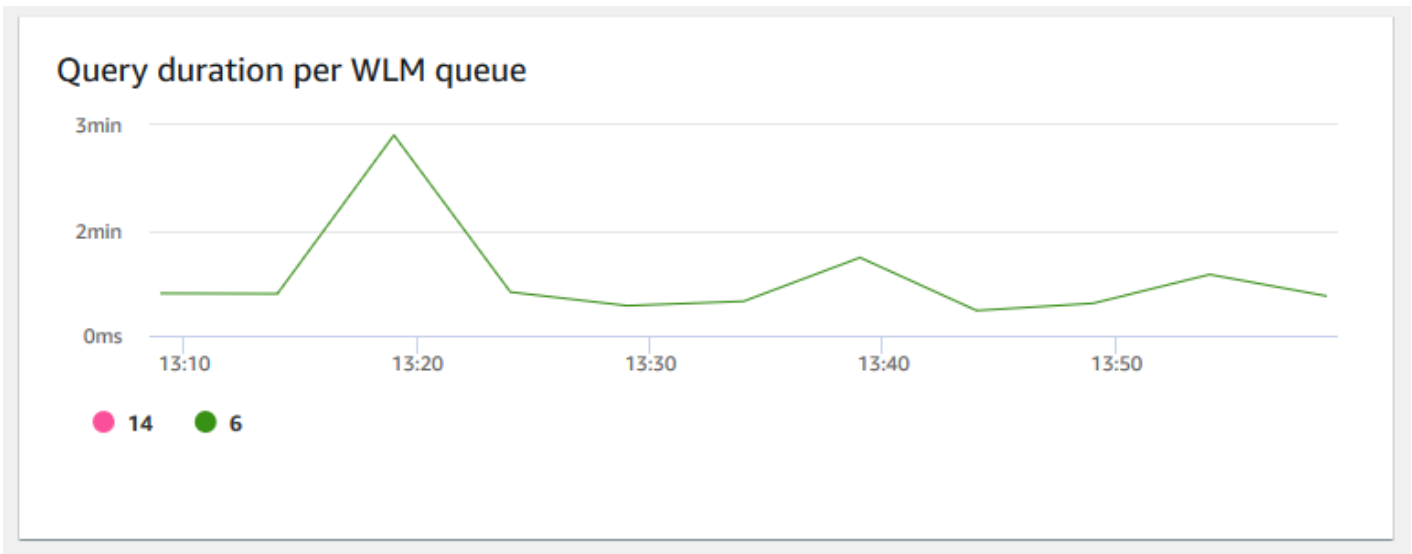
- **Durée de la requête** – Indique la durée moyenne d'exécution d'une requête en microsecondes. Vous pouvez comparer les données de ce graphique pour mesurer les performances d'I/O au sein du cluster et régler ses requêtes les plus longues si nécessaire.



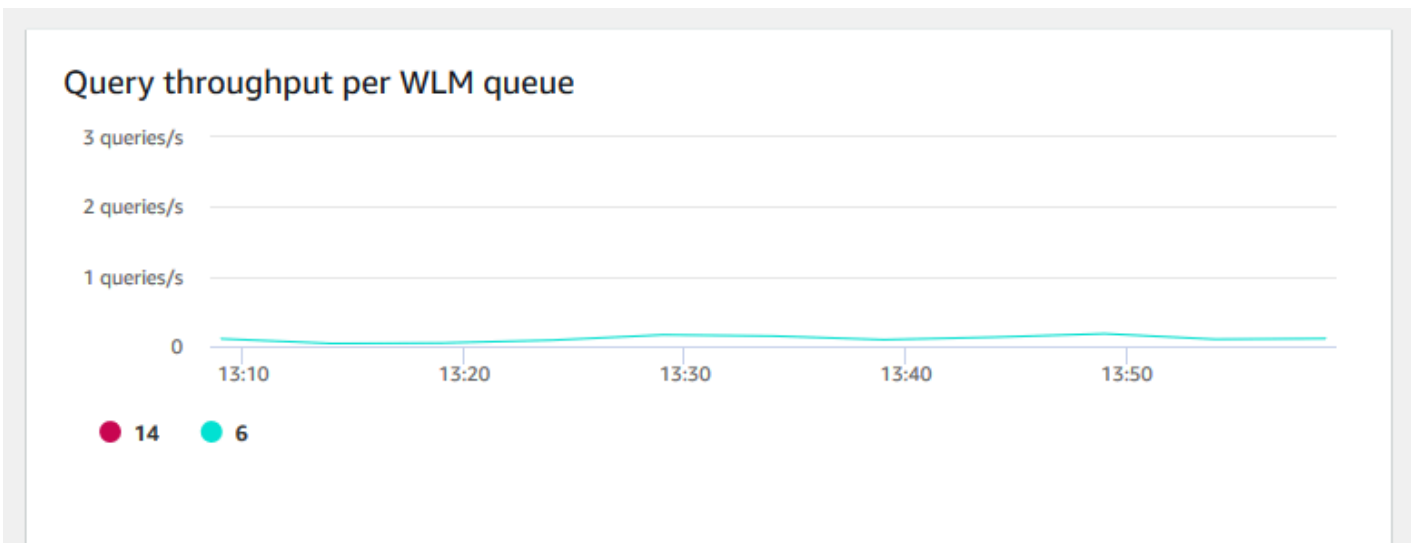
- Débit des requêtes – Indique le nombre moyen de requêtes terminées par seconde. Vous pouvez analyser les données de ce graphique pour mesurer les performances de la base de données et caractériser la capacité du système à traiter une charge de travail multiutilisateur de manière équilibrée.



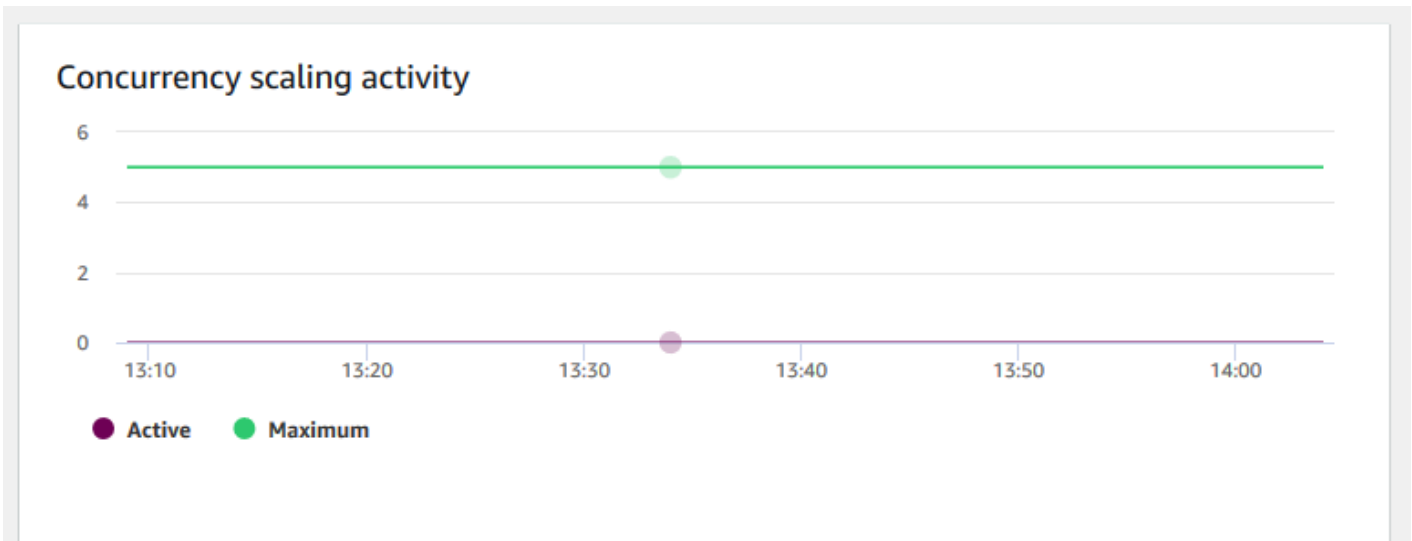
- Durée de la requête par file d'attente WLM – Indique la durée moyenne d'exécution d'une requête en microsecondes. Vous pouvez comparer les données de ce graphique pour mesurer les performances d'I/O par file d'attente WLM et régler ses requêtes les plus longues si nécessaire.



- 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 des détails de la requête](#).
- 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Datashares, 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.
- Requetes 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.

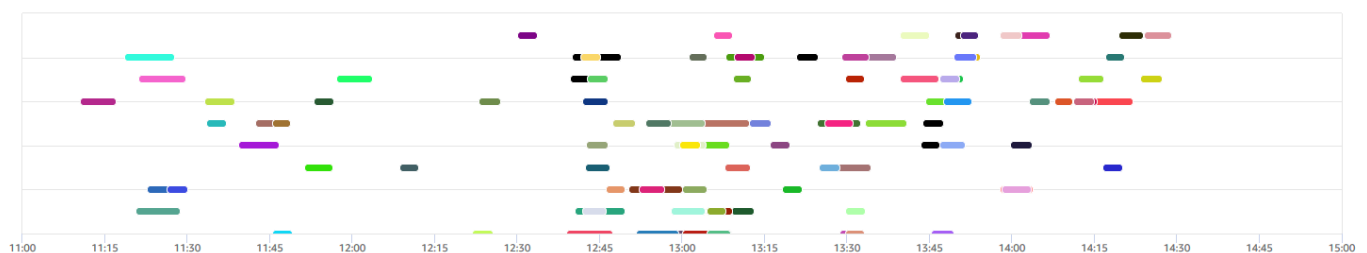
Note

Les graphiques de la console Amazon Redshift ne contiennent que les données des 100 000 requêtes les plus récentes.

Exécution de requête

Query runtime

The query activity on a timeline. Use this graph to see which queries are running in the same timeframe. Choose a query to view more query execution details.



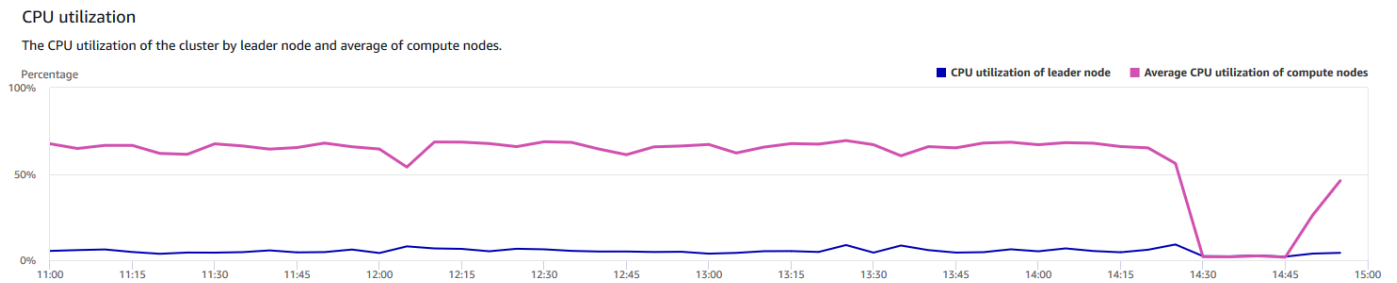
Requêtes et charges

Queries and loads(100) Terminate query

Filter queries

<input type="checkbox"/>	Start time	Query	Status	Duration	SQL	Copy SQL	User	Transaction ID
<input type="checkbox"/>	Apr 13th, 2020 01:00:55 PM 8 days ago	69248	Completed	11 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105501
<input type="checkbox"/>	Apr 13th, 2020 12:58:07 PM 8 days ago	69199	Completed	11 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105414
<input type="checkbox"/>	Apr 13th, 2020 12:54:15 PM 8 days ago	69111,69265,69253	Completed	10 min	with /* query_templates/query22.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105283
<input type="checkbox"/>	Apr 13th, 2020 12:50:17 PM 8 days ago	68976	Completed	10 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105128
<input type="checkbox"/>	Apr 13th, 2020 01:29:23 PM 8 days ago	70089	Completed	10 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	106659
<input type="checkbox"/>	Apr 13th, 2020 11:18:35 AM 8 days ago	65543	Completed	9 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_05cu_run01_nocache.stream-quer ...	Copy	rsperf	101092
<input type="checkbox"/>	Apr 13th, 2020 12:40:30 PM 8 days ago	68729	Completed	9 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	104789

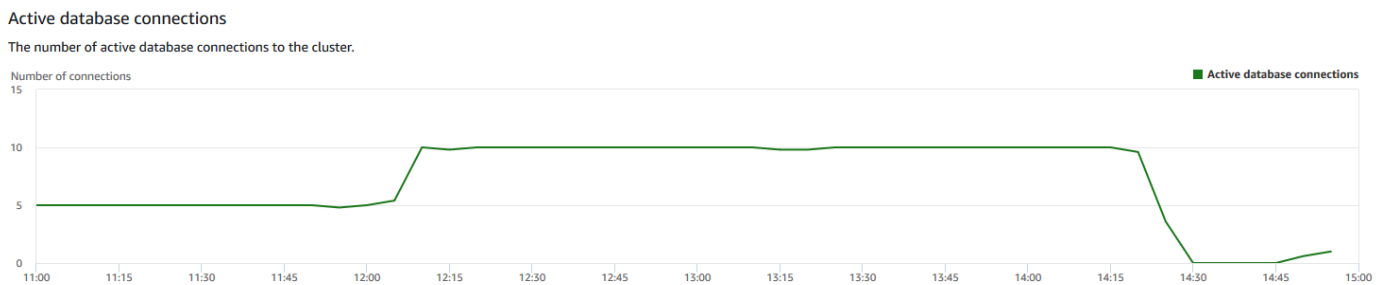
• Utilisation de l'UC



• 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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. 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.

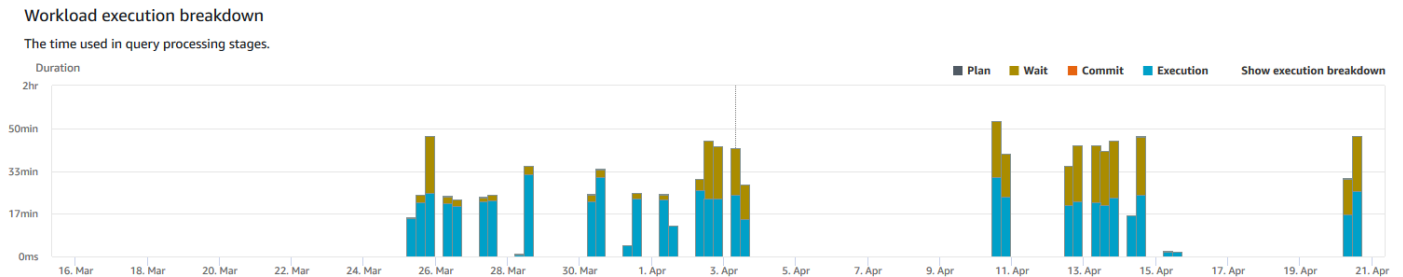
Lorsque vous choisissez des métriques de file d’attente WLM, l’onglet inclut les graphiques suivants :

- **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.

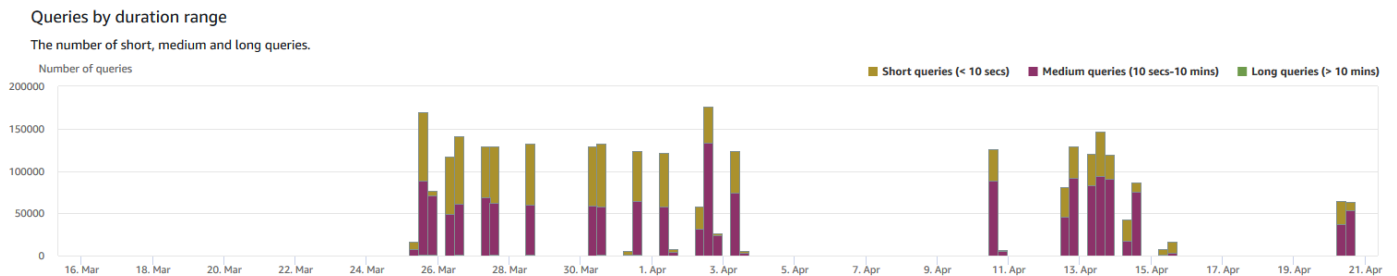
Graphiques de performances de base de données

Les exemples suivants illustrent les graphiques qui s’affichent dans la nouvelle console Amazon Redshift.

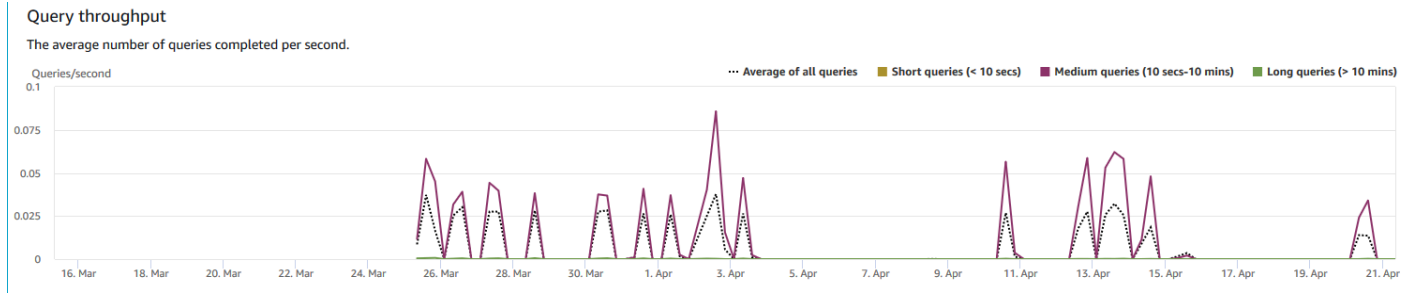
- **Répartition de l’exécution de la charge de travail**



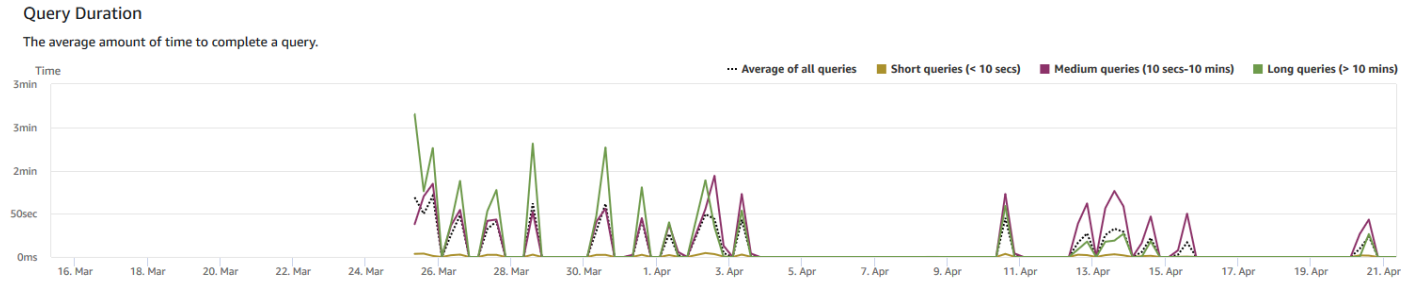
- **Requêtes par plage de durée**



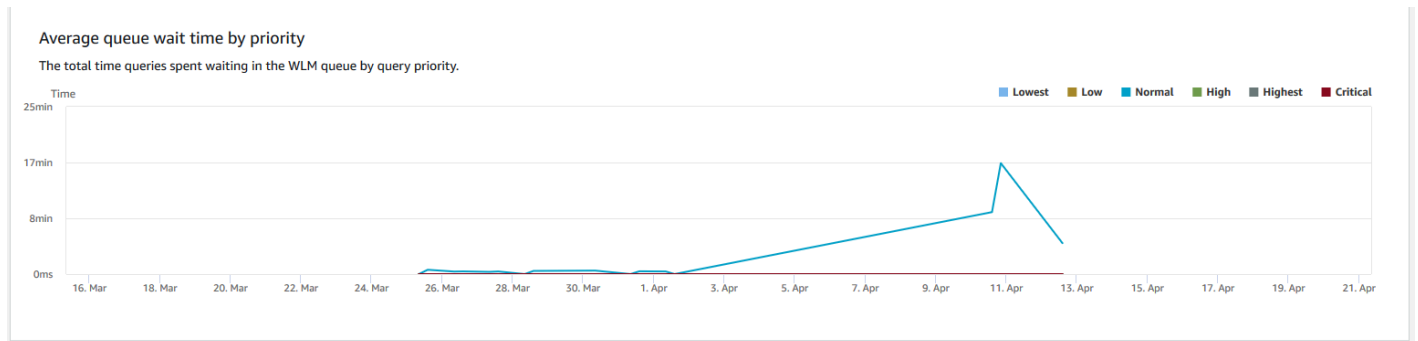
- **Débit de requête**



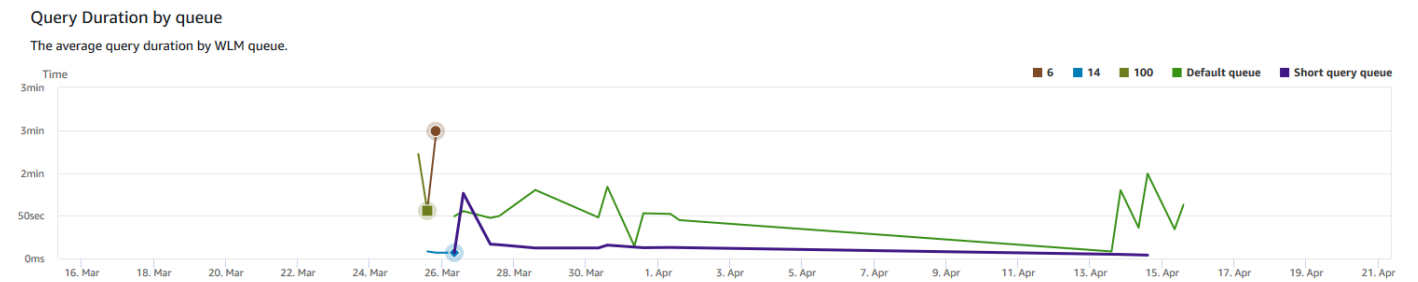
- **Durée de requête**



- **Temps d'attente moyen par priorité**



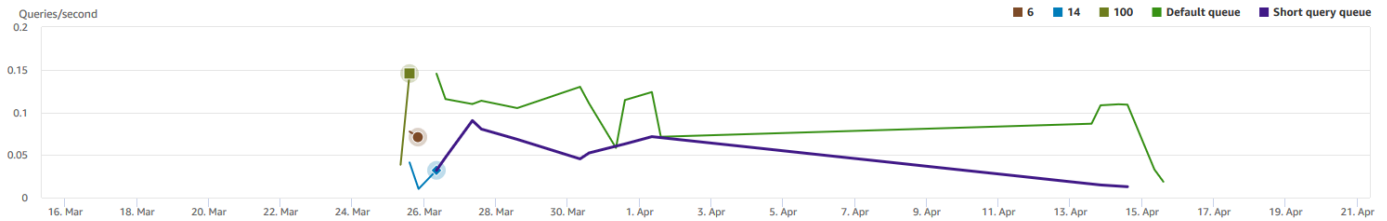
- **Durée de la requête par file d'attente**



- **Débit de requête par file d'attente**

Query throughput by queue

The average number of queries completed per second by WLM queue.



- Interroger le temps d'attente par file d'attente

Query wait time by queue

The average duration of queries spent waiting by WLM queue.



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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](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. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Datashares, 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.
- Requetes 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.

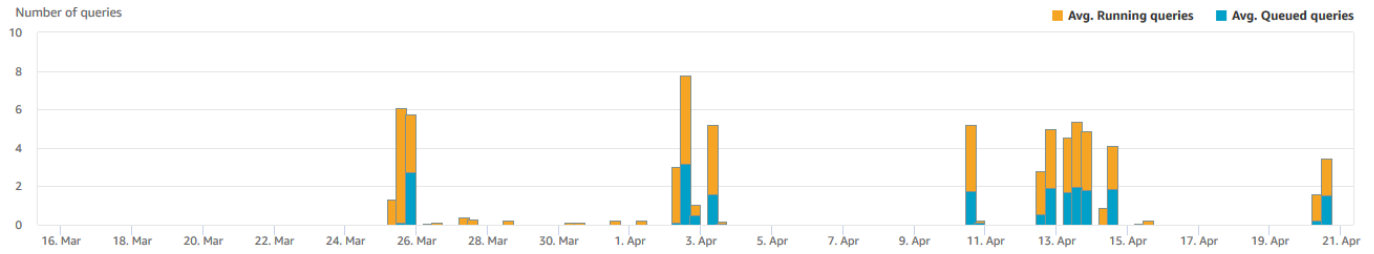
Graphiques de simultanéité des charges de travail

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 le dimensionnement de la simultanéité et les métriques WLM CloudWatch . Pour plus d'informations sur CloudWatch les métriques pour Amazon Redshift, consultez. [Surveillance d'Amazon Redshift à l'aide de métriques CloudWatch](#)

- Requetes en attente ou en cours d'exécution sur le cluster

Queued vs. Running queries on the cluster

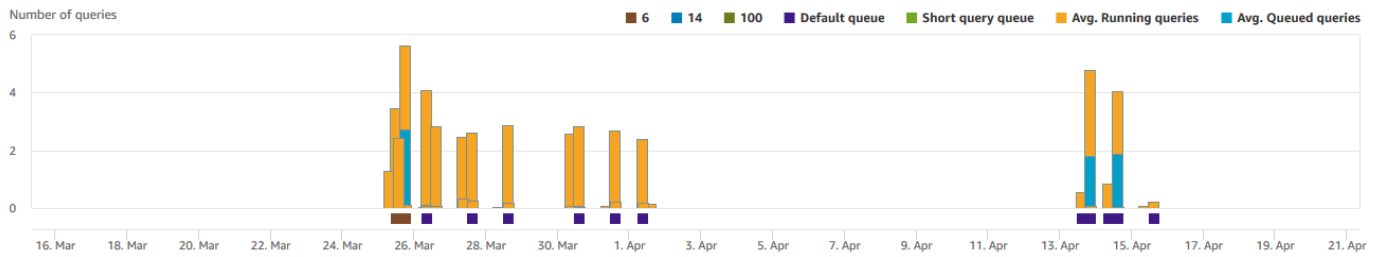
The number of queries running (from the main cluster and concurrency scaling cluster) compared to the number of queries waiting in all WLM queues in the cluster.



- Mise en file d'attente ou exécution de requêtes par file d'attente

Queued vs. Running queries per queue

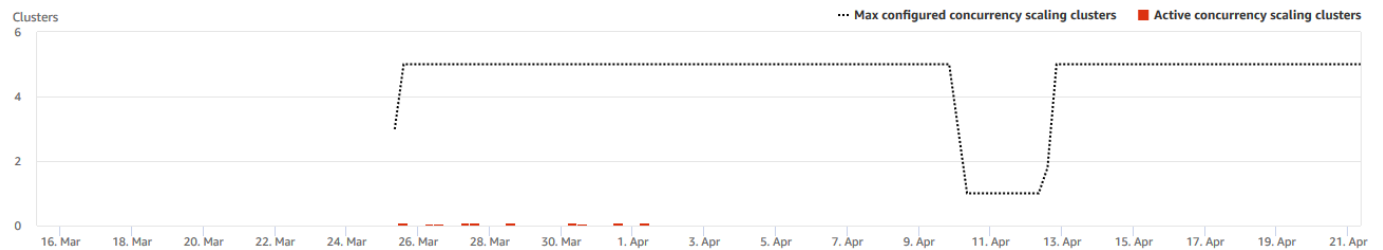
The number of queries running (from the main cluster and concurrency scaling cluster) compared to the number of queries waiting in each WLM queue.



- Activité de mise à l'échelle de simultanéité

Concurrency scaling activity

The number of concurrency scaling clusters that are actively processing queries.

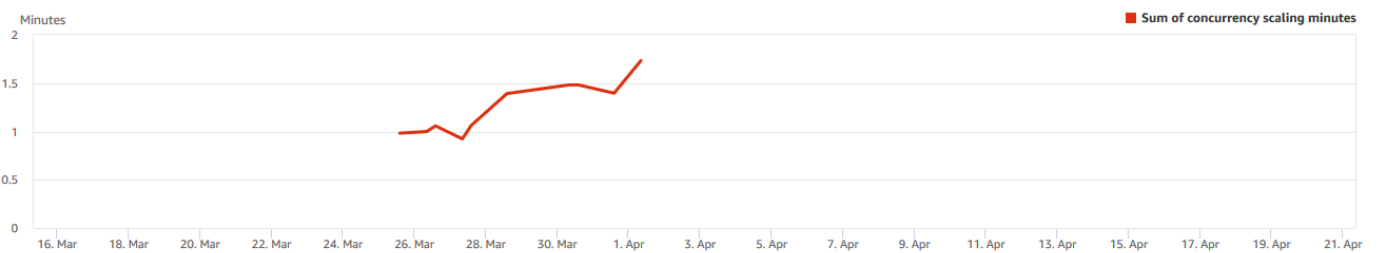


- Utilisation de la mise à l'échelle de la simultanéité

Concurrency scaling usage

The usage of concurrency scaling clusters that have active query processing activity.

Total usage: 12.51 mins ⓘ



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 goulots 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
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.

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 `redshift:CancelQuerySessionaction` à votre politique AWS Identity and Access Management (IAM). Cette exigence s'applique que vous sélectionniez la politique AWS gérée Amazon Redshift Read Only 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
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.

Affichage des détails de la requête

Vous pouvez analyser les détails de la requête sur la console Amazon Redshift. 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
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.

Analyse de l'exécution des requêtes

Pour analyser une requête

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dans le menu de navigation, choisissez Requetes 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 Requete 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.

Rewritten queries(5) <small>This query was rewritten by Amazon Redshift for optimization</small>						
	Start time ▲	Query ▼	Status ▼	Duration ▼	Executed on ▼	Query type ▼
<input type="radio"/>	Apr 15th, 2020 01:44:44 PM 6 days ago	122927,122928,122929...	✔ Completed	5 min		Parent query
<input checked="" type="radio"/>	Apr 15th, 2020 01:44:44 PM 6 days ago	122927	✔ Completed	4 sec	Main	Rewritten query
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122928	✔ Completed	22 ms	Main	Rewritten query
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122929	✔ Completed	19 ms	Main	Rewritten query
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122931	✔ Completed	5 min	Main	Rewritten query

- Une section Détails de la requête comme illustré dans la capture d'écran suivante.

Query details				
Query ID 122927	Cluster dnd-sudhare-qa	User	Type Rewritten query	Status Completed
From April 15, 2020 at 01:44:44 PM To April 15, 2020 at 01:44:48 PM				Total runtime 4sec

- 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

Cluster health status

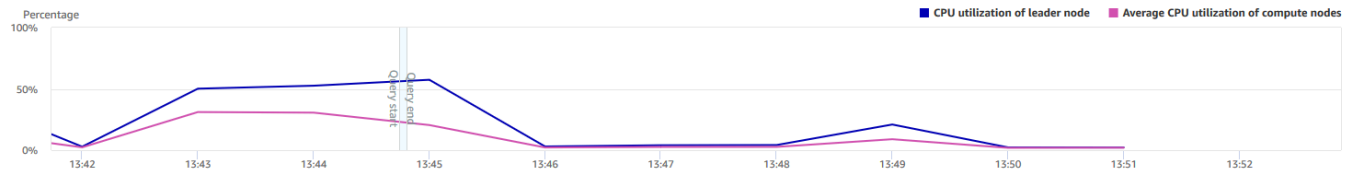
Cluster health during the workload.



- Utilisation de l'UC

CPU utilization

The CPU utilization of the cluster by leader node and average of compute nodes.



- Capacité de stockage utilisée

Storage capacity used

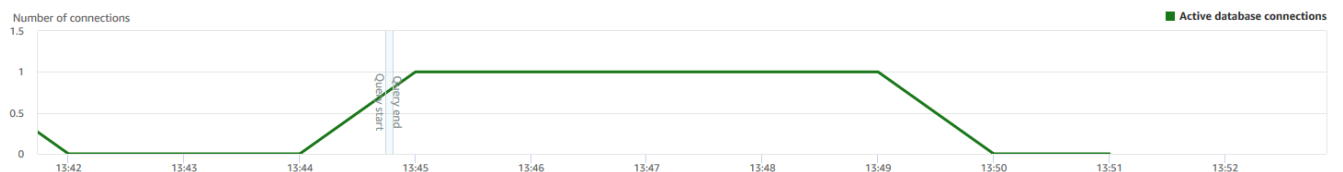
The percent of the storage capacity used.



- Connexions actives à la base de données

Active database connections

The number of active database connections to the cluster.



Afficher les performances de cluster pendant l'exécution des requêtes

Pour afficher les performances de cluster pendant l'exécution des requêtes

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Datashares, 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 `redshift:CancelQuerySessionaction` à votre politique AWS Identity and Access Management (IAM). Cette exigence s'applique que vous sélectionniez la politique AWS gérée par Amazon Redshift Read Only 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 la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Datashares, 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.

Analyse des performances de la charge de travail

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

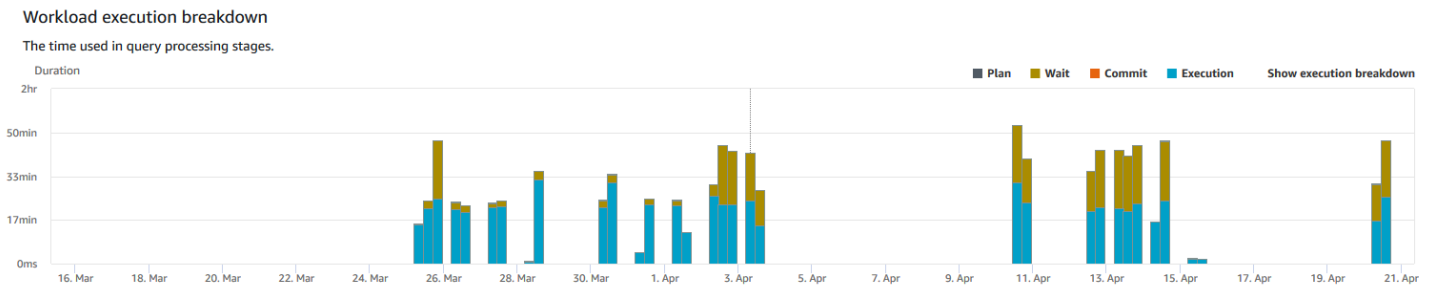
Le graphique de répartition de l'exécution de la charge de travail n'est pas affiché pour les clusters à nœud unique.

La liste de métriques suivante décrit les caractéristiques les différentes étapes du traitement :

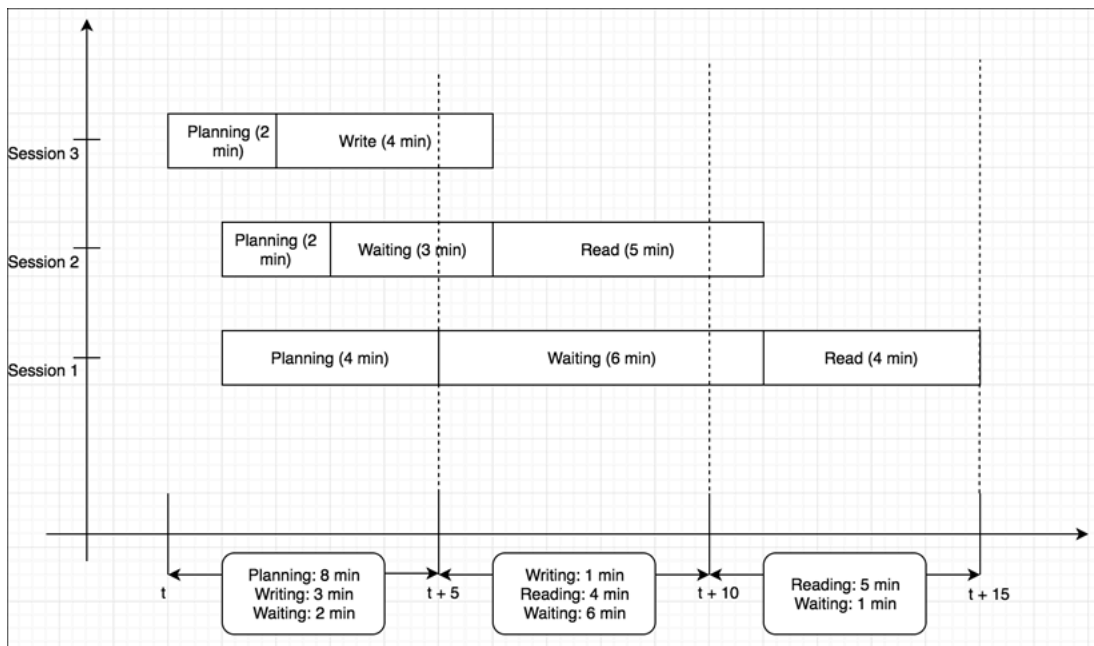
- `QueryPlanning` : Temps passé à analyser et à optimiser les instructions SQL.
- `QueryWaiting` : Temps passé dans la file d'attente de gestion de la charge de travail (WLM).
- `QueryExecutingRead` : Temps passé à exécuter des requêtes en lecture.
- `QueryExecutingInsert` : Temps passé à exécuter des 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 le graphique de répartition des charges de travail

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Datashares, 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

Gérer les alarmes

Les alarmes que vous créez dans la console Amazon Redshift sont CloudWatch des 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 [Surveillance d'Amazon Redshift à l'aide de métriques CloudWatch](#) . 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 Slack ou Slack à partir de laquelle envoyer une alerte CloudWatch à Slack ou Amazon Chime en spécifiant une URL de webhook Slack ou Amazon Chime.

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 avec le AWS CLI ou un AWS SDK.

Pour créer une CloudWatch alarme avec la console Amazon Redshift

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)

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.

Utilisation des indicateurs 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 CloudWatch contiennent des unités différentes de celles utilisées dans la console Amazon Redshift. Par exemple, elle `WriteThroughput` est affichée en Gbit/s (par rapport aux octets/s en entrée CloudWatch), qui est une unité plus pertinente pour l'espace de stockage typique d'un nœud.

Lorsque vous utilisez les métriques Amazon Redshift dans la CloudWatch console, les outils de ligne de commande ou un SDK Amazon, gardez les concepts suivants 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 plus d'informations sur les dimensions, consultez la section [Dimensions](#) du guide du CloudWatch développeur.
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 plus d'informations, consultez [Métriques Amazon Redshift](#).

CloudWatch espace de noms	Dimension	Description
AWS/Redshift	NodeID	Les filtres ont demandé des données spécifiques aux nœuds d'un cluster. NodeID a la valeur « Principal », « Partagé » ou « Calcul-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.
	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. De nombreuses 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](#)

Événements Amazon Redshift

Rubriques

- [Présentation des événements du cluster](#)
- [Utilisation d'Amazon Simple Notification Service](#)
- [Abonnement aux notifications d'événements d'un cluster Amazon Redshift](#)
- [Affichage des événements du cluster à l'aide de la console](#)
- [Affichage des événements du cluster à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift](#)
- [Gestion des notifications d'événement d'un cluster](#)
- [Notifications d'événement Amazon Redshift](#)
- [Notifications d'événements Amazon Redshift sans serveur avec Amazon EventBridge](#)
- [Notifications d'événements d'intégration sans ETL avec Amazon EventBridge](#)

Présentation des événements du cluster

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 plus d'informations, consultez [Abonnement aux notifications d'événements d'un 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 “Catégories d'événements et messages d'événements Amazon Redshift”](#)

Utilisation d'Amazon Simple Notification Service

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. 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).

Vous pouvez facilement désactiver les notifications sans supprimer d'abonnement en réglant le bouton radio Enabled sur No dans le AWS Management Console ou en définissant le Enabled paramètre sur false utilisation de la CLI ou de l'API Amazon Redshift.

La facturation des notifications d'événements d'Amazon Redshift se fait par le biais du service Amazon Simple Notification Service (Amazon SNS). Des frais d'Amazon SNS s'appliquent lors de l'utilisation de la notification d'événements. Pour plus d'informations sur la facturation d'Amazon SNS, consultez la rubrique [Tarification d'Amazon Simple Notification Service](#).

Vous pouvez également afficher les événements Amazon Redshift qui ont eu lieu à l'aide de la console de gestion. Pour plus d'informations, consultez [Événements Amazon Redshift](#).

Abonnement aux notifications d'événements d'un cluster Amazon Redshift

Vous pouvez créer un abonnement aux notifications d'événement Amazon Redshift afin de pouvoir 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](#).

Vous pouvez créer un abonnement aux notifications d'événement Amazon Redshift afin de pouvoir 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 AWS Management Console. Si vous choisissez de créer 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. Pour en savoir plus sur la création d'une rubrique Amazon SNS et sur l'abonnement, consultez [Mise en route avec Amazon SNS](#).

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'identifiant doit correspondre à une ressource située dans la même AWS région que l'abonnement à l'événement.
- 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 enverra des notifications pour les événements de configuration d'un niveau de gravité INFO provenant de n'importe quel cluster Amazon Redshift du AWS compte.
- 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. Pour plus d'informations sur la création des rubriques Amazon SNS et l'abonnement à ces rubriques, consultez [Premiers pas avec Amazon Simple Notification Service](#).

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.

Affichage des événements du cluster à l'aide de la console

Pour afficher les événements

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](https://console.aws.amazon.com/redshiftv2/)
2. Dans le menu de navigation, choisissez Événements.

Affichage des événements du cluster à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift

Vous pouvez utiliser l'opération suivante d'interface de ligne de commande Amazon Redshift pour afficher les événements.

- [describe-events](#)

Amazon Redshift fournit l'API suivante pour afficher les événements.

- [DescribeEvents](#)

Gestion des notifications d'événement d'un cluster

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 Amazon Redshift](#).

Gestion des notifications d'événement d'un cluster à l'aide de la console Amazon Redshift

Création d'un abonnement aux notifications d'événement

Pour créer un abonnement aux événements

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

Gestion des notifications d'événements du cluster à l'aide de l'API Amazon AWS CLI Redshift et de l'API Amazon Redshift

Vous pouvez utiliser les opérations d'interface de ligne de commande Amazon Redshift suivantes pour gérer les notifications d'événement d'un cluster.

- [create-event-subscription](#)
- [delete-event-subscription](#)
- [describe-event-categories](#)
- [describe-event-subscriptions](#)
- [describe-events](#)
- [modify-event-subscription](#)

Vous pouvez utiliser les actions d'API Amazon Redshift suivantes pour gérer les notifications d'événement.

- [CreateEventSubscription](#)
- [DeleteEventSubscription](#)
- [DescribeEventCategories](#)
- [DescribeEventSubscriptions](#)
- [DescribeEvents](#)
- [ModifyEventSubscription](#)

Pour de plus amples informations sur les notifications d'événements Amazon Redshift, consultez [Notifications d'événement Amazon Redshift](#).

Notifications d'événement Amazon Redshift

Catégories d'événements et messages d'événements Amazon Redshift

Cette section décrit les ID d'événement et les catégories de chaque type de source Amazon Redshift.

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.
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. Consultez AWS Management Console 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. Consultez AWS Management Console 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

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
			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 AWS Management Console pour corriger le problème.
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.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Configuration	REDSHIFT-EVENT-1509	ERROR	<p>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.</p> <p>Pour de plus amples informations, consultez Points de terminaison VPC dans le Guide de l'utilisateur Amazon VPC.</p>
Configuration	REDSHIFT-EVENT-1510	ERROR	<p>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.</p> <p>Pour plus d'informations, consultez Activation du routage VPC amélioré dans le Guide de gestion Amazon Redshift.</p>
Configuration	REDSHIFT-EVENT-1511	ERROR	<p>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.</p>

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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].
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 AWS Management Console.
Gestion	REDSHIFT-EVENT-2013	INFO	Votre cluster [nom du cluster] Amazon Redshift a été renommé à [heure].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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].
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].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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.
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.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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.
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.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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.
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].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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.
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].
Surveillance	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].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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].
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].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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].
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	La copie d'instantané entre régions 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'instantané [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'instantané 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 ».

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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.
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 ».
Gestion	REDSHIFT-EVENT-3629	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.
Gestion	REDSHIFT-EVENT-3630	INFO	Le cluster [nom du cluster] Amazon Redshift a été transféré avec succès de [zone de disponibilité] à [zone de disponibilité]. Vous pouvez utiliser le cluster maintenant.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Gestion	REDSHIFT-EVENT-3631	INFO	Amazon Redshift a réussi à relocaliser votre cluster [nom du cluster] Amazon Redshift depuis [zone de disponibilité] à [zone de disponibilité] pour la récupération.
Gestion	REDSHIFT-EVENT-3632	INFO	Amazon Redshift a temporairement désactivé la relocalisation de cluster pour votre cluster [nom du cluster] Amazon Redshift en raison de changements de configuration. Essayez à nouveau de relocaliser le cluster plus tard.
Surveillance	REDSHIFT-EVENT-3658	ERROR	La migration de EC2-Classique vers EC2-VPC a échoué pour le cluster Redshift [identifiant du cluster].
Contrôle	REDSHIFT-EVENT-3659	INFO	La migration de EC2-Classique vers EC2-VPC a réussi pour le cluster Redshift [identifiant du cluster].
Contrôle	REDSHIFT-EVENT-3660	INFO	Le cluster est placé en état de défaillance matérielle. Supprimez le cluster EC2-Classique et restaurez-le vers un cluster EC2-VPC à partir du dernier instantané [nom de l'instantané] créé à [heure UTC].
Gestion	REDSHIFT-EVENT-3666	INFO	Le cluster Amazon Redshift Multi-AZ [nom du cluster] a détecté une défaillance 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-3667	INFO	Le cluster Amazon Redshift Multi-AZ [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 AZ sera bientôt disponible.
Surveillance	REDSHIFT-EVENT-3668	ERROR	Le cluster Amazon Redshift Multi-AZ [nom du cluster] n'a pas pu être restauré à [heure en UTC].
Gestion	REDSHIFT-EVENT-3669	INFO	Le cluster Amazon Redshift Multi-AZ [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] s'est terminée à [heure en UTC] et peut être utilisée avec les ressources de calcul de [première zone de disponibilité]. Le calcul secondaire dans une autre AZ sera bientôt disponible.
Gestion	REDSHIFT-EVENT-3671	INFO	Le redimensionnement sur le cluster Amazon Redshift [nom du cluster] a été effectué à [heure en UTC] et est disponible pour une utilisation dans [première zone de disponibilité]. Le calcul secondaire dans une autre AZ sera bientôt disponible.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Gestion	REDSHIFT-EVENT-3672	INFO	Le cluster Amazon Redshift Multi-AZ [nom du cluster] a détecté une défaillance dans [deuxième zone de disponibilité] à [heure en UTC] et a déclenché une restauration automatique.
Gestion	REDSHIFT-EVENT-3673	INFO	L'opération d'activation du mode multi-AZ pour le cluster Amazon Redshift [nom du cluster] a débuté à [heure en UTC].
Gestion	REDSHIFT-EVENT-3674	INFO	L'opération d'activation de Multi-AZ pour le cluster Amazon Redshift [nom du cluster] s'est terminée avec succès à [heure en UTC].
Surveillance	REDSHIFT-EVENT-3675	ERROR	L'opération d'activation du mode multi-AZ pour le cluster Amazon Redshift [nom du cluster] a échoué à [heure en UTC].
Gestion	REDSHIFT-EVENT-3676	INFO	L'opération de désactivation du mode multi-AZ pour votre cluster Amazon Redshift multi-AZ [nom du cluster] a débuté à [heure en UTC].
Gestion	REDSHIFT-EVENT-3677	INFO	L'opération de désactivation du mode multi-AZ pour votre cluster Amazon Redshift [nom du cluster] s'est terminée avec succès à [heure en UTC].
Surveillance	REDSHIFT-EVENT-3678	ERROR	L'opération de désactivation du mode 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 correctement modifié.

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.
Surveillance	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 d'annulation. Essayez de procéder à une restauration sur un cluster avec une configuration différente.
Gestion	REDSHIFT-EVENT-3686	ERROR	L'opération de redimensionnement sur le cluster [nom du cluster] a échoué car il ne dispose pas de suffisamment d'espace disque disponible. L'opération est en cours d'annulation. Essayez de le redimensionner vers un cluster avec une configuration différente.
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].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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-4500	ERROR	Le groupe de sécurité [nom du groupe de sécurité] fourni n'est pas valide. Vos modifications de configuration du cluster [nom du cluster] n'ont pas été appliquées. Veuillez consulter le AWS Management Console pour corriger le problème.
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.
Sécurité	REDSHIFT-EVENT-4503	ERROR	Amazon Redshift ne peut pas accéder au secret de votre cluster [nom du cluster].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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.

Le tableau suivant affiche la catégorie d'événement et la liste d'événements quand un groupe de paramètres est le type source.

Catégories et événements pour le type de source groupe de paramètres

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].
Configuration	REDSHIFT-EVENT-1003	INFO	Le groupe de paramètres de cluster [nom du groupe] a été créé.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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 appliquées lorsque vous redémarrerez les clusters associés.

Le tableau suivant affiche la catégorie d'événement et la liste d'événements quand un groupe de sécurité est le type source.

Catégories et événements pour le type de source groupe de sécurité

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 modifications seront appliquées automatiquement à tous les clusters associés.

Le tableau suivant affiche la catégorie d'événement et la liste d'événements quand un snapshot est le type source.

Catégories et événements pour le type de source instantané

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 AWS Management Console.
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].
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].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
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. Rendez-vous sur le site AWS Management Console pour réessayer l'opération.
Surveillance	REDSHIFT-EVENT-3503	ERROR	L'instantané utilisateur [nom de l'instantané] de votre cluster [nom du cluster] Amazon Redshift a échoué à [heure]. L'équipe étudie le problème. Rendez-vous sur le site AWS Management Console 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 up-to-date 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 échoué à <time in UTC>.
Surveillance	REDSHIFT-SERVERLESS-EVENT-1003	INFO	Le logiciel a été mis à jour sur votre entrepôt des données Amazon Redshift

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
			<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.
Surveillance	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.

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
Surveillance	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
Surveillance	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, COPY/UNLOAD depuis 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
Surveillance	REDSHIFT-SERVERLESS-EVENT-1502	ERROR	Le sous-réseau <subnet id> n'a aucune adresse IP disponible. Cela empêchera les types de requêtes Amazon EMR, les requêtes fédérées Redshift, Redshift COPY/ UNLOAD, Redshift ML de s'exécuter correctement dans le groupe de travail <workgroup name>. 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>.
Surveillance	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>.

Notifications d'événements d'intégration sans ETL avec Amazon EventBridge

L'intégration Zero-ETL utilise Amazon EventBridge pour gérer les notifications d'événements afin de vous tenir au courant up-to-date 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 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 :

- 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
Surveillance	REDSHIFT-INTEGRATION-EVENT-0000	INFO	L'intégration zéro ETL <nom de l'intégration> a été créée et est désormais ACTIVE.
Surveillance	REDSHIFT-INTEGRATION-EVENT-0001	INFO	L'intégration zéro ETL <nom de l'intégration> a été

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
			supprimée à <heure UTC>.
Surveillance	REDSHIFT-INTEGRATION-EVENT-0002	INFO	Suppression initiée de l'intégration zéro ETL <nom de l'intégration> à <heure UTC>.
Surveillance	REDSHIFT-INTEGRATION-EVENT-0003	INFO	L'intégration zéro ETL <nom de l'intégration> synchronise les données transactionnelles dans l'entrepôt des données cible.

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
Surveillance	REDSHIFT-INTEGRATION-EVENT-0004	WARNING	Une ou plusieurs tables ne possèdent pas de clé primaire et ne peuvent pas être synchronisées. Effectuez une sauvegarde sur Amazon RDS, supprimez ces tables et recréez-les en suivant les bonnes pratiques d'Amazon Redshift en matière de conception de tables.

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
Surveillance	REDSHIFT-INTEGRATION-EVENT-0005	WARNING	Une ou plusieurs tables ne peuvent pas être synchronisées, car elles contiennent des types de données ou des longueurs non pris en charge. Corrigez les tables et réessayez. Pour savoir quels sont les types de données non pris en charge, consultez Types de données non pris en charge .
Surveillance	REDSHIFT-INTEGRATION-EVENT-0006	ERROR	Impossible de créer l'intégration. Supprimez et recréez l'intégration.
Surveillance	REDSHIFT-INTEGRATION-EVENT-0007	ERROR	Impossible de charger les données en raison d'une défaillance interne. Supprimez et recréez l'intégration.

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
Surveillance	REDSHIFT-INTEGRATION-EVENT-0008	ERROR	L'autorisation a échoué car les autorisations ont été révoquées du cluster de base de données Aurora source. Supprimez et recréez l'intégration.
Surveillance	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.
Surveillance	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.

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
Surveillance	REDSHIFT-INTEGRATION-EVENT-0013	INFO	L'intégration zéro ETL <nom de l'intégration> est désormais ACTIVE.
Surveillance	REDSHIFT-INTEGRATION-EVENT-0014	ERROR	L'intégration <nom de l'intégration> a échoué, car elle n'a pas pu être modifiée en raison d'une erreur interne. Supprimez et recréez l'intégration. Si l'erreur persiste, contactez le AWS Support.
Opération	REDSHIFT-INTEGRATION-EVENT-0015	INFO	Une modification DDL <modification DDL> a été appliquée à la table <schéma.nom>.
Opération	REDSHIFT-INTEGRATION-EVENT-0016	INFO	Votre intégration zéro ETL <nom de l'intégration> traite une demande de modification avec les arguments suivants : <copie des arguments de la demande>.

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
Opération	REDSHIFT-INTEGRATION-EVENT-0017	INFO	Votre modification de l'intégration zéro ETL <nom de l'intégration> a été appliquée.
Opération	REDSHIFT-INTEGRATION-EVENT-0018	WARNING	Le cluster Amazon Redshift cible est mis en pause. Attendez que le cluster soit mis en pause, puis reprenez son exécution pour continuer la diffusion des données.
Opération	REDSHIFT-INTEGRATION-EVENT-0019	WARNING	Le cluster Amazon Redshift cible est mis en pause. Reprenez l'exécution du cluster pour continuer la diffusion 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
Configuration	REDSHIFT-INTEGRATION-EVENT-1000	ERROR	Un ou plusieurs paramètres du cluster de base de données Aurora source sont mal configurés. Corrigez le groupe de paramètres et redémarrez le cluster pour appliquer les modifications, puis recréez l'intégration.
Configuration	REDSHIFT-INTEGRATION-EVENT-1001	ERROR	L'intégration a échoué, car la valeur du paramètre <code>enable_case_sensitive_identification</code> est incorrecte. Définissez la valeur sur <code>true</code> pour le cluster de base 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-1002	ERROR	L'intégration a échoué, car la valeur du paramètre <code>cdc_insert_enabled</code> est incorrecte. Définissez la valeur sur <code>true</code> pour le cluster de base de données Aurora source, puis supprimez et recréez l'intégration.
Configuration	REDSHIFT-INTEGRATION-EVENT-1003	ERROR	Le paramètre <code>binlog_format</code> du groupe de paramètres du cluster de bases de données source doit être défini sur <code>ROW</code> . Corrigez le groupe de paramètres et redémarrez le cluster 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-1004	ERROR	Impossible de charger les données, car le paramètre de cluster <code>binlog_transaction_compression</code> est activé. Définissez la valeur du paramètre sur OFF et redémarrez l'instance de l'enregistreur pour appliquer la modification, puis recréez l'intégration.
Configuration	REDSHIFT-INTEGRATION-EVENT-1005	ERROR	Impossible de charger les données, car le paramètre de cluster <code>binlog_row_value_options</code> 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.

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
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. Pour les quotas ajustables, vous pouvez demander une augmentation de votre AWS compte dans une AWS région en soumettant un formulaire d'[augmentation des limites Amazon Redshift](#).

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	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	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
é par AWS KMS key			
Rôles IAM du cluster permettant à Amazon Redshift d'accéder à d'autres services AWS	50 ¹	Non	<p>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.</p> <p>¹ Le quota est de 10 dans les cas suivants Régions AWS : us-iso-east -1, us-iso-west -1, us-isob-east -1.</p>
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.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Clusters de mise à l'échelle de la simultanéité	10	Oui	Nombre maximal de clusters de mise à l'échelle de la simultanéité.
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 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
Points de terminaison de VPC gérés par Redshift connectés à un cluster	30	Oui	Nombre maximal de points de terminaison de VPC gérés par Redshift que vous pouvez connecter à un cluster. Pour plus d'informations sur les points de terminaison de VPC gérés par Redshift, consultez Utilisation des points de terminaison de VPC gérés par RedShift.
Accès des bénéficiaires du cluster via un point de terminaison de VPC géré par Redshift	5	Oui	Nombre maximal de bénéficiaires qu'un propriétaire de cluster peut autoriser à créer un point de terminaison de VPC géré par Redshift pour ledit cluster. Pour plus d'informations sur les points de terminaison de VPC gérés par Redshift, consultez Utilisation des points de terminaison de VPC gérés par RedShift.
Points de terminaison de VPC gérés par Redshift par autorisation	5	Oui	Nombre maximal de points de terminaison de VPC gérés par Redshift que vous pouvez créer par autorisation. Pour plus d'informations sur les points de terminaison de VPC gérés par Redshift, consultez Utilisation des points de terminaison de VPC gérés par RedShift.
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 <code>pg_temp_*</code> 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	4	Non	Taille maximale (en Mo) d'une seule ligne lors du chargement à l'aide de la commande COPY.
Instantanés	700	Oui	Le nombre maximum de clichés utilisateur pour ce compte dans la AWS région actuelle.
Groupes de sous-réseaux	20	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
Tables pour le type de nœud de cluster <code>large</code>	9 900	Non	Nombre maximal de tables pour le type de nœud de cluster volumineux. 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 <code>xlarge</code>	9 900	Non	Nombre maximal de tables pour le type de nœud de cluster <code>xlarge</code> . 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 x1p1us avec un cluster à nœud unique.	9 900	Non	Nombre maximal de tables pour le type de nœud de cluster x1p1us 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 x1p1us avec un cluster à plusieurs nœuds.	20 000	Non	Nombre maximal de tables pour le type de nœud de cluster x1p1us 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 4xlarge	200 000	Non	Nombre maximal de tables pour le type de nœud de cluster 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 8xlarge	200 000	Non	Nombre maximal de tables pour le type de nœud de cluster 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.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Tables pour le type de nœud de cluster 16xlarge	200 000	Non	Nombre maximal de tables pour le type de nœud de cluster 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.
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.
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.

Nom du quota	AWS valeur par défaut	Ajustable	Description
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 maximal de connexions pour les nœuds RA3	2 000	Non	Nombre maximal de connexions à un cluster RA3. (Ceci s'applique spécifiquement aux types de nœuds ra3.xlplus, ra3.4xlarge et ra3.16xlarge.) Le nombre maximum de connexions autorisées varie selon le type de nœud.
Nombre maximal de connexions pour les nœuds DC2	Varie	Non	Le nombre maximum de connexions à un cluster dc2.large est de 500. Le nombre maximum de connexions par cluster dc2.8xlarge est de 2000.
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 Contrôle d'accès basé sur les rôles (RBAC) dans le Guide du développeur de base de données Amazon Redshift.

Quotas pour les objets Amazon Redshift sans serveur

Amazon Redshift dispose de quotas qui limitent l'utilisation de plusieurs types d'objets dans votre instance 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	Le nombre maximum de schémas autorisés dans une instance Amazon Redshift sans serveur.
Nombre de tables	200 000	Non	Le nombre maximum de tables autorisées dans une instance Amazon Redshift sans serveur.
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 d'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	2000	Non	Le nombre maximum de connexions autorisées pour se connecter à un groupe de travail.

Nom du quota	AWS valeur par défaut	Ajustable	Description
de connexions			
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.
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 Contrôle d'accès basé sur les rôles (RBAC) dans le Guide du développeur de base de données Amazon Redshift.

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 seconde (TPS) pour l'API DescribeTable	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 <code>ExecuteStatement</code>	30	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.
Transactions par seconde (TPS) pour l'API <code>GetStatementResult</code>	20	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.
Transactions par seconde (TPS) pour l'API <code>ListDatabases</code>	3	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.
Transactions par seconde (TPS) pour l'API <code>ListSchemas</code>	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 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 maximum de principaux pouvant utiliser simultanément l'éditeur de requêtes v2 dans ce compte dans la région actuelle.

Nom du quota	AWS valeur par défaut	Ajustable	Description
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.
Lignes récupérées par requête	100 000	Non	Nombre maximal de lignes récupérées par requête par l'éditeur de requêtes v2 dans ce compte dans la région actuelle.
Taille des données récupérées par requête	5	Non	Taille maximale, en mégaoctets, des données extraites par requête par l'éditeur de requêtes v2 dans ce compte dans la région actuelle.
Connexions socket simultanées par principal	10	Oui	Nombre maximal de connexions socket simultanées à l'éditeur de requêtes v2 qu'un seul principal peut établir dans la région actuelle. Évaluez si vous souhaitez augmenter ce quota si vous recevez des erreurs indiquant que vos connexions socket dépassent la limite.
Connexions socket simultanées par compte.	250	Oui	Nombre maximal de connexions socket simultanées à l'éditeur de requêtes v2 que tous les principaux du compte peuvent établir dans la région actuelle. Évaluez si vous souhaitez augmenter ce quota si vous recevez des erreurs indiquant que vos connexions socket dépassent la limite.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Nombre maximal de connexions simultanées	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'administrateur 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 Modification des paramètres de 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.
-

	<p>Son premier caractère doit être une lettre.</p> <ul style="list-style-type: none">• 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 base de données	<ul style="list-style-type: none">• 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 de VPC géré par Redshift	<ul style="list-style-type: none">• Le nom du point de terminaison doit contenir entre 1 et 30 caractères.• Les caractères valides sont : A-Z, a-z, 0-9 et le trait d'union (-).• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.• <p>Il peut utiliser n'importe quels caractères ASCII avec des codes ASCII 33 à 126, sauf ' (guillemet simple), " (guillemets doubles), :, \, / ou @.</p>
Nom du groupe de paramètres	<ul style="list-style-type: none">• 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.

<p>Nom du groupe de sécurité du cluster</p>	<ul style="list-style-type: none">• 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.
<p>Nom du groupe de sous-réseau</p>	<ul style="list-style-type: none">• 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-réseaux créés par votre AWS compte.
<p>Identifiant d'instantané de cluster</p>	<ul style="list-style-type: none">• 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.

Étiquetage des ressources Amazon Redshift

Rubriques

- [Présentation du balisage](#)
- [Gestion des balises des ressources à l'aide de la console](#)
- [Gestion des étiquettes à l'aide de l'API Amazon Redshift](#)

Présentation du balisage

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 souhaitez 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 vous 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 :

- Adresse 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

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 des ressources à l'aide de la console

Pour gérer les étiquettes de vos ressources Amazon Redshift

1. [Connectez-vous à la console Amazon Redshift AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/redshiftv2/`.](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.

Gestion des étiquettes à l'aide de l'API Amazon Redshift

Vous pouvez utiliser les AWS CLI opérations suivantes pour gérer les balises dans Amazon Redshift.

- [create-tags](#)
- [delete-tags](#)
- [describe-tags](#)

Vous pouvez utiliser les opérations d'API Amazon Redshift suivantes pour gérer les étiquettes :

- [CreateTags](#)
- [DeleteTags](#)
- [DescribeTags](#)
- [Balise](#)
- [TaggedResource](#)

En outre, vous pouvez utiliser les opérations d'API Amazon Redshift suivantes pour gérer et afficher les étiquettes d'une ressource spécifique :

- [CreateCluster](#)
- [CreateClusterParameterGroup](#)
- [CreateClusterSecurityGroup](#)
- [CreateClusterSnapshot](#)
- [CreateClusterSubnetGroup](#)
- [CreateHsmClientCertificate](#)
- [CreateHsmConfiguration](#)
- [DescribeClusters](#)
- [DescribeClusterParameterGroups](#)
- [DescribeClusterSecurityGroups](#)
- [DescribeClusterSnapshots](#)
- [DescribeClusterSubnetGroups](#)
- [DescribeHsmClientCertificates](#)
- [DescribeHsmConfigurations](#)

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();
```

Rubriques

- [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 181 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.69497 — Version sans serveur d'Amazon Redshift — Publiée le 18 juin 2024
- 1.0.69451 — Version actuelle du titre — Sortie le 18 juin 2024
- 1.0.69076 — Version sans serveur d'Amazon Redshift — Publiée le 14 juin 2024
- 1.0.69065 — Version actuelle du titre — Sortie le 14 juin 2024
- 1.0.68555 — Version sans serveur Amazon Redshift — Publiée le 31 mai 2024
- 1.0.68540 — Version actuelle du titre — Sortie le 31 mai 2024
- 1.0.68328 — Version sans serveur d'Amazon Redshift — Publiée le 23 mai 2024
- 1.0.68205 — Version actuelle du titre — Sortie le 23 mai 2024
- 1.0.67796 — Version sans serveur d'Amazon Redshift — Publiée le 15 mai 2024
- 1.0.67788 — Version actuelle du titre — Sortie le 15 mai 2024
- 1.0.67308 — Version sans serveur Amazon Redshift — Publiée le 1er mai 2024
- 1.0.67305 — Version actuelle du titre — Sortie le 1er mai 2024

Nouvelles fonctionnalités et améliorations de ce correctif

- Permet de modifier la clé de distribution et la clé de tri des vues matérialisées.
- 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 deviendrait invalide dans la nouvelle table.
- Résout un problème empêchant l'affichage de certaines tables externes dans SVV_ALL_TABLES.
- Améliore le temps de démarrage du cluster et accélère l'initialisation des requêtes pour les charges de travail simultanées élevées.
- 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 la clé de distribution initiées par l'utilisateur via les commandes ALTER TABLE... ALTER DISTSTYLE KEY DISTKEY sur les clusters de dimensionnement simultanés provisionnés et le calcul de mise à l'échelle automatique sans serveur.
- Prend en charge les vues matérialisées actualisées manuellement qui impliquent l'agrégation sur le dimensionnement simultané provisionné et le calcul de mise à l'échelle automatique sans serveur.

- Ajoute la prise en charge de Zero-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 Zero-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 SageMaker ressources Amazon utilisées par Amazon Redshift ML. Le balisage vous aide à gérer, identifier, organiser, rechercher et filtrer les ressources.
- Améliore les performances des requêtes impliquant des fonctions définies par l'utilisateur (UDF) Lambda 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 le support pour les nouvelles lignes (\n) dans la colonne dans la vue SYS_QUERY_HISTORY et pour la colonne query_text dans la vue SYS_QUERY_TEXT. text

Correctif 180 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.68870 — Version de suivi — Sortie le 3 juin 2024
- 1.0.68520 — Version de suivi — Sortie le 28 mai 2024
- 1.0.67699 — Version de suivi — Sortie le 15 mai 2024
- 1.0.66960 — Version de suivi — Sortie le 21 avril 2024
- 1.0.66954 — Version actuelle du titre — Sortie le 21 avril 2024
- 1.0.66276 — Version actuelle du titre — Sortie le 12 avril 2024
- 1.0.66290 — Version sans serveur Amazon Redshift — Publiée le 10 avril 2024
- 1.0.63590 — Version actuelle du titre — Sortie le 19 février 2024
- 1.0.63567 — Version sans serveur d'Amazon Redshift — Publiée le 16 février 2024
- 1.0.63282 — Version sans serveur d'Amazon Redshift — Publiée le 13 février 2024
- 1.0.63269 — Version actuelle du titre — Sortie le 13 février 2024
- 1.0.63215 — Version sans serveur d'Amazon Redshift — Publiée le 12 février 2024
- 1.0.63205 — Version actuelle du titre — Sortie le 12 février 2024
- 1.0.63030 — Version sans serveur d'Amazon Redshift — Publiée le 7 février 2024

- 1.0.62913 — Version actuelle du titre — Sortie le 7 février 2024
- 1.0.62922 — Version sans serveur d'Amazon Redshift — Publiée le 5 février 2024
- 1.0.62878 — Version actuelle du titre — Sortie 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 SageMaker modèles 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_FromLong Lat, 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 Trailing Track — Sortie 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 simultanée. Les clusters de mise à l'échelle de la simultanée 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 simultanée.
- 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 actuelle du titre — Sortie le 9 février 2024
- 1.0.63313 - Version Trailing Track — Sortie 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.
- Les clusters Amazon Redshift RA3 à nœud unique peuvent désormais bénéficier des améliorations du chiffrement, ce qui réduit le temps de chiffrement global et améliore la disponibilité de l'entrepôt des données pendant le 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.
- Ajout de la vue `SYS_COPY_REPLACEMENTS`, qui affiche un journal qui enregistre à quel moment des caractères UTF-8 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 [Encodage par dictionnaire d'octets](#) dans le Guide du développeur de la 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'une table, cette colonne stocke l'horodatage 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.
- Prend en charge par défaut la protection des objets protégés par RLS lorsqu'ils sont ajoutés à une unité de partage des données ou qu'ils en font déjà partie. 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 parmi les clés primaires composites afin d'améliorer out-of-the-box les performances.
- Ajoute une clé primaire automatique à la clé de distribution pour les tables comportant des clés primaires composites, améliorant ainsi les out-of-the-box performances.
- 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 le rôle comme paramètre pour la commande Alter Default Privileges (Modifier les privilèges par défaut) afin de prendre en charge le contrôle d'accès basé sur les rôles.
- Ajoute le paramètre ACCEPTINVCHARS pour prendre en charge le remplacement des caractères UTF-8 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 mai 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 out-of-the-box requêtes, Amazon Redshift choisit automatiquement une clé primaire à colonne unique pour des tables spécifiques comme clé de distribution.

Exemples de code pour Amazon Redshift à l'aide de kits de développement logiciel AWS

Les exemples de code suivants montrent comment utiliser Amazon Redshift avec un kit de développement AWS logiciel (SDK).

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 et dans des exemples interservices.

Les Scénarios sont des exemples de code qui vous montrent comment accomplir une tâche spécifique en appelant plusieurs fonctions au sein d'un même service.

Les Exemples de services croisés sont des exemples d'applications fonctionnant sur plusieurs Services AWS.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Mise en route

Bonjour Amazon Redshift

Les exemples de code suivants montrent comment commencer à utiliser Amazon Redshift.

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, consultez [DescribeClusters](#) dans AWS SDK for Java 2.x la référence des API.

Python

SDK pour 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 le [manuel de référence de l'API DescribeClusters](#) in AWS SDK for Python (Boto3).

Exemples de code

- [Actions pour Amazon Redshift à l'aide de kits de développement logiciel AWS](#)
 - [Utilisation CreateCluster avec un AWS SDK ou une CLI](#)
 - [Utilisation CreateTable avec un AWS SDK ou une CLI](#)
 - [Utilisation DeleteCluster avec un AWS SDK ou une CLI](#)
 - [Utilisation DescribeClusters avec un AWS SDK ou une CLI](#)
 - [Utilisation DescribeStatement avec un AWS SDK ou une CLI](#)
 - [Utilisation GetStatementResult avec un AWS SDK ou une CLI](#)
 - [Utilisation Insert avec un AWS SDK ou une CLI](#)
 - [Utilisation ModifyCluster avec un AWS SDK ou une CLI](#)
 - [Utilisation Query avec un AWS SDK ou une CLI](#)
- [Scénarios pour Amazon Redshift utilisant des kits de développement logiciel AWS](#)
 - [Commencez à utiliser les tables, les éléments et les requêtes Amazon Redshift](#)
- [Exemples multiservices pour Amazon AWS Redshift utilisant des kits de développement logiciel](#)
 - [Créer un outil de suivi des éléments Amazon Redshift.](#)

Actions pour Amazon Redshift à l'aide de kits de développement logiciel AWS

Les exemples de code suivants montrent comment effectuer des actions Amazon Redshift individuelles à l'aide AWS des SDK. Ces extraits appellent l'API Amazon Redshift et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour une liste complète, consultez le manuel [Amazon Redshift API Reference](#).

Exemples

- [Utilisation CreateCluster avec un AWS SDK ou une CLI](#)
- [Utilisation CreateTable avec un AWS SDK ou une CLI](#)
- [Utilisation DeleteCluster avec un AWS SDK ou une CLI](#)
- [Utilisation DescribeClusters avec un AWS SDK ou une CLI](#)

- [Utilisation DescribeStatement avec un AWS SDK ou une CLI](#)
- [Utilisation GetStatementResult avec un AWS SDK ou une CLI](#)
- [Utilisation Insert avec un AWS SDK ou une CLI](#)
- [Utilisation ModifyCluster avec un AWS SDK ou une CLI](#)
- [Utilisation Query avec un AWS SDK ou une CLI](#)

Utilisation **CreateCluster** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser `CreateCluster`.

CLI

AWS CLI

L' exemple `Create a Cluster with Minimal` crée un cluster avec un ensemble minimal de paramètres. Par défaut, la sortie est au format JSON. 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, reportez-vous [CreateCluster](#) à la section Référence des AWS CLI commandes.

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 .

```

public static void createCluster(RedshiftClient redshiftClient, String
clusterId, String masterUsername,
                                String masterUserPassword) {
    try {
        CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .masterUsername(masterUsername)
            .masterUserPassword(masterUserPassword)
            .nodeType("ra3.4xlarge")

```

```
        .publiclyAccessible(true)
        .numberOfNodes(2)
        .build();

        CreateClusterResponse clusterResponse =
redshiftClient.createCluster(clusterRequest);
        System.out.println("Created cluster " +
clusterResponse.cluster().clusterIdentifier());

    } catch (RedshiftException e) {

        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Pour plus de détails sur l'API, reportez-vous [CreateCluster](#) à la 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, reportez-vous [CreateCluster](#) à la section Référence des AWS SDK for 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
            masterUsername = masterUsernameVal
            masterUserPassword = masterUserPasswordVal
            nodeType = "ds2.xlarge"
            publiclyAccessible = true
            numberOfNodes = 2
        }

    RedshiftClient { 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 [CreateCluster](#) la section AWS SDK pour la référence de l'API Kotlin.

Python

SDK pour 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")
redshift_wrapper = RedshiftWrapper(client)
```

- Pour plus de détails sur l'API, consultez [CreateCluster](#) le 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, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation `CreateTable` avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser `CreateTable`.

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](#).

```
public static void createTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName) {
    try {
        ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
        .clusterIdentifier(clusterId)
        .dbUser(userName)
        .database(databaseName)
        .sql("CREATE TABLE Movies ("
            + "id INT PRIMARY KEY, "
            + "title VARCHAR(100), "
            + "year INT)")
        .build();

        redshiftDataClient.executeStatement(createTableRequest);
        System.out.println("Table created: Movies");

    } catch (RedshiftDataException e) {
        System.err.println("Error creating table: " + e.getMessage());
        System.exit(1);
    }
}
```

- Pour plus de détails sur l'API, reportez-vous [CreateTable](#) à la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour 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](#).

```
def create_table(self, cluster_id, database, username):
    self.redshift_data_wrapper.execute_statement(
        cluster_identifrier=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")
```

Appel ExecuteStatement d'objets Wrapper.

```
class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client

    def execute_statement(
        self, cluster_identifrier, 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
```

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 [CreateTable](#) le 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, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation `DeleteCluster` avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser `DeleteCluster`.

CLI

AWS CLI

Supprimer un cluster sans cluster final Snapshot. Cet 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, Snapshot. Cet 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, reportez-vous [DeleteCluster](#) à la section Référence des AWS CLI commandes.

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.

```
public static void deleteRedshiftCluster(RedshiftClient redshiftClient,  
String clusterId) {
```

```
    try {
        DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
        .clusterIdentifier(clusterId)
        .skipFinalClusterSnapshot(true)
        .build();

        DeleteClusterResponse response =
redshiftClient.deleteCluster(deleteClusterRequest);
        System.out.println("The status is " +
response.cluster().clusterStatus());

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Pour plus de détails sur l'API, reportez-vous [DeleteCluster](#) à la 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, reportez-vous [DeleteCluster](#) à la section Référence des AWS SDK for 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 { 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 [DeleteCluster](#) la section AWS SDK pour la référence de l'API Kotlin.

Python

SDK pour 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_identifiant):
        """
        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")
redshift_wrapper = RedshiftWrapper(client)
```

- Pour plus de détails sur l'API, consultez [DeleteCluster](#) le 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, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **DescribeClusters** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser `DescribeClusters`.

CLI

AWS CLI

L' `ClustersThis` exemple `Get a Description of All` renvoie une description de tous les clusters du compte. Par défaut, la sortie est au format JSON. 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` :

`--output text` Option. 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, reportez-vous [DescribeClusters](#) à la section Référence des AWS CLI commandes.

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.

```
public static void waitForClusterReady(RedshiftClient redshiftClient, String
clusterId) {
    boolean clusterReady = false;
    String clusterReadyStr;
    System.out.println("Waiting for cluster to become available. This may
take a few mins.");
```

```
    try {
        DescribeClustersRequest clustersRequest =
DescribeClustersRequest.builder()
            .clusterIdentifier(clusterId)
            .build();
        long startTime = System.currentTimeMillis();

        // Loop until the cluster is ready.
        while (!clusterReady) {
            DescribeClustersResponse clusterResponse =
redshiftClient.describeClusters(clustersRequest);
            List<Cluster> clusterList = clusterResponse.clusters();
            for (Cluster cluster : clusterList) {
                clusterReadyStr = cluster.clusterStatus();
                if (clusterReadyStr.contains("available"))
                    clusterReady = true;
                else {
                    long elapsedTimeMillis = System.currentTimeMillis() -
startTime;

                    long elapsedSeconds = elapsedTimeMillis / 1000;
                    long minutes = elapsedSeconds / 60;
                    long seconds = elapsedSeconds % 60;

                    System.out.printf("Elapsed Time: %02d:%02d - Waiting for
cluster... %n", minutes, seconds);
                    TimeUnit.SECONDS.sleep(5);
                }
            }
        }

        long elapsedTimeMillis = System.currentTimeMillis() - startTime;
        long elapsedSeconds = elapsedTimeMillis / 1000;
        long minutes = elapsedSeconds / 60;
        long seconds = elapsedSeconds % 60;

        System.out.println(String.format("Cluster is available! Total Elapsed
Time: %02d:%02d", minutes, seconds));
    } catch (RedshiftException | InterruptedException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Pour plus de détails sur l'API, reportez-vous [DescribeClusters](#) à la 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, reportez-vous [DescribeClusters](#) à la section Référence des AWS SDK for 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 { 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 [DescribeClusters](#) la section AWS SDK pour la référence de l'API Kotlin.

Python

SDK pour 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")  
redshift_wrapper = RedshiftWrapper(client)
```

- Pour plus de détails sur l'API, consultez [DescribeClusters](#) le 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, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **DescribeStatement** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser `DescribeStatement`.

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](#).

```
public static void checkStatement(RedshiftDataClient redshiftDataClient,  
String sqlId) {  
    try {
```

```
        DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
        .id(sqlId)
        .build();

        String status;
        while (true) {
            DescribeStatementResponse response =
redshiftDataClient.describeStatement(statementRequest);
            status = response.statusAsString();
            System.out.println("..." + status);

            if (status.compareTo("FAILED") == 0 ) {
                System.out.println("The Query Failed. Ending program");
                System.exit(1);

            } else if (status.compareTo("FINISHED") == 0) {
                break;
            }
            TimeUnit.SECONDS.sleep(1);
        }

        System.out.println("The statement is finished!");

    } catch (RedshiftDataException | InterruptedException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Pour plus de détails sur l'API, reportez-vous [DescribeStatement](#) à la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour 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 [DescribeStatement](#) le 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, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **GetStatementResult** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser `GetStatementResult`.

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 la déclaration.

```
public static void getResults(RedshiftDataClient redshiftDataClient, String
statementId) {
    try {
        GetStatementResultRequest resultRequest =
GetStatementResultRequest.builder()
            .id(statementId)
            .build();

        // Extract and print the field values using streams.
        GetStatementResultResponse response =
redshiftDataClient.getStatementResult(resultRequest);
        response.records().stream()
            .flatMap(List::stream)
            .map(Field::stringValue)
```

```
        .filter(value -> value != null)
        .forEach(value -> System.out.println("The Movie title field is "
+ value));

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Pour plus de détails sur l'API, voir [GetStatementResult](#) in AWS SDK for Java 2.x API Reference.

Python

SDK pour 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, voir [GetStatementResult](#) in AWS SDK for Python (Boto3) API Reference.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **Insert** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser `Insert`.

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](#).

```
public static void popTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName, String fileName, int number)
throws IOException {
    JsonParser parser = new JsonFactory().createParser(new File(fileName));
    com.fasterxml.jackson.databind.JsonNode rootNode = new
ObjectMapper().readTree(parser);
    Iterator<JsonNode> iter = rootNode.iterator();
    ObjectNode currentNode;
    int t = 0;
    while (iter.hasNext()) {
        if (t == number)
            break;
        currentNode = (ObjectNode) 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);";

        // Create the parameters.
        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);

try {
    ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
    .clusterIdentifier(clusterId)
    .sql(sqlStatement)
    .database(databaseName)
    .dbUser(userName)
    .parameters(parameterList)
    .build();

    redshiftDataClient.executeStatement(insertStatementRequest);
    System.out.println("Inserted: " + title + " (" + year + ")");
    t++;

} catch (RedshiftDataException e) {
    System.err.println("Error inserting data: " + e.getMessage());
    System.exit(1);
}
}
System.out.println(t + " records were added to the Movies table. ");
}
```

- Pour plus de détails sur l'API, voir [Insérer](#) dans la référence AWS SDK for Java 2.x d'API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **ModifyCluster** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser `ModifyCluster`.

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-identifiant mycluster --cluster-security-groups mysecuritygroup
```

Modifiez 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 3 h 15.

Commande :

```
aws redshift modify-cluster --cluster-identifiant 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-identifiant mycluster --master-user-password A1b2c3d4
```

- Pour plus de détails sur l'API, reportez-vous [ModifyCluster](#) à la section Référence des AWS CLI commandes.

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.

```
public static void modifyCluster(RedshiftClient redshiftClient, String
clusterId) {
    try {
        ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
        .clusterIdentifier(clusterId)
        .preferredMaintenanceWindow("wed:07:30-wed:08:00")
        .build();

        ModifyClusterResponse clusterResponse =
redshiftClient.modifyCluster(modifyClusterRequest);
        System.out.println("The modified cluster was successfully modified
and has "
            + clusterResponse.cluster().preferredMaintenanceWindow() + " as
the maintenance window");

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Pour plus de détails sur l'API, reportez-vous [ModifyCluster](#) à la 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, reportez-vous [ModifyCluster](#) à la section Référence des AWS SDK for 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 [ModifyCluster](#) la section AWS SDK pour la référence de l'API Kotlin.

Python

SDK pour 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")
redshift_wrapper = RedshiftWrapper(client)
```

- Pour plus de détails sur l'API, consultez [ModifyCluster](#) le 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, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **Query** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser `Query`.

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](#).

Interrogez une table.

```
public static String queryMoviesByYear(RedshiftDataClient redshiftDataClient,
                                       String database,
                                       String dbUser,
                                       int year,
                                       String clusterId) {

    try {
        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();

        ExecuteStatementResponse response =
redshiftDataClient.executeStatement(statementRequest);
        return response.id();

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
}
```

```
}
```

- Pour plus d'informations sur l'API, consultez [Requête](#) dans la référence d'API AWS SDK for Java 2.x .

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Scénarios pour Amazon Redshift utilisant des kits de développement logiciel AWS

Les exemples de code suivants vous montrent comment implémenter des scénarios courants dans Amazon Redshift à l'aide AWS de kits SDK. Ces scénarios vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein d'Amazon Redshift. Chaque scénario inclut un lien vers GitHub, où vous pouvez trouver des instructions sur la façon de configurer et d'exécuter le code.

Exemples

- [Commencez à utiliser les tables, les éléments et les requêtes Amazon Redshift](#)

Commencez à utiliser les tables, les éléments et les requêtes Amazon Redshift

Les exemples de code suivants montrent comment utiliser les tables, les éléments et les requêtes Amazon Redshift.

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 com.fasterxml.jackson.core.JsonFactory;
import com.fasterxml.jackson.databind.JsonNode;
import com.fasterxml.jackson.databind.ObjectMapper;
import com.fasterxml.jackson.databind.node.ObjectNode;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.redshift.RedshiftClient;
import software.amazon.awssdk.services.redshift.model.Cluster;
import software.amazon.awssdk.services.redshift.model.CreateClusterRequest;
import software.amazon.awssdk.services.redshift.model.CreateClusterResponse;
import software.amazon.awssdk.services.redshift.model.DeleteClusterRequest;
import software.amazon.awssdk.services.redshift.model.DeleteClusterResponse;
import software.amazon.awssdk.services.redshift.model.DescribeClustersRequest;
import software.amazon.awssdk.services.redshift.model.DescribeClustersResponse;
import software.amazon.awssdk.services.redshift.model.ModifyClusterRequest;
import software.amazon.awssdk.services.redshift.model.ModifyClusterResponse;
import software.amazon.awssdk.services.redshift.model.RedshiftException;
import software.amazon.awssdk.services.redshiftdata.RedshiftDataClient;
import
    software.amazon.awssdk.services.redshiftdata.model.DescribeStatementRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.DescribeStatementResponse;
import
    software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementResponse;
import software.amazon.awssdk.services.redshiftdata.model.Field;
import
    software.amazon.awssdk.services.redshiftdata.model.GetStatementResultRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.GetStatementResultResponse;
import software.amazon.awssdk.services.redshiftdata.model.ListDatabasesRequest;
import software.amazon.awssdk.services.redshiftdata.model.RedshiftDataException;
import software.amazon.awssdk.services.redshiftdata.model.SqlParameter;
import
    software.amazon.awssdk.services.redshiftdata.paginators.ListDatabasesIterable;
import com.fasterxml.jackson.core.JsonParser;
import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.Iterator;
import java.util.List;
import java.util.Scanner;
import java.util.concurrent.TimeUnit;
```

```
/**
 * 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 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",
"-");
    public static void main(String[] args) throws Exception {
        final String usage = ""

                Usage:
                <jsonFilePath>\s

                Where:
                jsonFilePath - The path to the Movies JSON file (you can locate
that file in ../../../../resources/sample_files/movies.json)
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }
    }
}
```

```
    }

    String jsonFilePath = args[0];
    String userName;
    String userPassword;
    String databaseName = "dev" ;
    Scanner scanner = new Scanner(System.in);

    Region region = Region.US_EAST_1;
    RedshiftClient redshiftClient = RedshiftClient.builder()
        .region(region)
        .build();

    RedshiftDataClient redshiftDataClient = RedshiftDataClient.builder()
        .region(region)
        .build();

    System.out.println(DASHES);
    System.out.println("Welcome to the Amazon Redshift SDK Getting Started
scenario.");
    System.out.println(""""
    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.
    """);

    System.out.println("Lets get started...");
    System.out.println("Please enter your user name (default is awsuser)");
    String user = scanner.nextLine();
    userName = user.isEmpty() ? "awsuser" : user;
    System.out.println(DASHES);
    System.out.println("Please enter your user password (default is
AwsUser1000)");
    String userpass = scanner.nextLine();
```

```
userPassword = userpass.isEmpty() ? "AwsUser1000" : userpass;
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("A Redshift cluster refers to the collection of
computing resources and storage that work together to process and analyze large
volumes of data.");
System.out.println("Enter a cluster id value (default is redshift-
cluster-movies): ");
String userClusterId = scanner.nextLine();
String clusterId = userClusterId.isEmpty() ? "redshift-cluster-movies" :
userClusterId;
createCluster(redshiftClient, clusterId, userName, userPassword);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Wait until "+clusterId+" is available.");
System.out.print("Press Enter to continue...");
scanner.nextLine();
waitForClusterReady(redshiftClient, clusterId);
System.out.println(DASHES);

System.out.println(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);

System.out.println(databaseInfo);
System.out.print("Press Enter to continue...");
scanner.nextLine();
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("List databases in "+clusterId);
System.out.print("Press Enter to continue...");
scanner.nextLine();
listAllDatabases(redshiftDataClient, clusterId, userName, databaseName);
System.out.println(DASHES);
```



```
System.out.println(DASHES);
System.out.println("Now you will create a table named Movies.");
System.out.print("Press Enter to continue...");
scanner.nextLine();
createTable(redshiftDataClient, clusterId, databaseName, userName);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Populate the Movies table using the Movies.json
file.");
System.out.println("Specify the number of records you would like to add
to the Movies Table.");
System.out.println("Please enter a value between 50 and 200.");
int numRecords;
do {
    System.out.print("Enter a value: ");
    while (!scanner.hasNextInt()) {
        System.out.println("Invalid input. Please enter a value between
50 and 200.");
        System.out.print("Enter a year: ");
        scanner.next();
    }
    numRecords = scanner.nextInt();
} while (numRecords < 50 || numRecords > 200);
popTable(redshiftDataClient, clusterId, databaseName, userName,
jsonFilePath, numRecords);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Query the Movies table by year. Enter a value between
2012-2014.");
int movieYear;
do {
    System.out.print("Enter a year: ");
    while (!scanner.hasNextInt()) {
        System.out.println("Invalid input. Please enter a valid year
between 2012 and 2014.");
        System.out.print("Enter a year: ");
        scanner.next();
    }
    movieYear = scanner.nextInt();
    scanner.nextLine();
} while (movieYear < 2012 || movieYear > 2014);
```

```
String id = queryMoviesByYear(redshiftDataClient, databaseName, userName,
movieYear, clusterId);
System.out.println("The identifier of the statement is " + id);
checkStatement(redshiftDataClient, id);
getResults(redshiftDataClient, id);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Now you will modify the Redshift cluster.");
System.out.print("Press Enter to continue...");
scanner.nextLine();
modifyCluster(redshiftClient, clusterId);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Would you like to delete the Amazon Redshift cluster?
(y/n)");
String delAns = scanner.nextLine().trim();
if (delAns.equalsIgnoreCase("y")) {
    System.out.println("You selected to delete " +clusterId);
    System.out.print("Press Enter to continue...");
    scanner.nextLine();
    deleteRedshiftCluster(redshiftClient, clusterId);
} else {
    System.out.println("The "+clusterId +" was not deleted");
}
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("This concludes the Amazon Redshift SDK Getting
Started scenario.");
System.out.println(DASHES);
}

public static void listAllDatabases(RedshiftDataClient redshiftDataClient,
String clusterId, String dbUser, String database) {
    try {
        ListDatabasesRequest databasesRequest =
ListDatabasesRequest.builder()
            .clusterIdentifier(clusterId)
            .dbUser(dbUser)
            .database(database)
            .build();
```

```
        ListDatabasesIterable listDatabasesIterable =
redshiftDataClient.listDatabasesPaginator(databasesRequest);
        listDatabasesIterable.stream()
            .flatMap(r -> r.databases().stream())
            .forEach(db -> System.out
                .println("The database name is : " + db));

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void deleteRedshiftCluster(RedshiftClient redshiftClient,
String clusterId) {
    try {
        DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .skipFinalClusterSnapshot(true)
            .build();

        DeleteClusterResponse response =
redshiftClient.deleteCluster(deleteClusterRequest);
        System.out.println("The status is " +
response.cluster().clusterStatus());

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void popTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName, String fileName, int number)
throws IOException {
    JsonParser parser = new JsonFactory().createParser(new File(fileName));
    com.fasterxml.jackson.databind.JsonNode rootNode = new
ObjectMapper().readTree(parser);
    Iterator<JsonNode> iter = rootNode.iterator();
    ObjectNode currentNode;
    int t = 0;
    while (iter.hasNext()) {
        if (t == number)
```

```
        break;
        currentNode = (ObjectNode) 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)";

        // Create the parameters.
        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);

        try {
            ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
                .clusterIdentifier(clusterId)
                .sql(sqlStatement)
                .database(databaseName)
                .dbUser(userName)
                .parameters(parameterList)
                .build();

            redshiftDataClient.executeStatement(insertStatementRequest);
            System.out.println("Inserted: " + title + " (" + year + ")");
            t++;
        } catch (RedshiftDataException e) {
```

```
        System.err.println("Error inserting data: " + e.getMessage());
        System.exit(1);
    }
}
System.out.println(t + " records were added to the Movies table. ");
}

public static void checkStatement(RedshiftDataClient redshiftDataClient,
String sqlId) {
    try {
        DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
            .id(sqlId)
            .build();

        String status;
        while (true) {
            DescribeStatementResponse response =
redshiftDataClient.describeStatement(statementRequest);
            status = response.statusAsString();
            System.out.println("..." + status);

            if (status.compareTo("FAILED") == 0 ) {
                System.out.println("The Query Failed. Ending program");
                System.exit(1);

            } else if (status.compareTo("FINISHED") == 0) {
                break;
            }
            TimeUnit.SECONDS.sleep(1);
        }

        System.out.println("The statement is finished!");

    } catch (RedshiftDataException | InterruptedException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void modifyCluster(RedshiftClient redshiftClient, String
clusterId) {
    try {
```

```
        ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
        .clusterIdentifier(clusterId)
        .preferredMaintenanceWindow("wed:07:30-wed:08:00")
        .build();

        ModifyClusterResponse clusterResponse =
redshiftClient.modifyCluster(modifyClusterRequest);
        System.out.println("The modified cluster was successfully modified
and has "
                + clusterResponse.cluster().preferredMaintenanceWindow() + " as
the maintenance window");

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static String queryMoviesByYear(RedshiftDataClient redshiftDataClient,
                                        String database,
                                        String dbUser,
                                        int year,
                                        String clusterId) {

    try {
        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();

        ExecuteStatementResponse response =
redshiftDataClient.executeStatement(statementRequest);
        return response.id();
    }
}
```

```
    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
}

public static void getResults(RedshiftDataClient redshiftDataClient, String
statementId) {
    try {
        GetStatementResultRequest resultRequest =
GetStatementResultRequest.builder()
            .id(statementId)
            .build();

        // Extract and print the field values using streams.
        GetStatementResultResponse response =
redshiftDataClient.getStatementResult(resultRequest);
        response.records().stream()
            .flatMap(List::stream)
            .map(Field::stringValue)
            .filter(value -> value != null)
            .forEach(value -> System.out.println("The Movie title field is "
+ value));

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void waitForClusterReady(RedshiftClient redshiftClient, String
clusterId) {
    boolean clusterReady = false;
    String clusterReadyStr;
    System.out.println("Waiting for cluster to become available. This may
take a few mins.");
    try {
        DescribeClustersRequest clustersRequest =
DescribeClustersRequest.builder()
            .clusterIdentifier(clusterId)
            .build();
        long startTime = System.currentTimeMillis();
```

```
// Loop until the cluster is ready.
while (!clusterReady) {
    DescribeClustersResponse clusterResponse =
redshiftClient.describeClusters(clustersRequest);
    List<Cluster> clusterList = clusterResponse.clusters();
    for (Cluster cluster : clusterList) {
        clusterReadyStr = cluster.clusterStatus();
        if (clusterReadyStr.contains("available"))
            clusterReady = true;
        else {
            long elapsedTimeMillis = System.currentTimeMillis() -
startTime;

            long elapsedSeconds = elapsedTimeMillis / 1000;
            long minutes = elapsedSeconds / 60;
            long seconds = elapsedSeconds % 60;

            System.out.printf("Elapsed Time: %02d:%02d - Waiting for
cluster... %n", minutes, seconds);
            TimeUnit.SECONDS.sleep(5);
        }
    }
}

long elapsedTimeMillis = System.currentTimeMillis() - startTime;
long elapsedSeconds = elapsedTimeMillis / 1000;
long minutes = elapsedSeconds / 60;
long seconds = elapsedSeconds % 60;

System.out.println(String.format("Cluster is available! Total Elapsed
Time: %02d:%02d", minutes, seconds));

} catch (RedshiftException | InterruptedException e) {
    System.err.println(e.getMessage());
    System.exit(1);
}

}

public static void createTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName) {
    try {
        ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
            .clusterIdentifier(clusterId)
```



```
        .dbUser(userName)
        .database(databaseName)
        .sql("CREATE TABLE Movies ("
            + "id INT PRIMARY KEY, "
            + "title VARCHAR(100), "
            + "year INT)")
        .build();

        redshiftDataClient.executeStatement(createTableRequest);
        System.out.println("Table created: Movies");

    } catch (RedshiftDataException e) {
        System.err.println("Error creating table: " + e.getMessage());
        System.exit(1);
    }
}

public static void createCluster(RedshiftClient redshiftClient, String
clusterId, String masterUsername,
                                String masterUserPassword) {
    try {
        CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .masterUsername(masterUsername)
            .masterUserPassword(masterUserPassword)
            .nodeType("ra3.4xlarge")
            .publiclyAccessible(true)
            .numberOfNodes(2)
            .build();

        CreateClusterResponse clusterResponse =
redshiftClient.createCluster(clusterRequest);
        System.out.println("Created cluster " +
clusterResponse.cluster().clusterIdentifier());

    } catch (RedshiftException e) {

        System.err.println(e.getMessage());
        System.exit(1);
    }
}
}
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans la référence de l'API AWS SDK for Java 2.x .
 - [createCluster](#)
 - [Décrire les clusters](#)
 - [Décrire une déclaration](#)
 - [Exécuter une instruction](#)
 - [obtenir StatementResult](#)
 - [liste DatabasesPaginator](#)
 - [Modifier le cluster](#)

Python

SDK pour 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 redshift_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.redshift_scenario(
        f"{os.path.dirname(__file__)}/../../resources/sample_files/
movies.json"
    )

```

Les fonctions wrapper utilisées dans le scénario.

```

def create_cluster(
    self,
    cluster_identifcier,
    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 d'informations sur l'API, consultez les rubriques suivantes dans AWS SDK for Python (Boto3) API Reference.
 - [createCluster](#)
 - [Décrire les clusters](#)
 - [Décrire une déclaration](#)
 - [Exécuter une instruction](#)

- [obtenir StatementResult](#)
- [liste DatabasesPaginator](#)
- [Modifier le cluster](#)

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Exemples multiservices pour Amazon AWS Redshift utilisant des kits de développement logiciel

Les exemples d'applications suivants utilisent des AWS SDK pour associer Amazon Redshift à d'autres applications. Services AWS Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions sur la façon de configurer et d'exécuter l'application.

Exemples

- [Créer un outil de suivi des éléments Amazon Redshift.](#)

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, consultez [Utilisation de ce service avec un AWS SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Historique du document

Note

Pour obtenir une description des nouvelles fonctionnalités d'Amazon Redshift, consultez la section [Nouveautés](#).

Le tableau suivant décrit les modifications importantes apportées à la documentation du 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](#).

Pour plus d'informations sur les nouvelles fonctions, y compris une liste des correctifs et les numéros de version de cluster associés pour chaque version de produit, consultez le [Historique des versions de cluster](#).

Modification	Description	Date
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 plus d'informations sur cette version, consultez le correctif 181 d'Amazon Redshift .	1er mai 2024

[Mise à jour des politiques gérées de l'éditeur de requêtes v2](#)

Mises à jour de AmazonRedshiftQueryEditorV2 FullAccess AmazonRedshiftQueryEditorV2 NoSharing AmazonRedshiftQueryEditorV2 ReadSharing , et politiques AmazonRedshiftQueryEditorV2ReadWriteSharing gérées avec 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](#)

Mises à jour de la politique AmazonRedshiftReadOnlyAccess gérée avec autorisation redshift:ListRecommendations de 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 Purpose : RedshiftMigrateToVpc resource.

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 pour les points de terminaison inter-VPC pour Amazon Redshift, alimenté par AWS PrivateLink	Vous pouvez à présent utiliser des points de terminaison d'un VPC gérés par RedShift 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 nœuds 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

Authentification multifacteur	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 description 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 documentation 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 et Configurer une connexion ODBC .	4 février 2019

Maintenance différée

20 novembre 2018

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](#).

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

[Nouveaux pilotes ODBC](#)

Les pilotes ODBC Amazon Redshift ont été mis à jour vers la version 1.4.3.1000. Pour plus d'informations, consultez [Configurer la connexion ODBC](#).

le 8 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 chiffrement 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'effectuer des étapes de configuration 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.

Modification	Description	Date de publication
Nouveaux CloudWatch indicateurs	De nouvelles CloudWatch mesures ont été ajoutées pour surveiller les performances des requêtes. Pour de plus amples informations, veuillez consulter Surveillance d'Amazon Redshift à l'aide de métriques CloudWatch .	17 mai 2018
Chiffrement HSM	Amazon Redshift prend uniquement en charge la gestion AWS CloudHSM des clés du module de	6 mars 2018

Modification	Description	Date de publication
	sécurité matérielle (HSM). Pour plus d'informations, 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

Modification	Description	Date de publication
Certificats ACM	Amazon Redshift remplace les certificats SSL de vos clusters par des certificats émis 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
Rôles liés à un service	Un rôle lié à un service est un type unique de rôle IAM lié directement à Amazon Redshift. Les rôles liés aux services sont prédéfinis par Amazon Redshift et incluent toutes les autorisations requises par le service pour AWS appeler 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

Modification	Description	Date de publication
La restauration au niveau de la table prend en charge le routage VPC amélioré	La restauration au niveau de la table est désormais prise en charge sur les clusters qui utilisent Routage VPC amélioré . Pour plus d'informations, consultez Restauration d'une table à partir d'un instantané .	19 juillet 2017
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 Configuration de la 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 Amélioration du routage VPC dans Amazon 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
Nouveaux pilotes ODBC	Les pilotes ODBC Amazon Redshift ont été mis à jour vers la version 1.2.7.1007. Pour plus d'informations, consultez Configuration d'une connexion ODBC .	30 mars 2016

Modification	Description	Date de publication
Rôles IAM pour les commandes COPY et UNLOAD	Vous pouvez désormais spécifier un ou plusieurs rôles AWS Identity and Access Management (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 Autoriser Amazon Redshift à accéder à d'AWS autres 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 son 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

Modification	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 des instantanés chiffrés vers une autre région AWS .	28 juillet 2015

Modification	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 Présentation .	9 juin 2015
Nouveaux pilotes ODBC	Le pilote ODBC Amazon Redshift a été mis à jour. Ajout d'une section pour les versions antérieures de ces pilotes et d'un lien vers les notes de mise à jour des pilotes. Pour plus d'informations, consultez Configuration d'une connexion ODBC .	5 juin 2015
Correctifs de la documentation	Publication de divers correctifs de la documentation.	30 avril 2015

Modification	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 Connexion 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	Mise à jour des recommandations sur la configuration de l'unité de transmission maximale (MTU) pour désactiver les trames jumbo TCP/IP. Pour plus d'informations, consultez Utilisez EC2-VPC lorsque vous créez 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 <code>wlm_json_configuration</code> relatif au paramètre et fourni un exemple de syntaxe pour configurer ce paramètre à AWS CLI l'aide des systèmes d'exploitation Linux, MacOS X et Microsoft Windows. Pour plus d'informations, consultez Configuration de la gestion de la charge de travail .	13 janvier 2015

Modification	Description	Date de publication
Mise à jour de la documentation	Ajout des notifications d'événements et des descriptions manquantes. Pour plus d'informations, consultez Catégories d'événements et messages d'événements 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 Gestion des clusters à l'aide de la console .	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 Étiquetage des ressources Amazon Redshift .	4 novembre 2014

Modification	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
Mise à jour de la documentation	Ajout de liens aux packages redistribuables Microsoft Visual C++ 2010 qui sont nécessaires à Amazon Redshift pour utiliser les pilotes ODBC PostgreSQL. Pour plus d'informations, consultez Installer et configurer le pilote ODBC Amazon Redshift sur Microsoft Windows .	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 de clusters 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 Présentation d'Amazon Redshift .	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 Gestion des clusters à l'aide de la console .	11 juillet 2014

Modification	Description	Date de publication
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 des clusters .	27 juin 2014
Nouvelle fonctionnalité	Ajout de la possibilité de renommer les clusters. Pour plus d'informations, consultez Renommer les clusters et Modification d'un cluster .	2 juin 2014
Mise à jour de la documentation	Mise à jour de l'exemple de code .NET pour utiliser le fournisseur de données ODBC lors de la connexion à un cluster par programmation à l'aide de .NET. Pour plus d'informations, consultez Connectez-vous à votre entrepôt de données par programmation .	15 mai 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 pour décrire comment configurer une CloudWatch alarme Amazon par défaut afin de 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 Connexion à l'aide du protocole SSL .	22 avril 2014

Modification	Description	Date de publication
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 Connexion à l'aide du protocole SSL .	18 avril 2014
Mise à jour de la documentation	Révision et réorganisation des rubriques de la section Connexion 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
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 Achat de nœuds réservés pour Amazon Redshift .	2 avril 2014
Nouvelle fonctionnalité	Ajout d'une section sur un nouveau paramètre, <code>max_cursor_result_set_size</code> , 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

Modification	Description	Date de publication
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
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 Gestion des clusters dans un VPC et Création d'un cluster 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

Modification	Description	Date de publication
Nouvelle fonctionnalité	Ajout d'informations sur le nouveau journal d'activité utilisateur et le paramètre de base de données <code>enable_user_activity_logging</code> 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
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 Copie d'instantanés sur une autre région AWS .	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

Modification	Description	Date de publication
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 pour Amazon Redshift à l'aide de modules de sécurité matérielle , et Rotation des clés de chiffrement dans Amazon Redshift .	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 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
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

Modification	Description	Date de publication
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

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.