aws

Management Guide

Amazon Redshift

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Redshift: Management Guide

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist Amazon Redshift? 1
Verwenden Sie Amazon Redshift zum ersten Mal? 1
Übersicht über die Funktionen von Amazon Redshift Serverless 2
Bereitgestellte Amazon-Redshift-Cluster – Überblick 5
Clusterverwaltung 5
Zugriff und Sicherheit bei Clustern 6
Überwachung von Clustern 8
Datenbanken 9
Vergleich zwischen Amazon Redshift Serverless und einem von Amazon Redshift bereitgestellten Data Warehouse 10
Verwendung der Amazon Redshift Redshift-Verwaltungsschnittstellen für bereitgestellte Cluster 38
Mit AWS SDKs arbeiten 39
Signieren von HTTP-Anforderungen 40
Einrichten der Amazon-Redshift-CLI 47
Amazon Redshift Serverless 49
Was ist Amazon Redshift Serverless? 49
Konsole von Amazon Redshift Serverless 50
Überlegungen zur Verwendung von Amazon Redshift Serverless 54
Rechenkapazität für Amazon Redshift Serverless 57
Grundlegendes zur Amazon-Redshift-Serverless-Kapazität 57
KI-gestützte Skalierung und Optimierung (Vorschau) 58
Fakturierung für Amazon Redshift Serverless 60
Preisgestaltung 60
Fakturierung für Rechenkapazität 60
Fakturierung für Speicher 65
Verwenden von kostenlosen Testversion von Amazon Redshift Serverless 66
Hinweise zur Fakturierungsnutzung 66
Verbinden mit Amazon Redshift Serverless 68
Verbinden mit Amazon Redshift Serverless 68
Verbinden mit Amazon Redshift Serverless über JDBC-Treiber 69
Verbinden mit Amazon Redshift Serverless über die Daten-API 71
Verbinden mit Amazon Redshift Serverless über SSL 71

Herstellen einer Verbindung mit Amazon Redshift Serverless von einem von Amazon Redshift verwalteten VPC-Endpunkt aus ... 73
Verbinden mit Amazon Redshift Serverless über einen Redshift-VPC-Endpunkt in einem anderen Konto oder einer anderen Region ... 73
Konfiguration geeigneter Netzwerkverkehrseinstellungen für Amazon Redshift Serverless ... 79
Definieren von Datenbankrollen, die Verbundbenutzern in Amazon Redshift Serverless zugewiesen werden sollen ... 79
Weitere Ressourcen ... 79
Definieren von Datenbankrollen, die Verbundbenutzern in Amazon Redshift Serverless zugewiesen werden sollen ... 79
Identity and Access Management in Amazon Redshift Serverless ... 83
Amazon Redshift Serverless Berechtigungen gewähren ... 83
Erste Schritte mit IAM-Anmeldeinformationen für Amazon Redshift ... 86
Verwalten des Zugriffs auf Datenbankobjekte von Amazon Redshift Serverless mit Datenbankrollenberechtigungen ... 87
Migrieren eines bereitgestellten Clusters zu Amazon Redshift Serverless ... 89
Erstellen eines Snapshots Ihres bereitgestellten Clusters ... 89
Herstellen einer Verbindung mit Amazon Redshift Serverless über einen Treiber ... 90
Verwenden des Amazon-Redshift-Serverless-SDK ... 93
Übersicht über Arbeitsgruppen und Namespaces in Amazon Redshift Serverless ... 93
Übersicht über Arbeitsgruppen und Namespaces in Amazon Redshift Serverless ... 93
Verwalten von Amazon Redshift Serverless mithilfe der Konsole ... 96
Ersteinrichtung von Amazon Redshift Serverless ... 96
Arbeiten mit Arbeitsgruppen ... 96
Arbeiten mit Namespaces ... 102
Verwalten von Nutzungs- und Abfragelimits und andere administrative Aufgaben ... 107
Überwachen von Abfragen und Workloads mit Amazon Redshift Serverless ... 109
Überwachen von Abfragen und Workloads mit Amazon Redshift Serverless ... 109
Prüfungsprotokollierung für Amazon Redshift Serverless ... 114
Exportieren von Protokollen ... 114
Arbeiten mit Snapshots und Wiederherstellungspunkten ... 124
Snapshots ... 125
Wiederherstellungspunkte ... 129
Planen von Snapshots ... 129
Kopieren von Sicherungen zu einer anderen AWS-Region ... 133
Wiederherstellen einer Tabelle ... 134

Verwenden der AWS Command Line Interface und Amazon-Redshift-Serverless-API 136
Datenfreigabe in Amazon Redshift Serverless 139
Datenfreigabe in Amazon Redshift Serverless 139
Markieren von Ressourcen – Übersicht 141
Von Amazon Redshift bereitgestellte Cluster 143
Überblick über Amazon Redshift 143
Cluster und Knoten 144
Verwenden von EC2-VPC beim Erstellen Ihres Clusters 150
EC2-VPC 150
EC2-Classic 151
Starten Sie einen Cluster. 151
Standard-Festplattenspeicherplatzalarm 152
Cluster-Status 153
Überlegungen zur Verwendung von von Amazon Redshift bereitgestellten Clustern 155
Überlegungen zu Regionen und Availability Zones 156
Clusterwartung 156
Verwalten von Nutzungslimits 163
Netzwerkfunktionen, die von RA3-Knoten unterstützt werden 165
Knotentypen 166
Cluster-Operationen 179
Größenanpassung von Clustern 180
Anhalten und Fortsetzen von Clustern 197
Umbenennen von Clustern 199
Schließen und Löschen von Clustern 200
Verlagerung Ihres Clusters 201
Snapshots und Sicherungen 207
Konfigurieren einer Multi-AZ-Bereitstellung 239
Einrichten einer Multi-AZ-Bereitstellung 239
Verwalten der Multi-AZ-Bereitstellung 242
Failover bei einer Multi-AZ-Bereitstellung 250
Abfrageüberwachung für Multi-AZ 252
Verwalten von Clustern mithilfe der Konsole 255
Erstellen eines Clusters 256
Erstellen eines Vorschau-Clusters 260
Modifizieren eines Clusters 261
Löschen eines Clusters 262

Neustart eines Clusters ... 263
Größenanpassung eines Clusters ... 264
Upgrade der Release-Version eines Clusters ... 264
Abruf von Informationen zur Clusterkonfiguration ... 265
Anzeige einer Übersicht über den Cluster-Status ... 265
Erstellen eines Snapshots eines Clusters ... 266
Erstellen oder Bearbeiten eines Speicherplatzalarms ... 266
Arbeiten mit Cluster-Leistungsdaten ... 266
Verwaltung von Clustern mithilfe der AWS CLI und der Amazon Redshift Redshift-API ... 267
Verwaltung von Clustern in einer VPC ... 268
Übersicht ... 268
Erstellen eines Clusters in einer VPC ... 271
Verwalten von VPC-Sicherheitsgruppen für einen Cluster ... 272
Konfigurieren der Kommunikationseinstellungen von Sicherheitsgruppen für einen Amazon-Redshift-Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe ... 274
So funktioniert Amazon Redshift mit VPC-Freigabe für AWS-Ressourcen ... 277
Cluster-Subnetzgruppen ... 279
Cluster-Versionsverlauf ... 282
Arbeiten mit Null-ETL-Integrationen ... 283
Überlegungen ... 285
Erste Schritte mit Null-ETL-Integrationen ... 287
Erstellen und Konfigurieren eines Ziel-Data-Warehouse in Amazon Redshift ... 288
Unterscheidung zwischen Groß- und Kleinschreibung aktivieren ... 290
Autorisierung in Amazon Redshift konfigurieren ... 293
Nächste Schritte ... 297
Zieldatenbanken erstellen ... 297
Erstellen einer Zieldatenbank in Amazon Redshift ... 298
Hinzufügen von Daten zu Ihrer Quelle ... 299
Abfragen und Erstellen von materialisierten Ansichten mit replizierten Daten ... 300
Abfragen von replizierten Daten in Amazon Redshift ... 300
Erstellen von materialisierten Ansichten mit replizierten Daten ... 300
Verwalten von Null-ETL-Integrationen ... 302
Freigeben Ihrer Daten in Amazon Redshift ... 304
Metriken für Null-ETL-Integrationen ... 306
Fehlerbehebung bei Null-ETL-Integrationen ... 307
Abfragen einer Datenbank ... 318

Abfragen für Datenbanken mit dem Amazon-Redshift-Abfrage-Editor v2 319
Konfiguration Ihres AWS-Konto 320
Arbeiten mit dem Abfrage-Editor v2 328
Interaktion mit generativem SQL in Query Editor v2 (Vorschau) 348
Laden von Daten in eine Datenbank 356
Erstellen und Ausführen von Abfragen 367
Erstellen und Ausführen von Notebooks 373
Abfragen der AWS Glue Data Catalog 377
Abfragen eines Data Lake 380
Arbeiten mit Datashares 383
Planen einer Abfrage 386
Visualisieren von Ergebnissen 397
Zusammenarbeiten und Teilen im Team 404
Abfragen für Datenbanken mit dem Abfrage-Editor 406
Überlegungen 407
Aktivieren des Zugriffs 408
Verbinden mit dem Abfrage-Editor 409
Arbeiten mit dem Abfrage-Editor 411
Planen einer Abfrage 412
Mithilfe von SQL-Client-Tools eine Verbindung zu einem Data Warehouse herstellen 417
Empfehlungen für die Verbindung mit Client-Tools 418
Konfigurieren von Verbindungen in Amazon Redshift 419
Konfigurieren von Sicherheitsoptionen für Verbindungen 603
Herstellen von Verbindungen von Client-Tools aus und mit Code 612
Verbinden mit SQL Workbench/J 663
Stellen Sie programmgesteuert Connect zu Ihrem Data Warehouse her 664
Verwenden eines Authentifizierungsprofils zur Verbindung mit Amazon Redshift 664
Beheben von Problemen mit Verbindungen in Amazon Redshift 667
Verwenden der Daten-API 676
Arbeiten mit der Data API 676
Wichtige Punkte beim Aufrufen der Data API 677
Ausführen von SQL-Anweisungen mit einem Idempotenz-Token 683
Autorisieren des Zugriffs 685
Aufrufen der Daten-API 692
Fehlerbehebung bei Problemen mit der Data-API 717
Planung von Daten-API-Vorgängen mit Amazon EventBridge 718

Überwachen der Data API ... 723
Parametergruppen ... 726
Übersicht ... 726
Über Parametergruppen ... 726
Standard-Parameterwerte ... 727
Konfiguration von Parameterwerten mit der AWS CLI ... 729
Workload-Management-Konfiguration ... 730
Dynamische und statische WLM-Eigenschaften ... 731
Eigenschaften des Parameters wlm_json_configuration ... 731
Konfiguration des Parameters wlm_json_configuration mit der AWS CLI ... 739
Verwaltung von Parametergruppen mit der Konsole ... 748
Erstellen einer Parametergruppe ... 749
Modifizieren einer Parametergruppe ... 749
Erstellen oder Modifizieren einer Abfrageüberwachungsregel mit der Konsole ... 752
Löschen einer Parametergruppe ... 754
Zuordnung einer Parametergruppe zu einem Cluster ... 754
Verwalten von Parametergruppen mit der AWS CLI und der Amazon Redshift API ... 755
Integration mit einem Partner AWS ... 756
Integration mit einem AWS Partner über die Amazon Redshift Redshift-Konsole ... 756
Daten mit AWS Partnern werden geladen ... 758
Kauf reservierter Knoten ... 759
Übersicht ... 759
Über Angebote reservierter Knoten ... 760
Vergleich der Preise für Lösungen mit reservierten Knoten ... 761
So funktionieren reservierte Knoten: ... 762
Reservierte Knoten und konsolidierte Fakturierung ... 763
Beispiele für reservierte Knoten ... 764
Kauf einer reservierten Knotenlösung mit der Konsole ... 765
Aktualisierung reservierter Knoten mit dem AWS CLI ... 766
Kaufen eines Angebots reservierter Knoten über die AWS CLI und die Amazon-Redshift-API ... 768
Sicherheit ... 769
Datenschutz ... 771
Datenverschlüsselung ... 772
Datenaufgliederung in Token ... 792
Richtlinie für den Datenverkehr zwischen Netzwerken ... 792
Identity and Access Management ... 793

Authentifizierung mit Identitäten ... 794
Zugriffskontrolle ... 797
Übersicht über die Verwaltung von Zugriffsberechtigungen ... 798
Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) ... 805
Nativer Identitätsanbieter(IdP)-Verbund für Amazon Redshift ... 866
Connect Redshift mit IAM Identity Center, um Benutzern eine Single-Sign-On-Erfahrung zu bieten ... 871
Verwenden von serviceverknüpften Rollen ... 888
Verwenden der IAM-Authentifizierung zur Erstellung von Anmeldeinformationen für Datenbankbenutzern ... 894
Autorisieren von Amazon Redshift für den Zugriff auf Dienste AWS ... 956
Verwaltung von Amazon Redshift Redshift-Administratorkennwörtern mit AWS Secrets Manager ... 993
Für die AWS Secrets Manager Integration sind Berechtigungen erforderlich ... 994
Rotieren des Secrets mit dem Administratorpasswort ... 995
Abrufen des Amazon-Ressourcennamens (ARN) des Secrets in Amazon Redshift ... 995
Ein Geheimnis für Datenbankverbindungsdaten erstellen ... 996
Überlegungen zur Verwendung AWS Secrets Manager mit Amazon Redshift ... 998
Protokollierung und Überwachung ... 998
Datenbank-Prüfungsprotokollierung ... 999
Protokollieren mit CloudTrail ... 1012
Compliance-Validierung ... 1024
Ausfallsicherheit ... 1026
Sicherheit der Infrastruktur ... 1026
Netzwerkisolierung ... 792
Sicherheitsgruppen ... 1028
Verbinden über einen Schnittstellen-VPC-Endpunkt ... 1029
Konfigurations- und Schwachstellenanalyse ... 1035
Netzwerkaufgaben ... 1036
Verwenden eines benutzerdefinierten Domain-Namens für Client-Verbindungen ... 1036
Sicherheit für einen benutzerdefinierten Domain-Namen ... 1037
Einrichten eines benutzerdefinierten Domain-Namens ... 1037
Arbeiten mit von RedShift verwalteten VPC-Endpunkten ... 1048
Überlegungen ... 1049
Verwaltung von Endpunkten mit der Redshift-Konsole ... 1050
Verwaltung mit dem AWS CLI ... 1052

Verwalten mit Amazon-Redshift-API-Operationen ... 1052
Verwaltung mit AWS CloudFormation ... 1053
Enhanced VPC routing (Erweitertes VPC-Routing ... 1053
Arbeiten mit VPC-Endpunkten ... 1055
Enhanced VPC routing (Erweitertes VPC-Routing ... 1056
Redshift Spectrum und Enhanced VPC Routing ... 1058
Überwachung der Leistung von Clustern ... 1063
Übersicht ... 1063
Leistungsdaten ... 1064
Amazon-Redshift-Metriken ... 1065
Dimensionen für Amazon Redshift-Metriken ... 1076
Abfrage- und Ladeleistungsdaten von Amazon Redshift ... 1079
Arbeiten mit Leistungsdaten ... 1080
Anzeigen von Cluster-Leistungsdaten ... 1081
Anzeigen der Abfrageverlaufsdaten ... 1090
Anzeigen von Datenbankleistungsdaten ... 1094
Anzeigen der Parallelität des Workloads und der Parallelitätsskalierungsdaten ... 1098
Anzeigen von Abfragen und Ladevorgänge ... 1100
Anzeigen von Cluster-Metriken während der Ausführung von Lade-Operationen ... 1105
Analysieren der Workload-Leistung ... 1106
Verwalten von Alarmen ... 1109
Arbeiten mit Leistungskennzahlen in der CloudWatch Konsole ... 1110
Ereignisse ... 1112
Übersicht über Cluster-Ereignisse ... 1112
Arbeiten mit Amazon Simple Notification Service ... 1113
Abonnieren von Cluster-Ereignisbenachrichtigungen von Amazon Redshift ... 1114
Anzeigen von Cluster-Ereignissen unter Verwendung der Konsole ... 1116
Cluster-Ereignisse mithilfe der Amazon Redshift-API AWS CLI und der Amazon Redshift Redshift-API anzeigen ... 1116
Verwalten von Cluster-Ereignisbenachrichtigungen ... 1117
Verwalten von Cluster-Ereignisbenachrichtigungen mit der Amazon-Redshift-Konsole ... 1117
Verwaltung von Cluster-Ereignisbenachrichtigungen mithilfe der AWS CLI und der Amazon Redshift Redshift-API ... 1117
Ereignisbenachrichtigungen zu Amazon Redshift ... 1118
Amazon-Redshift-Ereigniskategorien und -Ereignismeldungen ... 1118
Ereignisbenachrichtigungen von Amazon Redshift Serverless mit Amazon EventBridge ... 1144

Ereignisbenachrichtigungen zur Null-ETL-Integration mit Amazon EventBridge 1152
Kontingente und -Einschränkungen 1163
Kontingente für Amazon-Redshift-Objekte 1163
Kontingente für Objekte von Amazon Redshift Serverless 1171
Kontingente für die Amazon-Redshift-Daten-API 1173
Kontingente für Objekte im Abfrage-Editor v2 1176
Kontingente und Limits in Objekten von Amazon Redshift Spectrum 1178
Benennungseinschränkungen: 1179
Tagging 1183
Markieren – Übersicht 1183
Anforderungen zum Markieren 1184
Verwalten der Ressourcen-Tags über die Konsole 1185
Verwalten von Tags über die Amazon Redshift API 1185
Cluster-Versionen 1187
Patch 180 1187
Neue Features 1188
Patch 179 1189
Neue Features 1190
Patch 178 1191
Neue Features 1192
Patch 177 1194
Neue Features 1195
Patch 176 1196
Neue Features 1197
Patch 175 1198
Neue Features 1199
Patch 174 1199
Neue Funktionen für diese Version 1199
Neue Funktionen für diese Version 1199
Neue Funktionen für diese Version 1199
Neue Funktionen für diese Version 1199
Neue Funktionen für diese Version 1199
Neue Funktionen für diese Version 1199
Neue Funktionen für diese Version 1199
Patch 173 1201
Neue Funktionen für diese Version 1201

Neue Funktionen für diese Version 1201
Neue Funktionen für diese Version 1201
Neue Funktionen für diese Version 1201
Neue Funktionen für diese Version 1201
Neue Funktionen für diese Version 1201
Neue Funktionen für diese Version 1201
Neue Funktionen für diese Version 1201
Neue Funktionen für diese Version 1201
Neue Funktionen für diese Version 1201
Patch 172 1202
Neue Features 1203
Patch 171 1203
Neue Features 1204
Patch 170 1204
Neue Features 1204
Patch 169 1204
Neue Features 1205
Patch 168 1205
Neue Funktionen 1205
Codebeispiele 1206
Aktionen 1208
Erstellen eines -Clusters 1209
Erstellen einer Tabelle 1213
Einen Cluster löschen 1214
Beschreiben Sie eine Abfrageanweisung 1218
Beschreiben Sie Cluster 1219
Rufen Sie das Kontoauszugsergebnis ab 1224
Fügen Sie Daten in eine Tabelle ein 1226
Modifizieren Sie einen Cluster 1228
Abfragen einer Tabelle 1231
Szenarien 1233
Erste Schritte mit Amazon Redshift 1233
Serviceübergreifende Beispiele 1247
Erstellen einer Webanwendung zur Verfolgung von Amazon-Redshift-Daten 1247
Dokumentverlauf 1249
..... mcclxxx

Was ist Amazon Redshift?

Willkommen beim Amazon-Redshift-Verwaltungshandbuch. Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service in Petabytegröße in der Cloud. Mit Amazon Redshift Serverless können Sie auf Daten zugreifen und diese analysieren, ohne alle Konfigurationen wie bei einem bereitgestellten Data Warehouse vornehmen zu müssen. Ressourcen werden automatisch bereitgestellt und die Data-Warehouse-Kapazität wird intelligent skaliert, um eine schnelle Leistung selbst für anspruchsvollste und unvorhersehbare Workloads zu erzielen. Es fallen keine Kosten an, wenn das Data Warehouse inaktiv ist, Sie zahlen also nur für das, was Sie tatsächlich nutzen. Sie können Daten laden und sofort mit der Abfrage beginnen. Hierfür können Sie Amazon Redshift Query Editor v2 oder Ihr bevorzugtes Business Intelligence (BI)-Tool nutzen. Genießen Sie das beste Preis-Leistungs-Verhältnis und die vertrauten SQL-Funktionen in einer easy-to-use Umgebung ohne Verwaltungsaufwand.

Amazon Redshift bietet unter Verwendung derselben SQL-basierten Tools und Business-Intelligence-Anwendungen, die Sie bereits heute verwenden, eine hohe Abfrageleistung und eine schnelle Abfrageausführung, unabhängig von der Größe des Datensatzes.

Verwenden Sie Amazon Redshift zum ersten Mal?

Wenn Sie Amazon Redshift zum ersten Mal verwenden, empfehlen wir Ihnen, zunächst die folgenden Abschnitte zu lesen:

- Service-Merkmale und Preise – Auf der Produktdetailseite werden das Nutzenversprechen, die Service-Merkmale und die Preise von Amazon Redshift erläutert.
- Erste Schritte mit Amazon Redshift Serverless – Unter diesem Thema erfahren Sie, wie Sie ein Serverless Data Warehouse einrichten, Ressourcen erstellen und Beispieldaten abfragen.
- Datenbankentwicklerhandbuch zu Amazon Redshift – Dieses Handbuch, das sich an Datenbankentwickler richtet, erläutert das Entwickeln, Erstellen, Abfragen und Pflegen der Datenbanken, die Ihr Data Warehouse bilden.

Wenn Sie Ihre Amazon-Redshift-Ressourcen lieber manuell verwalten möchten, können Sie bereitgestellte Cluster für Ihre Datenabfrageanforderungen erstellen. Weitere Informationen finden Sie unter Amazon-Redshift-Cluster.

Als Anwendungsentwickler können Sie die Amazon Redshift Redshift-API oder die AWS Software Development Kit (SDK) -Bibliotheken verwenden, um Cluster programmgesteuert zu verwalten.

Wenn Sie die Amazon Redshift Redshift-API verwenden, müssen Sie jede HTTP- oder HTTPS-Anfrage an die API authentifizieren, indem Sie sie signieren. Weitere Informationen zum Signieren von Anforderungen finden Sie unter Signieren von HTTP-Anforderungen.

Weitere Informationen zur API, zur CLI und zu den SDKs finden Sie unter den folgenden Links:

- Amazon Redshift Serverless – API-Referenz
- Amazon Redshift API-Referenz
- Amazon-Redshift-Daten-API – API-Referenz
- AWS CLI Befehlsreferenz
- SDK-Referenzen in Tools für Amazon Web Services.

Übersicht über die Funktionen von Amazon Redshift Serverless

Die meisten Funktionen, die von einem von Amazon Redshift bereitgestellten Data Warehouse unterstützt werden, werden auch von Amazon Redshift Serverless unterstützt. Im Folgenden sind einige der wichtigsten Funktionen aufgeführt.

Funktion	Beschreibung
Snapshots	Sie können einen Snapshot von Amazon Redshift Serverless oder ein bereitgestelltes Data Warehouse in Amazon Redshift Serverless wiederherstellen. Weitere Informationen finden Sie unter Arbeiten mit Snapshots und Wiederherstellungspunkten.
Wiederherstellungspunkte	Amazon Redshift Serverless erstellt automatisch alle 30 Minuten einen Wiederherstellungspunkt. Diese Wiederherstellungspunkte werden 24 Stunden lang gespeichert. Sie können sie zur Wiederherstellung nach versehentlichem Überschreiben oder Löschen verwenden. Wenn Sie von einem Wiederherstellungspunkt wiederherstellen, werden alle Daten in Ihrer Amazon-Redshift-Serverless-Datenbank zu einem früheren Zeitpunkt wiederhergestellt. Sie können einen Snapshot auch von einem Wiederherstellungspunkt aus erstellen, wenn Sie einen Wiederherstellungspunkt für einen längeren Zeitraum beibehalten müssen. Weitere Informationen finden Sie unter Arbeiten mit Snapshots und Wiederherstellungspunkten.

Funktion	Beschreibung
RPU-Basiskapazität	Sie können eine Basiskapazität in Redshift Processing Units (RPUs) festlegen . Eine RPU bietet 16 GB Arbeitsspeicher. Mit dieser Einstellung können Sie das Gleichgewicht zwischen verwendeten Ressourcen und Kosten für Ihre Workload steuern. Sie können diesen Wert steigern, um die verfügbaren Ressourcen zu erhöhen und die Abfrageleistung zu verbessern, oder den Wert senken, um Ihre Ausgaben zu begrenzen. Der Standardwert beträgt 128 RPUs. Sie können auch Nutzungslimits wie RPUs festlegen, die pro Tag verwendet werden, um die Kosten zu kontrollieren. Weitere Informationen finden Sie unter Fakturierung für Amazon Redshift Serverless.
Nutzungslimits für die Datenfreigabe	Sie können einschränken, wie viele Daten mit der Konsole oder der API von einer Produzentenregion an eine Konsumentenregion übertragen werden. Diese Datenübertragungskosten unterscheiden sich um AWS-Region Terabyte und werden in Terabyte gemessen. Weitere Informationen zur Datenfreigabe finden Sie unter Erste Schritte mit der Datenfreigabe über die Konsole im Datenbank entwicklerhandbuch zu Amazon Redshift.
Benutzerdefinierte Funktionen (User-defined functions, UDFs)	Sie können benutzerdefinierte Funktionen (UDFs) in Amazon Redshift Serverless ausführen. Weitere Informationen finden Sie unter Erstellen von benutzerdefinierten Funktionen im Datenbankentwicklerhandbuch zu Amazon Redshift.
Gespeicherte Prozeduren	Sie können gespeicherte Prozeduren in Amazon Redshift Serverless ausführen. Weitere Informationen finden Sie unter Erstellen von gespeicherten Prozeduren im Datenbankentwicklerhandbuch zu Amazon Redshift.
Materialisierte Ansichten	In Amazon Redshift Serverless können Sie materialisierte Ansichten erstellen. Weitere Informationen finden Sie unter Erstellen von materialisierten Ansichten im Datenbankentwicklerhandbuch zu Amazon Redshift.
Geofunktionen	Sie können Geofunktionen in Amazon Redshift Serverless ausführen. Weitere Informationen finden Sie unter Abfrage von Geodaten im Datenbankentwicklerhandbuch zu Amazon Redshift.

Funktion	Beschreibung
Verbundabfragen	Sie können Abfragen ausführen, um Daten von Amazon Redshift Serverless aus mit Aurora- und Amazon-RDS-Datenbanken zu verbinden. Weitere Informationen finden Sie unter Abfragen von Daten mit Verbundabfragen im Datenbankentwicklerhandbuch zu Amazon Redshift.
Data-Lake-Abfragen	Sie können Abfragen ausführen, um Daten von Ihrem Amazon S3 Data Lake aus mit Amazon Redshift Serverless zu verbinden. Weitere Informationen finden Sie unter Abfragen eines Data Lake im Amazon-Redshift-Verwaltungshandbuch.
HyperLogLog	Sie können HyperLogLog Funktionen in Amazon Redshift Serverless ausführen. Weitere Informationen finden Sie unter Using HyperLogLog Sketches im Amazon Redshift Database Developer Guide.
Datenbankübergreifendes Abfragen von Daten	Sie können Daten datenbankübergreifend mit Amazon Redshift Serverless abfragen. Weitere Informationen finden Sie unter Datenbankübergreifendes Abfragen von Daten im Datenbankentwicklerhandbuch zu Amazon Redshift.
Datenfreigabe	Sie können mit Amazon Redshift Serverless auf Datashares in bereitgestellten Data Warehouses zugreifen. Weitere Informationen finden Sie unter Dateifreigabe über Cluster hinweg im Datenbankentwicklerhandbuch zu Amazon Redshift.
Abfragen von halbstrukturierten Daten	Sie können halbstrukturierte Daten mit dem Datentyp SUPER mit Amazon Redshift Serverless erfassen und speichern. Weitere Informationen finden Sie unter Erfassen und Abfragen von halbstrukturierten Daten im Datenbankentwicklerhandbuch zu Amazon Redshift.
Markieren von Ressourcen	Sie können die AWS CLI oder die Amazon Redshift Serverless API verwenden, um Ressourcen mit Metadaten zu kennzeichnen, die sich auf die Ressource beziehen. Weitere Informationen finden Sie unter Markieren von Ressourcen.
Machine Learning	Sie können Amazon-Redshift-Machine-Learning mit Amazon Redshift Serverless verwenden. Weitere Informationen finden Sie unter Verwenden von Machine Learning im Datenbankentwicklerhandbuch zu Amazon Redshift.

Funktion	Beschreibung
SQL-Befehle und -Funktionen	Mit wenigen Ausnahmen (wie `REBOOT_CLUSTER`) können Sie Amazon-Redshift-SQL-Befehle und -Funktionen mit Amazon Redshift Serverless verwenden. Weitere Informationen finden Sie in der SQL-Referenz im Datenbankentwicklerhandbuch zu Amazon Redshift.
CloudFormation Ressourcen	Mithilfe von CloudFormation Vorlagen können Sie Amazon Redshift Serverless-Ressourcen bereitstellen und aktualisieren. Diese Integration bedeutet, dass Sie weniger Zeit mit der Verwaltung von Ressourcen verbringen und sich auf Ihre Anwendungen konzentrieren können. Weitere Informationen zu CloudFormation Ressourcen in Amazon Redshift Serverless finden Sie in der Amazon Redshift Serverless Resource Type Reference.
CloudTrail Ressourcen	Amazon Redshift Serverless ist integriert, AWS CloudTrail um eine Aufzeichnung der in Amazon Redshift Serverless durchgeführten Aktionen bereitzustellen. CloudTrail erfasst alle API-Aufrufe für Amazon Redshift Serverless als Ereignisse. Weitere Informationen finden Sie unter CloudTrail Amazon Redshift Serverless.

Bereitgestellte Amazon-Redshift-Cluster – Überblick

Der Amazon-Redshift-Service verwaltet alle Arbeiten zur Einrichtung, zum Betrieb und zum Skalieren eines Data Warehouse. Zu diesen Aufgaben gehören auch die Bereitstellung von Kapazitäten, die Überwachung und das Sichern des Clusters sowie das Anwenden von Patches und Upgrades auf die Amazon-Redshift-Engine.

Das folgende Video zeigt Ihnen, wie Sie mit Amazon Redshift Query Editor v2 einen Cluster erstellen und Daten abfragen.

Clusterverwaltung

Ein Amazon-Redshift-Cluster besteht aus einer Reihe von Knoten, darunter einem Führungsknoten und einem oder mehreren Rechenknoten. Die Anzahl und Art der benötigten Rechenknoten hängt von der Größe Ihrer Daten, der Anzahl der auszuführenden Abfragen und der benötigten Abfrage-Laufzeitleistung ab.

Erstellen und Verwalten von Clustern

Sie können, je nach Anforderungen an Ihr Data Warehousing, zunächst mit einem kleinen Cluster mit einem Arbeitsknoten beginnen, bei Bedarf jedoch problemlos die Anzahl der Knoten in dem Cluster beliebig hochskalieren, wenn sich Ihre Anforderungen ändern. Sie können einem Cluster im laufenden Betrieb Verarbeitungsknoten hinzufügen und entfernen. Weitere Informationen finden Sie unter Von Amazon Redshift bereitgestellte Cluster.

Reservieren von Datenverarbeitungsknoten

Wenn Sie planen, Ihren Cluster ein ganzes Jahr und länger zu betrieben, können Sie Geld sparen, indem Sie Knoten für einen Zeitraum von 1 oder 3 Jahren reservieren. Das Reservieren von Verarbeitungsknoten ist deutlich preisgünstiger als die Stundensätze, die anfallen, wenn Sie Verarbeitungsknoten auf Anfrage bereitstellen. Weitere Informationen finden Sie unter Kaufen reservierter Amazon-Redshift-Knoten.

Erstellen von Cluster-Snapshots

Snapshots sind point-in-time Backups eines Clusters. Es gibt zwei Arten von Snapshots: automatisierte und manuelle. Amazon Redshift speichert diese Snapshots intern in Amazon Simple Storage Service (Amazon S3) unter Verwendung einer verschlüsselten Secure Sockets Layer (SSL)-Verbindung. Wenn Sie einen Cluster anhand eines Snapshots wiederherstellen müssen, erstellt Amazon Redshift einen neuen Cluster und importiert dann die Daten aus dem von Ihnen angegebenen Snapshot. Weitere Informationen zu -Snapshots finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.

Zugriff und Sicherheit bei Clustern

Es gibt in Amazon Redshift mehrere Funktionen für den Zugriff auf und die Sicherheit von Clustern. Mit diesen Funktionen können Sie den Zugriff auf Ihre Cluster steuern, Konnektivitätsregeln definieren sowie Daten und Verbindungen verschlüsseln. Diese Funktionen ergänzen die Datenbankzugriffs- und Sicherheitsfunktionen in Amazon Redshift. Weitere Informationen zum Thema Datenbanksicherheit finden Sie unter Verwalten der Datenbanksicherheit im Datenbankentwicklerhandbuch zu Amazon Redshift.

AWS Konten und IAM-Anmeldeinformationen

Standardmäßig ist ein Amazon Redshift Redshift-Cluster nur für das AWS Konto zugänglich, das den Cluster erstellt. Der Cluster wird für den Zugriff durch andere Benutzer gesperrt. In Ihrem AWS Konto

verwenden Sie den AWS Identity and Access Management (IAM) -Service, um Benutzerkonten zu erstellen und die Berechtigungen für diese Konten zur Steuerung des Clusterbetriebs zu verwalten. Weitere Informationen finden Sie unter Sicherheit in Amazon Redshift. Weitere Informationen zur Verwaltung von IAM-Identitäten, einschließlich Leitlinien und bewährten Methoden für IAM-Rollen, finden Sie unter Identity and Access Management in Amazon Redshift.

Sicherheitsgruppen

Standardmäßig ist jeder von Ihnen erstellte Cluster für alle gesperrt. Mit den IAM-Anmeldeinformationen wird lediglich der Zugriff auf Amazon Redshift API-bezogene Ressourcen gesteuert: die Amazon-Redshift-Konsole, die Befehlszeilenschnittstelle (CLI), die API und das SDK. Zur Steuerung des Zugriffs auf den Cluster über SQL-Client-Tools über JDBC oder ODBC werden Sicherheitsgruppen verwendet:

- Wenn Sie für Ihren Amazon-Redshift-Cluster die EC2-VPC-Plattform nutzen, müssen Sie VPC-Sicherheitsgruppen verwenden. Wir empfehlen, Ihren Cluster auf einer EC2-VPC-Plattform zu starten.

  Sie können einen Cluster nicht zu einer VPC verschieben, nachdem er mit EC2-Classic gestartet wurde. Sie können mit der Amazon-Redshift-Konsole jedoch einen EC2-Classic-Snapshot auf einen EC2-VPC-Cluster wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot.
- Wenn Sie für Ihren Amazon-Redshift-Cluster die EC2-Classic-Plattform nutzen, müssen Sie Amazon-Redshift-Sicherheitsgruppen verwenden.

Sie müssen in beiden Fällen Regeln zur Sicherheitsgruppe hinzufügen, um explizit eingehenden Zugriff auf einen bestimmten Bereich von CIDR/IP-Adressen bzw. auf eine Amazon Elastic Compute Cloud (EC2)-Sicherheitsgruppe zu gewähren, falls Ihr SQL-Client auf einer Amazon-EC2-Instance ausgeführt wird. Weitere Informationen finden Sie unter Amazon-Redshift-Cluster-Sicherheitsgruppen.

Außer den eingehenden Zugriffsregeln müssen Sie auch Datenbankbenutzer anlegen, mit deren Anmeldeinformationen eine Authentifizierung an der Datenbank in dem Cluster selbst durchgeführt werden kann. Weitere Informationen finden Sie unter Datenbanken in diesem Thema.

Verschlüsselung

Wenn Sie den Cluster bereitstellen, können Sie ihn optional verschlüsseln und auf diese Weise zusätzlich schützen. Wenn die Verschlüsselung aktiviert ist, speichert Amazon Redshift alle Daten

in vom Benutzern erstellten Tabellen in verschlüsselter Form. Sie können AWS Key Management Service (AWS KMS) zur Verwaltung Ihrer Verschlüsselungsschlüssel für Amazon Redshift verwenden.

Verschlüsselung ist eine unveränderliche Eigenschaft eines Clusters. Die einzige Möglichkeit, von einem verschlüsselten Cluster zu einem nicht verschlüsselten Cluster zu wechseln, besteht darin, die Daten zu entladen und in einen neuen Cluster neu zu laden. Die Verschlüsselung gilt für den Cluster selbst sowie für alle Sicherungen. Wenn Sie einen Cluster aus einem verschlüsselten Snapshot wiederherstellen, wird auch der wiederhergestellte Cluster verschlüsselt.

Weitere Informationen zu Verschlüsselung in Hardwaresicherheitsmodulen finden Sie unter Verschlüsselung von Amazon-Redshift-Datenbanken.

SSL-Verbindungen

Wenn Sie die Verbindung zwischen Ihrem SQL-Client und Ihrem Cluster verschlüsseln möchten, können Sie eine verschlüsselte Secure Sockets Layer (SSL)-Verbindung verwenden. Weitere Informationen finden Sie unter Konfigurieren von Sicherheitsoptionen für Verbindungen.

Überwachung von Clustern

Es gibt in Amazon Redshift mehrere Funktionen zur Überwachung. Sie können die Datenbankprüfungs–Protokollierung verwenden, um Aktivitätsprotokolle zu erstellen und Ereignisse und Benachrichtigungsabonnements zu konfigurieren, um interessante Informationen zu verfolgen. Verwenden Sie die Metriken in Amazon Redshift und Amazon CloudWatch , um mehr über den Zustand und die Leistung Ihrer Cluster und Datenbanken zu erfahren.

Datenbank-Prüfungsprotokollierung

Sie können die Datenbank-Auditprotokollierung verwenden, um Informationen zu Authentifizierungsversuchen, Verbindungen, Verbindungstrennungen, Änderungen bezüglich der Definition der Datenbankbenutzer und in der Datenbank ausgeführten Abfragen zu erhalten. Diese Informationen können zu Sicherheits- und Fehlerbehebungszwecken in Amazon Redshift nützlich sein. Die Protokolle werden in Amazon-S3-Buckets gespeichert. Weitere Informationen finden Sie unter Datenbank-Prüfungsprotokollierung.

Ereignisse und Benachrichtigungen

Amazon Redshift verfolgt Ereignisse und speichert Informationen über sie für einen Zeitraum von mehreren Wochen in Ihrem AWS Konto. Amazon Redshift meldet bei jedem Ereignis Informationen

wie Datum und Uhrzeit, zu denen das Ereignis auftrat, eine Beschreibung, die Ereignisquelle (z. B. ein Cluster, eine Parametergruppe oder ein Snapshot) und die Quell-ID. Sie können Abonnements für Amazon-Redshift-Ereignisbenachrichtigungen erstellen, die eine Gruppe von Ereignisfiltern angeben. Wenn ein Ereignis eintritt, das den Filterkriterien entspricht, nutzt Amazon Redshift Amazon Simple Notification Service, um Sie über das Eintreten des Ereignisses zu informieren. Weitere Informationen zu Ereignissen und Benachrichtigungen finden Sie unter Amazon-Redshift-Ereignisse.

Leistung

Amazon Redshift stellt Leistungsmetriken und Daten bereit, mit denen Sie den Zustand und die Leistung Ihrer Cluster und Datenbanken überwachen können. Amazon Redshift verwendet CloudWatch Amazon-Metriken, um die physischen Aspekte des Clusters wie CPU-Auslastung, Latenz und Durchsatz zu überwachen. Amazon Redshift bietet außerdem Abfrage- und Ladeleistungsdaten, mit denen Sie die Datenbankaktivität in Ihrem Cluster überwachen können. Weitere Informationen zu Leistungsmetriken und -überwachung finden Sie unter Überwachen der Amazon-Redshift-Cluster-Leistung.

Datenbanken

Amazon Redshift erstellt eine einzige Datenbank, wenn Sie einen Cluster bereitstellen. Diese Datenbank wird verwendet, um Daten zu laden und Abfragen für Ihre Daten auszuführen. Sie können natürlich bei Bedarf weitere Datenbanken hinzufügen, indem Sie einen geeigneten SQL-Befehl ausführen. Weitere Informationen zum Erstellen weiterer Datenbanken finden Sie unter Schritt 1: Erstellen einer Datenbank im Datenbankentwicklerhandbuch zu Amazon Redshift.

Wenn Sie einen Cluster bereitstellen, geben Sie ein Administratorkonto an, das Zugriff auf alle Datenbanken hat, die in dem Cluster erstellt werden. Dieser Administrator ist ein Superuser und zunächst der einzige Benutzer, der auf die Datenbank zugreifen darf. Dieser Masterbenutzer darf dann weitere Superuser und Benutzer anlegen. Weitere Informationen finden Sie unter Superuser und Benutzer im Datenbankentwicklerhandbuch zu Amazon Redshift.

Amazon Redshift legt das Verhalten (z. B. das Anzeigeformat für Datumsangaben oder die Genauigkeit für Fließkommaberechnungen) für alle Datenbanken in einem Cluster über Parametergruppen fest. Wenn Sie bei der Bereitstellung Ihres Clusters kein Parametergruppe angeben, ordnet Amazon Redshift dem Cluster eine Standardparametergruppe zu. Weitere Informationen finden Sie unter Amazon-Redshift-Parametergruppen.

Weitere Informationen über Datenbanken in Amazon Redshift finden Sie im Datenbankentwicklerhandbuch zu Amazon Redshift.

Vergleich zwischen Amazon Redshift Serverless und einem von Amazon Redshift bereitgestellten Data Warehouse

Einige Konzepte und Funktionen von Amazon Redshift Serverless unterscheiden sich von den entsprechenden Funktionen eines von Amazon Redshift bereitgestellten Data Warehouse. Ein Unterschied besteht beispielsweise darin, dass Amazon Redshift Serverless keine Cluster oder Knoten verwendet. In der folgenden Liste werden Funktionen und Verhaltensweisen in Amazon Redshift Serverless beschrieben und es wird erläutert, inwieweit sie sich von einem bereitgestellten Data Warehouse unterscheiden.

Funktion	Beschreibung	Serverless	Bereitgestellt
Arbeitsgruppe und Namespace	Wenn Sie Workloads isolieren und verschiedene Ressourcen in Amazon Redshift Serverless verwalten möchten, können Sie Namespaces und Arbeitsgruppen erstellen, um Speicher- und Rechenres	Ein Namespace ist eine Sammlung von Datenbankobjekten und Benutzern. Eine Arbeitsgruppe ist eine Sammlung von Rechenressourcen. Weitere Informationen, die Ihnen helfen, das Design von	Ein bereitgestellter Cluster ist eine Sammlung von Rechenknoten und ein Leader-Knoten, die Sie direkt verwalten. Weitere Informationen finden Sie unter Von Amazon Redshift bereitgestellte Cluster.

Funktion	Beschreibung	Serverless	Bereitgestellt
	sourcen separat zu verwalten.	Amazon Redshift Serverless zu verstehen, finden Sie unter Amazon Redshift Serverless.	

Funktion	Beschreibung	Serverless	Bereitgestellt
Knotentypen	Wenn Sie mit Amazon Redshift Serverless arbeiten, wählen Sie keine Knotentypen aus oder geben die Knotenanzahl an wie bei einem bereitgestellten Amazon-Redshift-Cluster.	Amazon Redshift Serverless stellt die Kapazität automatisch für Sie bereit und verwaltet sie. Sie können die Basiskapazität des Data Warehouse optional angeben, um das richtige Preis-/Leistungsverhältnis für Ihre Workloads auszuwählen. Sie können auch maximale RPU-Stunden angeben, um	Sie erstellen einen Cluster mit Knotentypen, die Ihren Kosten- und Leistungsspezifikationen entsprechen. Weitere Informationen finden Sie unter Von Amazon Redshift bereitgestellte Cluster.

Funktion	Beschreibung	Serverless	Bereitgestellt
		Kostenkontrollen festzulegen und so die Vorhersehbarkeit der Kosten zu gewährleisten. Weitere Informationen finden Sie unter Grundlegendes zur Amazon-Redshift-Serverless-Kapazität.	

Funktion	Beschreibung	Serverless	Bereitgestellt
Workload-Management und Parallelitätsskalierung	Amazon Redshift kann für Zeiten mit hoher Auslastung skaliert werden. Amazon Redshift Serverless kann auch skaliert werden, um zeitweilig auftretende Zeiten hoher Auslastung zu bewältigen.	Amazon Redshift Serverless verwaltet Ressourcen automatisch effizient und skaliert basierend auf Workloads innerhalb der Schwellenwerte von Kostenkontrollen. Weitere Informationen finden Sie unter Fakturierung für Rechenkapazität.	Bei einem bereitgestellten Data Warehouse aktivieren Sie die Gleichzeitigkeitsskalierung in Ihrem Cluster, um Zeiten mit hoher Auslastung zu bewältigen. Weitere Informationen finden Sie unter Gleichzeitigkeitsskalierung.

Funktion	Beschreibung	Serverless	Bereitgestellt
Port	Die Portnummer, die Sie für die Verbindung verwenden.	Mit Amazon Redshift Serverless können Sie zu einem anderen Port aus dem Portbereich 5431–5455 oder 8191–8215 wechseln. Weitere Informationen finden Sie unter Verbinden mit Amazon Redshift Serverless.	Bei einem bereitgestellten Data Warehouse können Sie einen beliebigen Port für die Verbindung auswählen.

Funktion	Beschreibung	Serverless	Bereitgestellt
Größenanpassung	Fügen Sie Rechenressourcen hinzu oder entfernen Sie sie, um eine gute Leistung für die Workload zu erzielen.	Die Größenanpassung ist in Amazon Redshift Serverless nicht anwendbar. Sie können jedoch die Basis-RPU-Kapazität des Data Warehouse basierend auf Ihren Preis- und Leistungsanforderungen ändern. Weitere Informationen finden Sie unter Grundlegendes zur Amazon-Redshift-Serverless-Kapazität.	Bei einem bereitgestellten Cluster führen Sie eine Größenanpassung des Clusters aus, um Knoten hinzuzufügen oder zu entfernen. Weitere Informationen finden Sie unter Übersicht über die Verwaltung von Clustern in Amazon Redshift.

Funktion	Beschreibung	Serverless	Bereitgestellt
Anhalten und Fortsetzen	Wenn Sie keine Workloads ausführen müssen, können Sie einen bereitgestellten Cluster anhalten, um Kosten zu sparen.	Bei Amazon Redshift Serverless zahlen Sie, wenn Abfragen ausgeführt werden, sodass Anhalten oder Fortsetzen nicht erforderlich ist. Weitere Informationen finden Sie unter Fakturierung für Rechenkapazität.	Sie können einen Cluster basierend auf einer Bewertung der Workload zu verschiedenen Zeiten manuell anhalten und fortsetzen. Weitere Informationen finden Sie unter Übersicht über die Verwaltung von Clustern in Amazon Redshift.

Funktion	Beschreibung	Serverless	Bereitgestellt
Abfragen externer Daten mit Spectrum-Abfragen	Sie können Daten in Amazon-S3-Buckets in verschiedenen Formaten, z. B. JSON, abfragen.	Die Abrechnung erfolgt, wenn Rechenressourcen Workloads verarbeiten. Kosten fallen wie bei jeder anderen Transaktion an, wenn externe Redshift-Spectrum-Daten abgefragt werden. Weitere Informationen finden Sie unter Fakturierung für Rechenkapazität.	Bei einem bereitgestellten Data Warehouse ist die Kapazität von Amazon Redshift Spectrum auf separaten Servern vorhanden, die vom Amazon-Redshift-Cluster abgefragt werden. Weitere Informationen finden Sie unter Abfragen externer Daten mit Amazon Redshift Spectrum.

Funktion	Beschreibung	Serverless	Bereitgestellt
Abrechnung von Computerressourcen	So erfolgt die Abrechnung für Amazon Redshift im Vergleich zu Amazon Redshift Serverless.	Bei Amazon Redshift Serverless bezahlen Sie für die Workloads, die Sie ausführen, in RPU-Stunden pro Sekunde und einer Mindestgebühr von 60 Sekunden Dies schließt Abfragen ein, die auf Daten in geöffneten Dateiformaten in Amazon S3 zugreifen. Weitere Informationen finden Sie unter	Bei einem bereitgestellten Cluster erfolgt die Abrechnung pro Sekunde, wenn der Cluster nicht angehalten wurde.

Funktion	Beschreibung	Serverless	Bereitgestellt
		Fakturierung für Rechenkapazität.	
Wartungsfenster	So funktioniert die Serverwartung.	Bei Amazon Redshift Serverless gibt es kein Wartungsfenster. Updates werden nahtlos verarbeitet. Weitere Informationen finden Sie unter Was ist Amazon Redshift Serverless?.	Bei einem bereitgestellten Cluster geben Sie ein Wartungsfenster für Patches an. (In der Regel wählen Sie ein wiederkehrendes Zeitfenster, in dem die Auslastung gering ist.)

Funktion	Beschreibung	Serverless	Bereitgestellt
Verschlüsselung	Sie können die Datenbankverschlüsselung aktivieren.	Amazon Redshift Serverless ist immer mit AWS KMS, mit AWS verwalteten oder vom Kunden verwalteten Schlüsseln verschlüsselt.	Die Daten in einem bereitgestellten Data Warehouse können mit AWS KMS (mit AWS verwalteten oder vom Kunden verwalteten Schlüsseln) oder unverschlüsselt werden. Siehe Verschlüsselung von Amazon-Redshift-Datenbanken.
Speicherfakturierung	So wird Speicher abgerechnet.	Bei Amazon Redshift Serverless. Der Satz wird mit GB pro Monat berechnet. Siehe Fakturierung für Rechenkapazität.	Speicher wird abgesehen von Rechenressourcen für einen bereitgestellten Cluster mit RA3-Knoten in Rechnung gestellt.

Funktion	Beschreibung	Serverless	Bereitgestellt
Benutzerverwaltung	So werden Benutzer verwaltet.	Sowohl bei einem bereitgestellten Data Warehouse als auch bei Amazon Redshift Serverless sind Benutzer IAM- oder Redshift-Benutzer. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift Serverless. Weitere Informationen zur Verwaltung von IAM-	

Funktion	Beschreibung	Serverless	Bereitgestellt
		Identitäten, einschließlich bewährter Methoden für IAM-Rollen, finden Sie unter Identity and Access Management in Amazon Redshift.	

Funktion	Beschreibung	Serverless	Bereitgestellt
JDBC- und ODBC-Tools und -Kompatibilität	So funktionieren Client-Verbindungen.	Sowohl ein bereitgestelltes Data Warehouse als auch Amazon Redshift Serverless sind mit allen JDBC- oder ODBC-kompatiblen Tools oder Clientanwendungen kompatibel. Weitere Informationen zu Treibern finden Sie unter Konfigurieren von Verbindungen im Amazon-Redshift-Verwaltungs	

Funktion	Beschreibung	Serverless	Bereitgestellt
		handbuch. Weitere Informationen zum Verbinden mit Amazon Redshift Serverless finden Sie unter Konfigurieren von Verbindungen.	

Funktion	Beschreibung	Serverless	Bereitgestellt
Erfordernis von Anmeldeinformationen bei der Anmeldung	So werden Anmeldeinformationen verarbeitet.	Bei Amazon Redshift Serverless müssen Sie nicht in jeder Instance Anmeldeinformationen eingeben. Weitere Informationen finden Sie unter Verbinden mit Amazon Redshift Serverless.	Für den Zugriff auf Amazon Redshift sind Anmeldeinformationen von einem Benutzer erforderlich, dem eine IAM-Rolle zugewiesen ist. Der IAM-Rolle sind spezifische Berechtigungen für ein bereitgestelltes Data Warehouse angefügt. Nach der Authentifizierung kann sich der Benutzer direkt mit der Datenbank, der Redshift-Konsole und Query Editor v2 verbinden.

Funktion	Beschreibung	Serverless	Bereitgestellt
Daten-API	Sie können auf Daten von Webservices und anderen Anwendungen zugreifen.	Amazon Redshift Serverless unterstützt die Amazon-Redshift-Daten-API. Bei Amazon Redshift Serverless verwenden Sie den Parameter `workgroup-name` anstelle des Parameters `cluster-identity`. Weitere Informationen zum Aufrufen der Daten-API finden Sie unter Verwenden der	

Funktion	Beschreibung	Serverless	Bereitgestellt
		Amazon Redshift Data API.	
Snapshots	Sorgt für Wiederherstellung point-in-time .	Amazon Redshift Serverless unterstützt Snapshots und Wiederherstellungspunkte. Weitere Informationen zu Snapshots und Wiederherstellungspunkten für einen Namespace finden Sie unter Arbeiten mit Snapshots und Wiederherstellungspunkten.	Bereitgestellte Cluster unterstützen Snapshots. Weitere Informationen finden Sie unter Verwalten von Snapshots mithilfe der Konsole.

Funktion	Beschreibung	Serverless	Bereitgestellt
Datenfreigabe	Bietet die Möglichkeit, Daten aus Datenbanken desselben Kontos oder in verschiedenen Konten gemeinsam zu nutzen.	Amazon Redshift Serverless unterstützt alle Funktionen zur Datenfreigabe, die ein bereitgestelltes Data Warehouse bietet. Auch die Datenfreigabe zwischen Amazon Redshift Serverless und einem bereitgestellten Data Warehouse, einem Tool oder einer Client-Anwendung wird unterstützt.	Bereitgestellte Cluster unterstützen datenbank übergreifende, kontenübergreifende, regionsübergreifende und gemeinsame Nutzung von AWS Data Exchange Daten. Weitere Informationen finden Sie unter Freigeben von Daten über Cluster in Amazon Redshift.

Funktion	Beschreibung	Serverless	Bereitgestellt
Tracks	Stellt einen Zeitplan für Softwareupdates bereit.	Bei Amazon Redshift Serverless gibt es kein Konzept von Tracks. Versionen und Updates werden vom Service verarbeitet. Weitere Informationen zum Design von Amazon Redshift Serverless finden Sie unter Arbeiten mit Snapshots und Wiederherstellungspunkten.	Bereitgestellte Cluster unterstützen das Umschalten zwischen aktuellen und nachfolgenden Tracks.

Funktion	Beschreibung	Serverless	Bereitgestellt
Systemtabellen und Ansichten	Bietet eine Möglichkeit, Ihre Ressourcen und Systemmetadaten zu überwachen.	Amazon Redshift Serverless unterstützt neue Systemtabellen und Ansichten. Weitere Informationen zu Systemtabellen finden Sie unter Überwachungsansichten. Informationen dazu, wie Sie Ihre Abfragen von der Verwendung der älteren bereitgestellten Systemtabellen und Ansichten zu den neuen	Ein bereitgestelltes Data Warehouse unterstützt die vorhandenen Systemtabellen und Ansichten für die Überwachung und andere Aufgaben, die Systemmetadaten erfordern.

Funktion	Beschreibung	Serverless	Bereitgestellt
		Ansichten migrieren, finden Sie unter Migrieren zu SYS-Überwachungsansichten.	

Funktion	Beschreibung	Serverless	Bereitgestellt
Parametergruppen	Dabei handelt es sich um eine Gruppe von Parametern, die für alle Datenbanken gelten, die in einem Cluster erstellt werden. Diese Parameter konfigurieren Datenbankeinstellungen wie Abfrage-Timeout oder Datumsstil.	Bei Amazon Redshift Serverless gibt es das Konzept von Parametergruppen nicht.	Bereitgestellte Data Warehouses unterstützen Parametergruppen. Weitere Informationen zu Parametergruppen für einen bereitgestellten Cluster finden Sie unter Amazon-Redshift-Parametergruppen.

Funktion	Beschreibung	Serverless	Bereitgestellt
Abfrageüberwachung	Stellt eine zeitbasierte Ansicht der ausgeführten Abfragen bereit.	Für die Abfrageüberwachung in Amazon Redshift Serverless müssen Benutzer eine Verbindung zur Datenbank herstellen, um Systemtabellen verwenden zu können. Daher sind Abfrageüberwachung und Systemtabellen synchronisiert. Abfragen von Systemtabellen in Amazon Redshift Serverless	Die Abfrageüberwachung in bereitgestellten Clustern zeigt nicht alle Daten in Systemtabellen an.

Funktion	Beschreibung	Serverless	Bereitgestellt
		verwenden den Datenbankbenutzer zur Abfrageüberwachung, der dem IAM-Benutzer zugeordnet ist. Weitere Informationen zur Überwachung von Abfragen finden Sie unter Überwachen von Abfragen und Workloads mit Amazon Redshift Serverless.	

Funktion	Beschreibung	Serverless	Bereitgestellt
Audit-Protokollierung	Stellt Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereit.	Mit Amazon Redshift Serverless CloudWatch ist dies ein Ziel für Audit-Logs. Die Bereitstellung von Amazon-S3-basierten Audit-Protokollen wird für Amazon Redshift Serverless nicht unterstützt. Weitere Informationen finden Sie unter Audit-Protokollierung für Amazon Redshift Serverless.	Für einen bereitgestellten Cluster war die Bereitstellung von Amazon-S3-basierten Audit-Protokollen die Norm. Jetzt wurde die Bereitstellung von Audit-Protokollen auf CloudWatch bereitgestellte Data Warehouses ausgedehnt.

Funktion	Beschreibung	Serverless	Bereitgestellt
Ereignis-Benachrichtigungen	Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Ereignisdaten aus einer Vielzahl von Quellen verbinden können.	Amazon Redshift Serverless verwendet Amazon EventBridge zur Verwaltung von Ereignisbenachrichtigungen, um Sie up-to-date über Änderungen in Ihrem Data Warehouse auf dem Laufenden zu halten. Weitere Informationen finden Sie unter Ereignisbenachrichtigungen von Amazon Redshift	Bei einem bereitgestellten Cluster verwalten Sie Ereignisbenachrichtigungen mit der Amazon-Redshift-Konsole, um Ereignisabonnements zu erstellen. Weitere Informationen finden Sie unter Verwalten von Cluster-Ereignisbenachrichtigungen .

Funktion	Beschreibung	Serverless	Bereitgestellt
		Serverless mit Amazon EventBridge.	

Verwendung der Amazon Redshift Redshift-Verwaltungsschnittstellen für bereitgestellte Cluster

> **Note**
>
> Dieses Thema konzentriert sich auf Amazon Redshift Redshift-Verwaltungsschnittstellen für bereitgestellte Cluster. Es gibt ähnliche Verwaltungsschnittstellen für Amazon Redshift Serverless und Amazon Redshift Data API.

Amazon Redshift unterstützt mehrere Verwaltungsschnittstellen, mit denen Sie Amazon Redshift Redshift-Cluster erstellen, verwalten und löschen können: die AWS SDKs, die AWS Command Line Interface (AWS CLI) und die Amazon Redshift Redshift-Management-API.

Amazon Redshift API – Sie können diese Amazon Redshift Management API aufrufen, indem Sie eine Anforderung senden. Die Anforderungen sind HTTP- oder HTTPS-Anforderungen, die die HTTP-Verben `GET` oder `POST` mit einem Parameter namens `Action` verwenden. Das Aufrufen der Amazon Redshift API ist der direkteste Weg, auf den Amazon-Redshift-Service zuzugreifen. Es ist jedoch erforderlich, dass Ihre Anwendung Details auf unterer Ebene verarbeitet, wie beispielsweise die Fehlerbehandlung und das Erstellen eines Hash-Zeichens zum Signieren der Anforderung.

- Informationen zum Erstellen und Signieren einer Amazon Redshift API-Anforderung finden Sie unter Signieren von HTTP-Anforderungen.
- Informationen zu den Amazon Redshift API-Aktionen und Datentypen für Amazon Redshift finden Sie in der Amazon-Redshift-API-Referenz.

AWS SDKs — Sie können die AWS SDKs verwenden, um Amazon Redshift Redshift-Cluster-bezogene Operationen durchzuführen. Mehrere der SDK-Bibliotheken kapseln die zugrunde liegende Amazon Redshift API. Sie integrieren die API-Funktionalität in die spezifische Programmiersprache und verarbeiten viele der Details auf unterer Ebene wie beispielsweise die Berechnung der Signaturen, die Verarbeitung des erneuten Absendens von Anforderungen und die Fehlerbehandlung. Durch Aufrufen der Wrapper-Funktionen in den SDK-Bibliotheken kann der Prozess des Schreibens einer Anwendung zum Verwalten eines Amazon-Redshift-Clusters erheblich vereinfacht werden.

- Amazon Redshift wird von den AWS SDKs für Java, .NET, PHP, Python, Ruby und Node.js unterstützt. Die Wrapper-Funktionen für Amazon Redshift sind in den Referenzhandbüchern zu den einzelnen SDKs dokumentiert. Eine Liste der AWS SDKs und Links zu deren Dokumentation finden Sie unter Tools for Amazon Web Services.
- Dieses Handbuch bietet Beispiele für die Verwendung von Amazon Redshift mit dem Java-SDK. Allgemeinere AWS SDK-Codebeispiele finden Sie unterCodebeispiele für Amazon Redshift mit SDKs AWS.

AWS CLI— Die CLI bietet eine Reihe von Befehlszeilentools, mit denen Sie AWS Dienste von Windows-, Mac- und Linux-Computern aus verwalten können. Die AWS CLI enthält Befehle, die auf den Amazon Redshift API-Aktionen basieren.

- Informationen zur Installation und Einrichtung der Amazon-Redshift-CLI finden Sie unter Einrichten der Amazon-Redshift-CLI.
- Referenzmaterial zu den Amazon-Redshift-CLI-Befehlen finden Sie unter Amazon Redshift in der AWS CLI -Referenz.

Verwenden Sie diesen Dienst mit einem AWS SDK

AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Codebeispiele
AWS SDK for C++	AWS SDK for C++ Code-Beispiele

SDK-Dokumentation	Codebeispiele
AWS SDK for Go	AWS SDK for Go Code-Beispiele
AWS SDK for Java	AWS SDK for Java Code-Beispiele
AWS SDK for JavaScript	AWS SDK for JavaScript Code-Beispiele
AWS SDK for Kotlin	AWS SDK for Kotlin Code-Beispiele
AWS SDK for .NET	AWS SDK for .NET Code-Beispiele
AWS SDK for PHP	AWS SDK for PHP Code-Beispiele
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) Code-Beispiele
AWS SDK for Ruby	AWS SDK for Ruby Code-Beispiele
AWS SDK for Rust	AWS SDK for Rust Code-Beispiele
AWS SDK für SAP ABAP	AWS SDK für SAP ABAP Code-Beispiele
AWS SDK for Swift	AWS SDK for Swift Code-Beispiele

Beispiel für die Verfügbarkeit

Sie können nicht finden, was Sie brauchen? Fordern Sie ein Codebeispiel an, indem Sie unten den Link Feedback geben auswählen.

Signieren von HTTP-Anforderungen

In Amazon Redshift müssen alle Anforderungen, die Sie an die Verwaltungs-API senden, durch eine Signatur authentifiziert werden. In diesem Thema wird beschrieben, wie Sie Ihre HTTP-Anforderungen signieren.

Wenn Sie eines der AWS Software Development Kits (SDKs) oder das verwenden AWS Command Line Interface, erfolgt das Signieren von Anfragen automatisch, und Sie können diesen Abschnitt überspringen. Weitere Informationen zur Verwendung von AWS SDKs finden Sie unter. Verwendung der Amazon Redshift Redshift-Verwaltungsschnittstellen für bereitgestellte Cluster Weitere

Informationen zur Verwendung der Amazon-Redshift-Befehlszeilenschnittstelle finden Sie in der Amazon-Redshift-Befehlszeilenreferenz.

Zum Signieren einer Anforderung berechnen Sie mit einer kryptografischen Hash-Funktion eine digitale Signatur. Ein kryptografischer Hash ist eine Funktion, die einen einzigartigen, auf Grundlage der Eingabe berechneten Hash-Wert zurückgibt. Die Eingabe in die Hash-Funktion besteht aus dem Text Ihrer Anforderung und Ihrem geheimen Zugriffsschlüssel, den Sie aus den temporären Anmeldeinformationen ableiten können. Die Hash-Funktion gibt einen Hash-Wert zurück, den Sie in die Anforderung als Ihre Signatur einfügen. Die Signatur ist Teil des Headers `Authorization` in der Anforderung.

> **Note**
>
> Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS Management Console Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS
> Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS Command Line Interface Benutzerh andbuch. • Informationen zu AWS SDKs, Tools und AWS

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldedaten im Benutzerhandbuch. AWS CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Nachdem Amazon Redshift Ihre Anforderung erhalten hat, berechnet der Service die Signatur erneut unter Verwendung derselben Hash-Funktion und Eingaben, die Sie zum Signieren der Anforderung verwendet haben. Wenn die resultierende Signatur mit der Signatur in der Anforderung übereinstimmt, verarbeitet Amazon Redshift die Anforderung; ansonsten wird die Anforderung zurückgewiesen.

Amazon Redshift unterstützt die Authentifizierung mit AWS Signature Version 4. Der Prozess zum Berechnen einer Signatur lässt sich in drei Aufgaben untergliedern: Diese Aufgaben werden in dem folgenden Beispiel illustriert.

- Aufgabe 1: Erstellen einer kanonischen Anforderung

  Ordnen Sie Ihre HTTP-Anforderung in einer kanonischen Form an. Die Verwendung einer kanonischen Form ist erforderlich, weil Amazon Redshift bei der Berechnung der Signatur zum Vergleich mit der von Ihnen gesendeten Signatur dieselbe kanonische Form verwendet.

- Aufgabe 2: Erstellen einer zu signierenden Zeichenfolge

  Erstellen Sie eine Zeichenfolge, die Sie als einen der Eingabewerte für die kryptografische Hash-Funktion nutzen. Die als zu signierende Zeichenfolge bezeichnete Zeichenfolge ist eine Kombination aus dem Namen des Hash-Algorithmus, dem Anforderungsdatum, einer Zeichenfolge mit dem Umfang der Anmeldeinformationen und der kanonischen Anforderung aus der vorherigen Aufgabe. Die Zeichenfolge mit dem Umfang der Anmeldeinformationen selbst ist eine Kombination aus Datum, Region und Serviceinformationen.

- Aufgabe 3: Berechnen einer Signatur

  Berechnen Sie eine Signatur für Ihre Anforderung. Verwenden Sie dazu eine kryptografische Hash-Funktion, die zwei Eingabezeichenfolgen akzeptiert: die zu signierende Zeichenfolge und einen abgeleiteten Schlüssel. Der abgeleitete Schlüssel wird unter Nutzung des geheimen Zugriffsschlüssels und der Zeichenfolge mit dem Umfang der Anmeldeinformationen berechnet, um eine Reihe von Hash-Nachrichtenauthentifizierungscodes (HMAC-SHA256) zu erstellen.

Beispiel für eine Signatur-Berechnung

Das folgende Beispiel führt Sie durch die Einzelheiten der Erstellung einer Signatur für CreateClustereine Anfrage. Sie können dieses Beispiel als Referenz verwendet, um Ihre eigene Signaturberechnungsmethode zu überprüfen. Weitere Referenzberechnungen sind im Abschnitt Anfordern von Signaturbeispielen des IAM-Benutzerhandbuchs enthalten.

Sie können zum Senden von Anforderungen an Amazon Redshift wahlweise GET- oder POST-Anforderungen verwenden. Der Unterschied zwischen den beiden Anforderungen ist, dass bei GET die Abfrageparameter als Parameter in der Abfragezeichenfolge übermittelt werden. Bei POST werden die Abfrageparameter im Text der Anforderung übermittelt. In dem folgenden Beispiel ist eine POST-Anforderung dargestellt.

In diesem Beispiel wird Folgendes angenommen:

- Der Zeitstempel der Anforderung ist `Fri, 07 Dec 2012 00:00:00 GMT`.
- Der Endpunkt ist die Region USA Ost (Nord-Virginia), `us-east-1`.

Das allgemeine Format für Anforderungen lautet wie folgt:

```
https://redshift.us-east-1.amazonaws.com/
   ?Action=CreateCluster
   &ClusterIdentifier=examplecluster
   &MasterUsername=masteruser
   &MasterUserPassword=12345678Aa
   &NumberOfNode=2
   &NodeType=ds2.xlarge
   &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
```

Die kanonische Form der für Aufgabe 1: Erstellen einer kanonischen Anforderung berechneten Anforderung ist:

```
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
```

Die letzte Zeile der kanonischen Anforderungen ist der Hash des Anforderungstextes. Die dritte Zeile in der kanonischen Anforderung ist leer, weil dieser API-Aufruf keine Abfrageparameter hat.

Die zu signierende Zeichenfolge für Aufgabe 2: Erstellen einer zu signierenden Zeichenfolge ist:

```
AWS4-HMAC-SHA256
20121207T000000Z
```

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

Die erste Zeile der zu signierenden Zeichenfolge ist der Name des Algorithmus, die zweite Zeile der Zeitstempel, die dritte Zeile der Geltungsbereich der Anmeldeinformationen und die letzte Zeile ein Hash der kanonischen Anforderung aus Aufgabe 1: Erstellen einer kanonischen Anforderung. In dem Geltungsbereich für die Anmeldeinformationen ist auch u.a. der Name des zu verwenden Service angegeben, `redshift`.

Für Aufgabe 3: Berechnen einer Signatur kann der abgeleitete Schlüssel wie folgt dargestellt werden:

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

Der abgeleitete Schlüssel wird durch eine Abfolge von Hash-Funktionen berechnet. In der am tiefsten verschachtelten HMAC-Anweisung in der Formel oben wird an die Zeichenfolge **`AWS4`** Ihr geheimer Zugriffsschlüssel angehängt und die so verkettete Zeichenfolge wird als Schlüssel zur Berechnung der Hashes für die Daten „us-east-1“ verwendet. Das Ergebnis dieses Hashes wird als Schlüssel für die nächste Hash-Funktion verwendet.

Sie verwenden diesen abgeleiteten Schlüssel in einer Hash-Funktion, die zwei Zeichenfolgen als Eingabeparameter entgegennimmt, nämlich die zu signierende Zeichenfolge und den abgeleiteten Schlüssel. Beispiel: Wenn Sie den geheimen Zugriffsschlüssel `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY` und die zu signierende Zeichenfolge oben verwenden, sieht die berechnete Signatur wie folgt aus:

```
9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

Der letzte Schritt besteht im Erstellen des `Authorization`-Headers. Für den Demo-Zugriffsschlüssel `AKIAIOSFODNN7EXAMPLE` (mit hinzugefügten Zeilenumbrüchen zur besseren Lesbarkeit) lautet der Header:

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

Einrichten der Amazon-Redshift-CLI

In diesem Abschnitt wird erklärt, wie Sie die AWS CLI Befehlszeilentools für die Verwaltung von Amazon Redshift einrichten und ausführen. Die Befehlszeilentools von Amazon Redshift werden auf der AWS Command Line Interface (AWS CLI) ausgeführt, die wiederum Python verwendet (https://www.python.org/). Das AWS CLI kann auf jedem Betriebssystem ausgeführt werden, das Python unterstützt.

Installationsanleitungen

Um mit der Verwendung der Amazon Redshift Redshift-Befehlszeilentools zu beginnen, richten Sie zunächst die Konfigurationsdateien ein und fügen dann die Konfigurationsdateien hinzu AWS CLI, die die Amazon Redshift Redshift-CLI-Optionen definieren.

Wenn Sie den bereits AWS CLI für einen anderen AWS Service installiert und konfiguriert haben, können Sie dieses Verfahren überspringen.

Um den zu installieren AWS Command Line Interface

1. Gehen Sie zu Installieren oder auf die neueste Version von aktualisieren AWS CLI, und folgen Sie dann den Anweisungen zur Installation von AWS CLI.

   Für CLI-Zugriff benötigen Sie eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel. Verwenden Sie möglichst temporäre Anmeldeinformationen anstelle langfristiger Zugriffsschlüssel. Temporäre Anmeldeinformationen bestehen aus einer Zugriffsschlüssel-ID, einem geheimen Zugriffsschlüssel und einem Sicherheits-Token, das angibt, wann die Anmeldeinformationen ablaufen. Weitere Informationen finden Sie unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
2. Erstellen Sie eine Datei mit den Konfigurationsinformationen wie beispielsweise Ihren Zugriffsschlüsseln, der Standardregion und dem Format der Befehlsausgabe. Legen Sie anschließend die `AWS_CONFIG_FILE`-Umgebungsvariable fest, um auf diese Datei zu verweisen. Ausführliche Anweisungen finden Sie im AWS Command Line Interface Benutzerhandbuch unter Konfiguration der AWS Befehlszeilenschnittstelle.
3. Führen Sie einen Testbefehl aus, um zu überprüfen, ob die AWS CLI Schnittstelle funktioniert. Beispielsweise sollte der folgende Befehl Hilfsinformationen für die anzeigen AWS CLI:

   ```
   aws help
   ```

Über den folgenden Befehl sollten Hilfeinformationen für Amazon Redshift angezeigt werden:

```
aws redshift help
```

Referenzmaterial zu den Amazon Redshift-CLI-Befehlen finden Sie unter Amazon Redshift in der AWS CLI Referenz.

Amazon Redshift Serverless

Mit Amazon Redshift Serverless können Sie ganz einfach Analysen ausführen und skalieren, ohne Data Warehouses bereitstellen und verwalten zu müssen. Mit Amazon Redshift Serverless können Datenanalysten, Entwickler und Datenwissenschaftler jetzt Amazon Redshift verwenden, um innerhalb von Sekunden Erkenntnisse aus Daten zu erhalten, indem sie einfach Daten in das Data Warehouse laden und abfragen. Amazon Redshift stellt die Data-Warehouse-Kapazität automatisch bereit und skaliert, um eine schnelle Leistung für anspruchsvolle und unvorhersehbare Workloads zu erzielen. Sie bezahlen nur für die Kapazität, die Sie nutzen. Sie können von dieser Einfachheit profitieren, ohne Ihre bestehenden Analytik- und Business-Intelligence-Anwendungen ändern zu müssen.

Was ist Amazon Redshift Serverless?

Amazon Redshift Serverless stellt automatisch Data-Warehouse-Kapazität bereit und skaliert die zugrunde liegenden Ressourcen in intelligenter Weise. Amazon Redshift Serverless passt die Kapazität in Sekundenschnelle an, um selbst für die anspruchsvollsten und volatilsten Workloads eine gleichbleibend hohe Leistung und eine vereinfachte Produktion zu gewährleisten.

Mit Amazon Redshift Serverless können Sie von den folgenden Funktionen profitieren:

- Greifen Sie auf Daten zu und analysieren Sie sie, ohne dass Sie von Amazon Redshift bereitgestellte Cluster einrichten, optimieren und verwalten müssen.
- Nutzen Sie die erstklassigen Amazon-Redshift-SQL-Funktionen, die branchenführende Leistung und die Data-Lake-Integration, um nahtlos ein Data Warehouse, einen Data Lake und betriebliche Datenquellen abzufragen.
- Bieten Sie konstant hohe Leistung und vereinfachte Abläufe für anspruchsvollste und dynamischste Workloads mit intelligenter und automatischer Skalierung.
- Verwenden Sie Arbeitsgruppen und Namespaces, um Rechenressourcen und Daten mit detaillierten Kostenkontrollen zu organisieren.
- Zahlen Sie nur, wenn das Data Warehouse verwendet wird.

Mit Amazon Redshift Serverless erreichen Sie über eine Konsolenschnittstelle ein Serverless Data Warehouse oder APIs zum Entwickeln von Anwendungen. Über das Data Warehouse können Sie auf Ihren von Amazon Redshift verwalteten Speicher und Ihren Amazon S3-Data Lake zugreifen.

Dieses Video zeigt Ihnen, wie Amazon Redshift Serverless das Ausführen und Skalieren von Analytik vereinfacht, ohne die Data-Warehouse-Infrastruktur verwalten zu müssen:

Konsole von Amazon Redshift Serverless

Sehen Sie sich das folgende Video an, um mehr über die ersten Schritte mit der Amazon-Redshift-Serverless-Konsole zu erfahren: Getting Started with Amazon Redshift Serverless (Erste Schritte mit Amazon Redshift Serverless).

Serverless-Dashboard

Auf der Seite Serverless Dashboard finden Sie eine Zusammenfassung Ihrer Ressourcen und eine grafische Darstellung Ihrer Nutzung.

- Namespace overview (Namespace-Übersicht) – Dieser Abschnitt gibt Aufschluss über die Anzahl der Snapshots und Datashares in Ihrem Namespace.
- Workgroups (Arbeitsgruppen) – Dieser Abschnitt zeigt alle Arbeitsgruppen in Amazon Redshift Serverless an.
- Queries metrics (Abfragemetriken) – Dieser Abschnitt zeigt die Abfrageaktivität für die letzte Stunde.
- RPU capacity used (Genutzte RPU-Kapazität) – Dieser Abschnitt zeigt die in der letzten Stunde genutzte Kapazität an.
- Free trial (Kostenlose Testversion) – In diesem Abschnitt werden die Guthaben der kostenlosen Testversion angezeigt, die in Ihrem AWS -Konto verbleiben. Dies deckt die gesamte Nutzung der Ressourcen und Vorgänge von Amazon Redshift Serverless ab, einschließlich Snapshots, Speicher, Arbeitsgruppe usw. unter demselben Konto.
- Alarms (Alarme) – Dieser Abschnitt zeigt die Alarme, die Sie in Amazon Redshift Serverless konfiguriert haben.

Datensicherung

Auf der Registerkarte Data backup (Datensicherung) finden Sie folgende Optionen:

- Snapshots – Sie können Snapshots Ihrer Amazon-Redshift-Serverless-Daten erstellen, löschen und verwalten. Der Standardaufbewahrungszeitraum ist `indefinitely`, aber Sie können die Aufbewahrungsfrist auf einen beliebigen Wert zwischen 1 und 3 653 Tagen festlegen. Sie können die Wiederherstellung von Namespaces aus einem Snapshot autorisieren AWS-Konten .

- Recovery points (Wiederherstellungspunkte) – Zeigt automatisch erstellte Wiederherstellungspunkte an, die eine Wiederherstellung nach versehentlichem Überschreiben oder Löschen innerhalb der letzten 24 Stunden ermöglichen. Zum Wiederherstellen von Daten können Sie einen Wiederherstellungspunkt in jedem verfügbaren Namespace wiederherstellen. Sie können einen Snapshot von einem Wiederherstellungspunkt aus erstellen, wenn Sie einen Wiederherstellungspunkt für einen längeren Zeitraum beibehalten möchten. Der Standardaufbewahrungszeitraum ist `indefinitely`, aber Sie können die Aufbewahrungsfrist auf einen beliebigen Wert zwischen 1 und 3 653 Tagen festlegen.

Datenzugriff

Auf der Registerkarte Data access (Datenzugriff) finden Sie folgende Optionen:

- Network and security (Netzwerk und Sicherheit)-Einstellungen – Anzeigen von VPC-bezogenen Werten, AWS KMS -Verschlüsselungswerten und Prüfungsprotokollierungswerten. Sie können nur die Prüfungsprotokollierung aktualisieren. Weitere Informationen zum Festlegen von Netzwerk- und Sicherheitseinstellungen über die Konsole finden Sie unter Verwalten von Nutzungs- und Abfragelimits und andere administrative Aufgaben.
- AWS KMS key— AWS KMS key Wird verwendet, um Ressourcen in Amazon Redshift Serverless zu verschlüsseln.
- Permissions (Berechtigungen) – Sie können die IAM-Rollen verwalten, die Amazon Redshift Serverless für die Verwendung von Ressourcen in Ihrem Namen annehmen kann. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift Serverless.
- Redshift-managed VPC endpoints (Von Redshift verwaltete VPC-Endpunkte) – Sie können von einer anderen VPC oder einem anderen Subnetz aus auf Ihre Amazon-Redshift-Serverless-Instance zugreifen. Weitere Informationen finden Sie unter Verbinden mit Amazon Redshift Serverless von anderen VPC-Endpunkten.

Einschränkungen

Auf der Registerkarte Limits finden Sie folgende Optionen:

- Einstellungen für die Base capacity in Redshift processing units (RPUs) (Basiskapazität an Redshift Processing Units (RPUs)) – Sie können die Basiskapazität festlegen, die zur Verarbeitung Ihrer Workloads verwendet wird. Um die Abfrageleistung zu verbessern, erhöhen Sie den RPU-Wert.
- Usage limits (Nutzungslimits) – Die maximalen Rechenressourcen, die Ihre Amazon-Redshift-Serverless-Instance in einem Zeitraum verwenden kann, bevor eine Aktion gestartet wird. Sie

begrenzen die Menge an Ressourcen, die Amazon Redshift Serverless zum Ausführen Ihrer Workload verwendet. Die Nutzung ergibt sich aus der Zeit in Stunden, in der Redshift Processing Units (RPUs) verwendet werden. Eine RPU-Stunde entspricht der Anzahl der RPUs, die in einer Stunde verwendet werden. Sie können wie folgt festlegen, dass eine Aktion ausgeführt wird, wenn ein von Ihnen festgelegtes Limit erreicht wird:

- Senden einer Warnung.
- Protokollieren eines Eintrags in einer Systemtabelle.
- Deaktivieren von Benutzerabfragen.

Sie können bis zu vier Limits festlegen.

- Query limits (Abfragelimits) – Sie können einen Grenzwert hinzufügen, um die Leistung und die Limits zu überwachen. Weitere Informationen zu Limits für die Abfrageüberwachung finden Sie unter WLM-Abfrageüberwachungsregeln.

Weitere Informationen finden Sie unter Grundlegendes zur Amazon-Redshift-Serverless-Kapazität.

Datashares

Auf der Registerkarte Datashares finden Sie folgende Optionen:

- Einstellungen für Datashares created in my namespace (In meinem Namespace erstellte Datashares) – Sie können ein Datashare erstellen und für andere Namespaces und AWS-Konten freigeben.
- Datenfreigaben aus anderen Namespaces und AWS-Konten — Sie können eine Datenbank aus einer Datenfreigabe aus einem anderen Namespace erstellen und. AWS-Konten

Weitere Informationen zur Datenfreigabe finden Sie unter Datenfreigabe in Amazon Redshift Serverless.

Abfrage- und Datenbanküberwachung

Auf der Seite Query and database monitoring (Abfrage- und Datenbanküberwachung) finden Sie Diagramme zu Query history (Abfrageverlauf) und Database performance (Datenbankleistung).

Auf der Registerkarte Query history (Abfrageverlauf) finden Sie folgende Diagramme (Sie können zwischen Query list (Abfrageliste) und Resource metrics (Ressourcenmetriken) wählen):

- Query runtime (Abfrage-Laufzeit) – Dieses Diagramm zeigt, welche Abfragen im selben Zeitrahmen ausgeführt werden. Wählen Sie einen Balken im Diagramm aus, um weitere Details zur Abfrageausführung anzuzeigen.
- Queries and loads (Abfragen und Ladevorgänge) – In diesem Abschnitt werden Abfragen und Ladevorgänge nach Query ID (Abfrage-ID) aufgeführt.
- RPU capacity used (Genutzte RPU-Kapazität) – Dieses Diagramm zeigt die Gesamtkapazität in Redshift Processing Units (RPUs) an.
- Database connections (Datenbankverbindungen) – Dieses Diagramm zeigt die Anzahl der aktiven Datenbankverbindungen an.

Datenbankleistung

Auf der Registerkarte Database Performance (Datenbankleistung) sehen Sie die folgenden Diagramme:

- Queries completed per second (Ausgeführte Abfragen pro Sekunde) – Dieses Diagramm zeigt die durchschnittliche Anzahl der ausgeführten Abfragen pro Sekunde.
- Query duration (Abfragedauer) – Dieses Diagramm zeigt die durchschnittliche Zeit zur Ausführung einer Abfrage.
- Database connections (Datenbankverbindungen) – Dieses Diagramm zeigt die Anzahl der aktiven Datenbankverbindungen an.
- Running queries (Laufende Abfragen) – Dieses Diagramm zeigt die Gesamtzahl der laufenden Abfragen zu einem bestimmten Zeitpunkt.
- Queued queries (Abfragen in der Warteschlange) – Dieses Diagramm zeigt die Gesamtzahl der Abfragen in der Warteschlange zu einem bestimmten Zeitpunkt.
- Query run time breakdown (Aufschlüsselung der Laufzeit von Abfragen) – Dieses Diagramm zeigt die Gesamtzeit der ausgeführten Abfragen nach Typ aufgeschlüsselt an.

Ressourcenüberwachung

Auf der Seite Resource monitoring (Ressourcenüberwachung) finden Sie Diagramme zu Ihren genutzten Ressourcen. Sie können die Daten nach mehreren Gesichtspunkten filtern.

- Metric filter (Metrikfilter) – Sie können Metrikfilter verwenden, um Filter für eine bestimmte Arbeitsgruppe auszuwählen sowie den Zeitraum und das Zeitintervall festzulegen.

- RPU capacity used (Genutzte RPU-Kapazität) – Dieses Diagramm zeigt die Gesamtkapazität in Redshift Processing Units (RPUs) an.
- Rechenressourcennutzung – Dieses Diagramm zeigt die Nutzung von RPU-Stunden nach Zeitraum für den ausgewählten Zeitbereich. Für Zeitbereiche von weniger als 6 Stunden werden die RPU-Stunden in exakter Zeit angezeigt. Für Zeitbereiche von 6 Stunden oder mehr werden die RPU-Stunden als Durchschnittswerte angezeigt.

Auf der Seite Datashares können Sie Datashares unter In my account (In meinem Konto) und From other accounts (Aus anderen Konten) verwalten. Weitere Informationen zur Datenfreigabe finden Sie unter Datenfreigabe in Amazon Redshift Serverless.

Überlegungen zur Verwendung von Amazon Redshift Serverless

Eine Liste, AWS-Regionen wo Amazon Redshift Serverless verfügbar ist, finden Sie in den Endpunkten, die für die Redshift Serverless API aufgeführt sind. Allgemeine Amazon Web Services-Referenz

Einige von Amazon Redshift Serverless verwendete Ressourcen unterliegen Kontingenten. Weitere Informationen finden Sie unter Kontingente für Objekte von Amazon Redshift Serverless.

Wenn Sie für einen Cursor DECLARE ausführen, werden die Größenangaben für den Ergebnissatz für Amazon Redshift Serverless in DECLARE angegeben.

Wartungsfenster – Bei Amazon Redshift Serverless gibt es kein Wartungsfenster. Softwareversionen werden automatisch aktualisiert. Es gibt keine Unterbrechung für bestehende Verbindungen oder Abfrageausführung, wenn Amazon Redshift die Versionen wechselt. Neue Verbindungen werden immer hergestellt und funktionieren sofort mit Amazon Redshift Serverless.

Availability Zone IDs – Wenn Sie Ihre Instance für Amazon Redshift Serverless konfigurieren, öffnen Sie Additional considerations (Weitere Überlegungen) und stellen Sie sicher, dass die Subnetz-IDs unter Subnet (Subnetz) mindestens drei der unterstützten Availability-Zone-IDs enthalten. Um das Mapping von Subnetzen und Availability-Zone-IDs anzuzeigen, öffnen Sie die VPC-Konsole und wählen Sie Subnets (Subnetze) aus, um die Liste der Subnetz-IDs mit ihren Availability-Zone-IDs anzuzeigen. Stellen Sie sicher, dass Ihr Subnetz einer unterstützten Availability-Zone-ID zugeordnet ist. Weitere Informationen zum Erstellen von Subnetzen finden Sie unter Erstellen eines Subnetzes in der VPC im Amazon-VPC-Benutzerhandbuch.

Drei Subnetze – Sie benötigen mindestens drei Subnetze, die sich über drei Availability Zones erstrecken. Zum Beispiel können Sie drei Subnetze verwenden, die den Availability Zones us-

east-1a, us-east-1b und us-east-1c zugeordnet sind. Eine Ausnahme bildet die Region USA West (Nordkalifornien). Genau wie die anderen Regionen erfordert sie drei Subnetze, diese dürfen sich jedoch nur über zwei Availability Zones erstrecken. Eine Bedingung ist, dass eine dieser Availability Zones zwei der Subnetze enthalten muss.

Anforderungen an kostenlose IP-Adressen — Sie müssen über kostenlose IP-Adressen verfügen, wenn Sie eine Amazon Redshift Serverless-Arbeitsgruppe erstellen. Die Mindestanzahl an IP-Adressen steigt mit der Anzahl der Redshift Processing Units (RPUs) für die Arbeitsgruppe. Insbesondere erfordert jedes Subnetz in der VPC Ihrer Arbeitsgruppe eine Mindestanzahl an IP-Adressen. Weitere Informationen zum Zuweisen von IP-Adressen finden Sie unter IP-Adressierung im Amazon-VPC-Benutzerhandbuch.

Die Mindestanzahl an freien IP-Adressen, die bei der Erstellung einer Arbeitsgruppe erforderlich sind, lautet wie folgt:

Anzahl der für jedes Subnetz erforderlichen freien IP-Adressen

Redshift Processing Units (RPUs)	Erforderliche freie IP-Adressen.	CIDR-Mindestgröße
8	9	/27
16	15	/27
32	13	/27
64	21	/27
128	37	/26
256	69	/25
512	133	/24

Sie benötigen außerdem freie IP-Adressen, wenn Sie Ihre Arbeitsgruppe aktualisieren, um mehr RPUs zu verwenden. Die Anzahl der freien IP-Adressen, die für die Aktualisierung der Subnetze für eine Arbeitsgruppe erforderlich sind, ist wie folgt:

Anzahl der erforderlichen freien IP-Adressen beim Aktualisieren eines Subnetzes

Redshift Processing Units (RPUs)	Aktualisierte Redshift Processing Units (RPUs)	Erforderliche freie IP-Adressen.
8	16	10
16	32	13
32	64	16
64	128	28
128	256	52
256	512	100

Speicherplatz nach der Migration – Wenn Sie kleine von Amazon Redshift bereitgestellte Cluster zu Amazon Redshift Serverless migrieren, können Sie nach der Migration ggf. eine Zunahme der Speicherplatzzuweisung feststellen. Dies ist das Ergebnis einer optimierten Speicherplatzzuweisung, die zu vorab zugewiesenem Speicherplatz führt. Dieser Speicherplatz wird im Laufe der Zeit genutzt, wenn die Datenmengen in Amazon Redshift Serverless zunehmen.

Datasharing zwischen Amazon Redshift Serverless und von Amazon Redshift bereitgestellten Clustern – Beim Datasharing, bei dem Amazon Redshift Serverless der Produzent und ein bereitgestellter Cluster der Verbraucher ist, muss der bereitgestellte Cluster eine höhere Clusterversion als 1.0.38214 aufweisen. Wenn Sie eine niedrigere Clusterversion verwenden, tritt beim Ausführen einer Abfrage ein Fehler auf. Sie können die Cluster-Version in der Amazon-Redshift-Konsole auf der Registerkarte Maintenance (Wartung) einsehen. Sie können auch `SELECT version();` ausführen.

Max. Ausführungszeit der Abfrage – Verstrichene Ausführungszeit für eine Abfrage in Sekunden. Die Ausführungszeit enthält nicht die in einer Warteschlange verbrachte Zeit. Wenn eine Abfrage die festgelegte Ausführungszeit überschreitet, stoppt Amazon Redshift Serverless die Abfrage. Gültige Werte liegen zwischen 0 und 86 399.

Migration für Tabellen mit überlappenden Sortierschlüsseln – Bei der Migration von bereitgestellten Amazon-Redshift-Clustern zu Amazon Redshift Serverless konvertiert Redshift Tabellen mit überlappenden Sortierschlüsseln und DISTSTYLE KEY in zusammengesetzte Sortierschlüssel. Der

DISTSTYLE ändert sich nicht. Weitere Informationen zu Verteilungsstilen finden Sie unter Arbeiten mit Datenverteilungsstilen im Amazon-Redshift-Entwicklerhandbuch. Weitere Informationen zu Sortierschlüsseln finden Sie unter Arbeiten mit Sortierschlüsseln.

VPC-Freigabe – Sie können Amazon-Redshift-Serverless-Arbeitsgruppen in einer geteilten VPC erstellen. In diesem Fall sollten Sie die Ressourcenfreigabe nicht löschen, da dies dazu führen kann, dass die Arbeitsgruppe nicht mehr verfügbar ist.

Rechenkapazität für Amazon Redshift Serverless

Grundlegendes zur Amazon-Redshift-Serverless-Kapazität

RPUs

Amazon Redshift Serverless misst die Kapazität von Data Warehouses in Redshift Processing Units (RPUs). RPUs sind Ressourcen, die zur Verarbeitung von Workloads verwendet werden.

Basiskapazität

Diese Einstellung gibt die Basiskapazität des Data Warehouse an, die Amazon Redshift zur Verarbeitung von Abfragen verwendet. Die Basiskapazität wird in RPUs angegeben. Sie können eine Basiskapazität in Redshift Processing Units (RPUs) festlegen. Eine RPU bietet 16 GB Arbeitsspeicher. Wenn Sie eine höhere Basiskapazität festlegen, wird die Abfrageleistung verbessert, insbesondere für Datenverarbeitungsaufträge, die viele Ressourcen verbrauchen. Die Standard-Basiskapazität für Amazon Redshift Serverless beträgt 128 RPUs. Sie können die Einstellung Basiskapazität von 8 RPUs bis 512 RPUs in Einheiten von 8 (8, 16, 24 ... 512) über die AWS-Konsole, die API-Operation `UpdateWorkgroup` oder die Operation `update-workgroup` in der AWS CLI anpassen.

Mit einer Mindestkapazität von 8 RPUs haben Sie jetzt mehr Flexibilität, um je nach Leistungsanforderungen einfachere bis hin zu komplexeren Workloads auszuführen. Die RPU-Basiskapazitäten von 8, 16 und 24 RPUs sind auf Workloads ausgerichtet, die weniger als 128 TB Daten benötigen. Wenn Ihre Datenanforderungen 128 TB übersteigen, müssen Sie mindestens 32 RPUs verwenden. Für Workloads mit Tabellen mit einer großen Anzahl von Spalten und höherer Parallelität empfehlen wir die Verwendung von 32 oder mehr RPUs.

Überlegungen und Einschränkungen für die Kapazität von Amazon Redshift Serverless

Im Folgenden finden Sie Überlegungen und Einschränkungen in Bezug auf die Kapazität von Amazon Redshift Serverless.

- Konfigurationen mit 8 oder 16 RPUs unterstützen eine von Redshift verwaltete Speicherkapazität von bis zu 128 TB. Wenn Sie mehr als 128 TB verwalteten Speicher verwenden, ist keine Herabstufung auf weniger als 32 RPUs möglich.
- Das Bearbeiten der Basiskapazität Ihrer Arbeitsgruppe kann zum Abbruch einiger Abfragen führen, die in Ihrer Arbeitsgruppe ausgeführt werden.

KI-gestützte Skalierung und Optimierung (Vorschau)

Dies ist eine vorab veröffentlichte Dokumentation für KI-gestützte Skalierungen und Optimierungen in Amazon Redshift Serverless. Dieser Service befindet sich in der Vorschau. Sowohl die Dokumentation als auch die Funktion können sich ändern. Wir empfehlen, diese Funktion nur in Test- und nicht in Produktionsumgebungen zu verwenden. Weitere Informationen zu den Bedingungen für Vorschauversionen finden Sie unter Betas und Vorversionen in den AWS-Servicebedingungen.

Diese Vorschau ist in den folgenden AWS-Regionen verfügbar:

- USA Ost (Ohio): (us-east-2)
- USA Ost (Nord-Virginia): (us-east-1)
- USA West (Nordkalifornien) (us-west-1)
- Asien-Pazifik (Tokyo) (ap-northeast-1)
- Europa (Irland) (eu-west-1)
- Europa (Stockholm) (eu-north-1)

Sie können eine Vorschau-Arbeitsgruppe erstellen, um neue Funktionen von Amazon Redshift Serverless zu testen. Sie können diese Features nicht in der Produktion verwenden oder Ihre Arbeitsgruppe zu einer anderen Arbeitsgruppe verschieben. Weitere Informationen zu den Nutzungsbedingungen für die Vorschau finden Sie unter „Beta- und Vorschauversionen“ in den AWS-Servicebedingungen. Eine Anleitung zur Erstellung von Vorschau-Arbeitsgruppen finden Sie unter Erstellen einer Vorschau-Arbeitsgruppe.

Sie können auch ein Preis-Leistungs-Ziel für Ihre Arbeitsgruppe festlegen, damit Redshift automatisch KI-gesteuerte Optimierungen für Ihre Ressourcen ausführen kann. So können Sie Ihre Preis-Leistungs-Ziele erreichen und gleichzeitig die Kosten optimieren. Diese automatische Preis-

Leistungs-Optimierung ist besonders nützlich, wenn Sie nicht wissen, welche Basiskapazität Sie für Ihre Workloads festlegen sollen, oder wenn einige Teile Ihres Workloads von der Zuweisung weiterer Ressourcen profitieren könnten.

Wenn Ihre Organisation beispielsweise normalerweise Workloads ausführt, die nur 32 RPUs benötigen, plötzlich jedoch eine komplexere Abfrage ausführen muss, wissen Sie möglicherweise nicht, welche Basiskapazität Sie benötigen. Die Festlegung einer höheren Basiskapazität führt zu einem besseren Preis-Leistungs-Verhältnis, verursacht jedoch auch höhere Kosten. Daher entsprechen die Kosten möglicherweise nicht Ihren Erwartungen. Über die KI-gestützte Skalierung und Ressourcenoptimierung passt Amazon Redshift Serverless die RPUs automatisch an Ihre Preis-Leistungs-Ziele an und optimiert gleichzeitig die Kosten für Ihre Organisation. Diese automatische Optimierung ist unabhängig von der Größe des Workloads nützlich. Die automatische Optimierung kann Ihnen helfen, bei komplexen Abfragen die Preis-Leistungs-Ziele Ihrer Organisation einzuhalten.

Die Preis-Leistungs-Ziele sind eine arbeitsgruppenspezifische Einstellung. Für unterschiedliche Arbeitsgruppen können unterschiedliche Preis-Leistungs-Ziele gelten.

Um die Kosten planen zu können, legen Sie ein Limit für die maximale Kapazität fest, die Amazon Redshift Serverless Ihren Workloads zuweisen darf.

Sie konfigurieren die Preis-Leistungs-Ziele über die AWS-Konsole. Standardmäßig ist die Einstellung für das Preis-Leistungs-Ziel aktiviert, wenn Sie eine neue Arbeitsgruppe erstellen, und auf Ausgewogen festgelegt. Wenn Sie ein anderes Preis-Leistungs-Ziel oder eine Basiskapazität für Ihre Arbeitsgruppe festlegen möchten, verwenden Sie beim Erstellen einer Arbeitsgruppe benutzerdefinierte Einstellungen. Weitere Informationen zum Erstellen einer Arbeitsgruppe finden Sie unter Erstellen einer Arbeitsgruppe mit einem Namespace.

So bearbeiten Sie das Preis-Leistungs-Ziel für Ihre Arbeitsgruppe:

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole die Option Arbeitsgruppenkonfiguration aus.
2. Wählen Sie die Arbeitsgruppe aus, deren Preis-Leistungs-Ziel Sie bearbeiten möchten. Wählen Sie die Registerkarte Leistung und anschließend Bearbeiten aus.
3. Wählen Sie Preis-Leistungs-Ziel aus und stellen Sie den Schieberegler auf das für Ihre Arbeitsgruppe gewünschte Ziel ein.
4. Wählen Sie Änderungen speichern aus.

Um die maximale Anzahl der RPUs zu aktualisieren, die Amazon Redshift Serverless Ihrem Workload zuweisen kann, wechseln Sie in der Arbeitsgruppenkonfiguration zur Registerkarte Limits.

Weitere Informationen zu KI-gesteuerten Optimierungen und Ressourcenskalierungen finden Sie im folgenden Video.

Fakturierung für Amazon Redshift Serverless

Preisgestaltung

Informationen zu Preisen finden Sie unter Amazon-Redshift-Preise.

Fakturierung für Rechenkapazität

Basiskapazität und ihre Auswirkungen auf die Abrechnung

Wenn Abfragen ausgeführt werden, wird Ihnen die Kapazität, die für eine bestimmte Dauer in RPU-Stunden pro Sekunde verwendet wird, in Rechnung gestellt. Wenn keine Anfragen ausgeführt werden, wird Ihnen keine Rechenkapazität in Rechnung gestellt. Basierend auf der Menge der gespeicherten Daten wird Ihnen auch Redshift Managed Storage (RMS) in Rechnung gestellt.

Wenn Sie Ihre Arbeitsgruppe erstellen, haben Sie die Möglichkeit, die Basiskapazität für die Datenverarbeitung festzulegen. Passen Sie die Basiskapazität für eine vorhandene Arbeitsgruppe nach oben oder nach unten an, um die Preis-/Leistungsanforderungen Ihrer Workload auf Arbeitsgruppenebene zu erfüllen. Wählen Sie die Arbeitsgruppe unter Arbeitsgruppenkonfiguration und die Registerkarte Limits aus, um die Basiskapazität über die Konsole zu ändern.

Mit zunehmender Anzahl der Abfragen skaliert Amazon Redshift Serverless automatisch, um eine konsistente Leistung zu gewährleisten.

Maximales Nutzungslimit für RPU-Stunden

Um die Kosten für Amazon Redshift Serverless vorhersehbar zu halten, können Sie Maximum RPU hours (Maximale RPU-Stunden) festlegen, die pro Tag, pro Woche oder pro Monat verwendet werden. Sie können dies über die Konsole oder die API festlegen. Sie können angeben, dass bei Erreichen eines Limits ein Protokolleintrag in eine Systemtabelle geschrieben wird, eine Warnung ausgegeben wird oder Benutzerabfragen deaktiviert werden. Die Einstellung der maximalen RPU-Stunden hilft Ihnen dabei, Ihre Kosten unter Kontrolle zu halten. Einstellungen für maximale RPU-

Stunden gelten für Ihre Arbeitsgruppe sowohl für Abfragen, die auf Daten in Ihrem Data Warehouse zugreifen, als auch für Abfragen, die auf externe Daten zugreifen, z. B. in einer externen Tabelle in Amazon S3.

Im Folgenden wird ein Beispiel gezeigt:

Angenommen, Sie legen für jede Woche ein Limit von 100 Stunden fest. Hierzu führen Sie in der Konsole die folgenden Schritte aus:

1. Wählen Sie Ihre Arbeitsgruppe und dann auf der Registerkarte Limits die Option Nutzungslimits verwalten aus.
2. Fügen Sie ein Nutzungslimit hinzu, wählen Sie als Häufigkeit Wöchentlich und als Dauer 100 Stunden aus und legen Sie die Aktion auf Benutzeranfragen deaktivieren fest.

In diesem Beispiel werden Abfragen deaktiviert, wenn Sie das Limit von 100 RPU-Stunden für eine Woche erreichen.

Durch Festlegen der maximalen RPU-Stunden für die Arbeitsgruppe werden weder Leistung noch Rechenressourcen für die Arbeitsgruppe eingeschränkt. Sie können die Einstellungen jederzeit ohne Unterbrechung der Abfrageverarbeitung ändern. Die Festlegung der maximalen RPU-Stunden soll Ihnen helfen, Preis- und Leistungsanforderungen zu erfüllen. Weitere Informationen zur Serverless-Fakturierung finden Sie unter Amazon Redshift – Preise.

Sie können die Kosten für Amazon Redshift Serverless auch planen, indem Sie die AWS-Funktion für die Entdeckung von Kostenanomalien verwenden, um Überraschungen bei der Abrechnung zu vermeiden und mehr Kontrolle zu erhalten.

> **Note**
>
> Der Amazon-Redshift-Preisrechner hilft bei der Schätzung von Preisen. Sie geben die benötigten Rechenressourcen ein und es wird eine Vorschau der Kosten angezeigt.

Festlegen der maximalen Kapazität zur Kontrolle der Kosten für Rechenressourcen

Die Einstellung für die maximale Kapazität dient als RPU-Obergrenze, bis zu der Amazon Redshift Serverless hochskaliert werden kann. Sie hilft Ihnen, Ihre Kosten für Rechenressourcen zu kontrollieren. Ähnlich wie die Basiskapazität eine Mindestmenge an verfügbaren Rechenressourcen

festlegt, legt die maximale Kapazität eine Obergrenze für die RPU-Nutzung fest. Dies hilft, die Ausgaben den Plänen entsprechend zu steuern. Die maximale Kapazität ist für jede Arbeitsgruppe spezifisch und schränkt die Rechenressourcennutzung zu allen Zeitpunkten ein.

Unterschied zwischen maximaler Kapazität und Nutzungslimits für RPU-Stunden

Nutzungslimits für RPU-Stunden und maximale Kapazität sollen eine Kostenkontrolle ermöglichen. Sie erreichen dies jedoch auf unterschiedliche Weise. Die folgenden Punkte erklären den Unterschied:

- Max. Kapazität – Diese Einstellung legt die höchste Anzahl von RPUs fest, auf die Amazon Redshift Serverless skaliert werden kann. Wenn Rechenressourcen automatisch skaliert werden müssen, kann ein höherer Wert für die maximale Kapazität den Abfragedurchsatz verbessern. Wenn die maximale Kapazität erreicht ist, erfolgt keine weitere Hochskalierung der Ressourcen durch die Arbeitsgruppe.
- Nutzungslimit für RPU-Stunden – Im Gegensatz zur maximalen Kapazität legt diese Einstellung keine Kapazitätsobergrenze fest. Es werden jedoch andere Aktionen ausgeführt, um die Kosten zu begrenzen. Dies umfasst das Hinzufügen eines Eintrags zu einem Protokoll, das Senden einer Benachrichtigung oder das Stoppen der Ausführung von Abfragen, wenn Sie dies wünschen.

Sie können die maximale Kapazität ausschließlich verwenden oder durch Aktionen im Rahmen des Nutzungslimits für RPU-Stunden ergänzen.

Ein Anwendungsfall für maximale Kapazität

Für jede Arbeitsgruppe kann eine andere Einstellung für die maximale Kapazität gelten. Die Einstellung hilft Ihnen, Budgetierungsanforderungen durchzusetzen. Im Folgenden finden Sie ein Beispiel dafür, wie dies funktioniert.

- Sie haben eine Arbeitsgruppe mit einer Basiskapazität von 256 RPUs. Sie führen die meiste Zeit des Monats konstante Workloads von knapp über 256 RPUs aus.
- Die maximale Kapazität ist auf 512 RPUs festgelegt.

Angenommen, es gibt über einen Zeitraum von drei Tagen eine unerwartet hohe Nutzung, um statistische Ad-Hoc-Berichte zu erstellen. Für Fälle wie diese haben Sie eine maximale Kapazität festgelegt, um Rechenkosten für mehr als 512 RPUs zu vermeiden. So können Sie sicher sein, dass die Rechenkapazität diese Obergrenze nicht überschreitet.

Hinweise zur Nutzung der maximalen Kapazität

Diese Hinweise können Ihnen helfen, die maximale Kapazität richtig festzulegen:

- Für jede Amazon-Redshift-Serverless-Arbeitsgruppe kann eine andere Einstellung für die maximale Kapazität gelten.
- Wenn es einen Zeitraum mit einem sehr hohen Ressourcenverbrauch gibt und die maximale Kapazität auf einen niedrigen RPU-Wert festgelegt ist, kann dies die Workload-Verarbeitung verzögern und zu einer nicht optimalen Benutzererfahrung führen.
- Die Konfiguration der Einstellung für die maximale Kapazität beeinträchtigt die Ausführung von Abfragen nicht, auch nicht in Zeiten einer hohen RPU-Nutzung. Sie funktioniert nicht wie ein Nutzungslimit, das die Ausführung von Abfragen stoppen kann. Sie schränkt lediglich die Zahl der Rechenressourcen ein, die der Arbeitsgruppe zur Verfügung stehen. Sie können die über einen bestimmten Zeitraum genutzte Kapazität im Amazon-Redshift-Serverless-Dashboard anzeigen. Weitere Informationen zum Anzeigen von Übersichtsdaten finden Sie unter Überprüfen von Amazon-Redshift-Serverless-Übersichtsdaten über das Dashboard.
- Der höchstmögliche Wert für die maximale Kapazität ist 5632 RPUs.

Festlegen der maximalen Kapazität

Sie können die maximale Kapazität in der Konsole festlegen. Für eine vorhandene Arbeitsgruppe können Sie die Einstellung unter Arbeitsgruppenkonfiguration ändern. Sie können für die Festlegung auch die CLI verwenden, indem Sie einen Befehl wie im folgenden Beispiel verwenden:

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

Hierdurch wird die maximale Kapazität für die Arbeitsgruppe mit dem angegebenen Namen festgelegt. Nach der Festlegung können Sie den Wert in der Konsole überprüfen. Sie können den Wert auch über die CLI mit dem Befehl `get-workgroup` überprüfen.

Sie können die Einstellung für die maximale Kapazität durch Festlegung auf `-1` deaktivieren, wie im folgenden Beispiel gezeigt:

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

Überwachung von Nutzung und Kosten von Amazon Redshift Serverless

Es gibt mehrere Möglichkeiten, die Nutzung und Fakturierung für Amazon Redshift Serverless zu schätzen. Systemansichten können hilfreich sein, da die Systemmetadaten, einschließlich Abfrage- und Nutzungsdaten, rechtzeitig sind und Sie keine Einrichtung durchführen müssen, um sie abzufragen. CloudWatch kann auch für die Überwachung der Nutzung Ihrer Amazon-Redshift-Serverless-Instance nützlich sein und über zusätzliche Funktionen verfügen, um Erkenntnisse zu gewinnen und Aktionen festzulegen.

Visualisieren der Nutzung durch Abfragen einer Systemansicht

Fragen Sie die Systemtabelle SYS_SERVERLESS_USAGE ab, um die Nutzung zu verfolgen und die Gebühren für Abfragen abzurufen:

```
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
```

Mit dieser Abfrage erhalten Sie die Kosten pro Tag für Amazon Redshift Serverless basierend auf der Nutzung.

Nutzungshinweise zur Bestimmung der Nutzung und der Kosten

- Sie bezahlen für die Workloads, die Sie ausführen, in RPU-Stunden pro Sekunde mit einer Mindestgebühr von 60 Sekunden.
- Datensätze aus der Systemtabelle sys_serverless_usage zeigen die angefallenen Kosten in Intervallen von einer Minute an. Es ist wichtig, die folgenden Spalten zu verstehen:

  Die Spalte charged_seconds:

  - Gibt die Recheneinheiten (in RPU-Sekunden) für dieses Zeitintervall an. Die Ergebnisse beinhalten alle Mindestgebühren für Amazon Redshift Serverless.
  - Enthält Informationen zur Nutzung der Datenverarbeitungsressourcen nach Abschluss der Transaktionen. Daher kann dieser Spaltenwert 0 sein, wenn die Transaktionen noch nicht abgeschlossen sind.

  Die Spalte compute_seconds:

  - Stellt Informationen zur Rechenauslastung in Echtzeit bereit. Mindestgebühren für Amazon Redshift Serverless sind darin nicht enthalten. Daher kann der Wert bis zu einem gewissen Grad von den während des Intervalls in Rechnung gestellten Sekunden abweichen..
  - Zeigt Nutzungsinformationen während der einzelnen Transaktionen an (auch wenn eine Transaktion noch nicht beendet ist), d. h. es handelt sich um Echtzeitdaten.
- Es gibt Situationen, in denen compute_seconds 0, charged_seconds jedoch größer als 0 ist oder umgekehrt. Dies ist ein normales Verhalten, das sich aus der Art und Weise ergibt, wie Daten in der Systemansicht aufgezeichnet werden. Für eine genauere Darstellung der Details zur Serverless-Nutzung empfehlen wir, die Daten in SYS_SERVERLESS_USAGE zu aggregieren.

Weitere Informationen zur Überwachung von Tabellen und Ansichten finden Sie unter Überwachen von Abfragen und Workloads mit Amazon Redshift Serverless.

Visualisieren der Nutzung mit CloudWatch

Sie können die in verfügbaren Metriken verwenden CloudWatch , um die Nutzung nachzuverfolgen. Die für generierten Metriken CloudWatch sind `ComputeSeconds`, d. h. die Gesamtzahl der in der aktuellen Minute verwendeten RPU-Sekunden und `ComputeCapacity`, d. h. die gesamte Rechenkapazität für diese Minute. Nutzungsmetriken finden Sie auch in der Redshift-Konsole auf dem Redshift Serverless dashboard (Redshift-Serverless-Dashboard). Weitere Informationen zu CloudWatchfinden Sie unter Was ist Amazon CloudWatch?

Fakturierung für Speicher

Die primäre Speicherkapazität wird als Redshift Managed Storage (RMS) in Rechnung gestellt. Die Fakturierung für Speicher erfolgt nach GB/Monat. Die Speicherfakturierung ist von der Fakturierung für Rechenkapazität getrennt. Der für Benutzer-Snapshots verwendete Speicher wird zu den standardmäßigen Backup-Fakturierungstarifen je nach Nutzungskontingent abgerechnet.

Kosten für Datenübertragung und Machine Learning (ML) fallen separat an, genau wie Kosten für bereitgestellte Cluster. Snapshot-Replikation und Datenfreigaben über AWS-Regionen hinweg werden zu den auf der Preisseite angegebenen Übertragungstarifen abgerechnet. Weitere Informationen finden Sie unter Amazon Redshift – Preise.

Visualisieren der Fakturierungsnutzung mit CloudWatch

Die Metrik `SnapshotStorage`, die die Nutzung des Snapshot-Speichers verfolgt, wird generiert und an gesendet CloudWatch. Weitere Informationen zu CloudWatchfinden Sie unter Was ist Amazon CloudWatch?

Verwenden von kostenlosen Testversion von Amazon Redshift Serverless

Amazon Redshift Serverless bietet eine kostenlose Testversion. Wenn Sie die kostenlose Testversion in Anspruch nehmen, können Sie das Guthaben dieser Testversion in der Redshift-Konsole einsehen und die Nutzung dieser Testversion in der Systemansicht SYS_SERVERLESS_USE überprüfen. Beachten Sie, dass die Abrechnungsdetails für die Nutzung der kostenlosen Testversion nicht in der Rechnungskonsole angezeigt werden. Sie können die Nutzung erst in der Rechnungskonsole anzeigen, nachdem die kostenlose Testversion beendet wurde. Weitere Informationen zur kostenlosen Testversion von Amazon Redshift Serverless finden Sie unter Kostenlose Testversion von Amazon Redshift Serverless.

Hinweise zur Fakturierungsnutzung

- Nutzungsaufzeichnung – Eine Abfrage oder Transaktion wird erst gemessen und aufgezeichnet, nachdem die Transaktion abgeschlossen ist, zurückgesetzt oder gestoppt wurde. Wenn eine Transaktion beispielsweise zwei Tage lang ausgeführt wird, wird die RPU-Nutzung nach Abschluss aufgezeichnet. Sie können die laufende Nutzung in Echtzeit überwachen, indem Sie `sys_serverless_usage` abfragen. Die Transaktionsaufzeichnung kann sich als Variation der RPU-Nutzung widerspiegeln und auf die Kosten für bestimmte Stunden und die tägliche Nutzung auswirken.
- Schreiben von expliziten Transaktionen – Dies ist eine wichtige bewährte Methode zum Beenden von Transaktionen. Wenn Sie eine offene Transaktion nicht beenden oder zurücksetzen, verwendet Amazon Redshift Serverless weiterhin RPUs. Wenn Sie beispielsweise eine explizite `BEGIN TRAN`-Anweisung schreiben, ist es wichtig, auch entsprechende `COMMIT`- und `ROLLBACK`-Anweisungen anzugeben.
- Abgebrochene Abfragen – Wenn Sie eine Abfrage ausführen und abbrechen, bevor sie abgeschlossen ist, wird Ihnen die Zeit, während der die Abfrage ausgeführt wurde, dennoch in Rechnung gestellt.
- Skalierung – Die Amazon-Redshift-Serverless-Instance kann zur Bewältigung von Zeiträumen mit höherer Belastung Skalierungen einleiten, um eine konsistente Leistung aufrechtzuerhalten. Die

Fakturierung für Amazon Redshift Serverless umfasst sowohl Basis-Rechenkapazität als auch skalierte Kapazität zum gleichen RPU-Tarif.

- Herunterskalieren – Amazon Redshift Serverless skaliert von seiner Basis-RPU-Kapazität hoch, um Zeiträume mit höherer Belastung zu bewältigen. In einigen Fällen kann die RPU-Kapazität für einen Zeitraum nach dem Rückgang der Abfragelast auf einer höheren Einstellung bleiben. Wir empfehlen Ihnen, maximale RPU-Stunden in der Konsole so einzustellen, dass Sie vor unerwarteten Kosten geschützt sind.
- Systemtabellen – Wenn Sie eine Systemtabelle abfragen, wird die Abfragezeit in Rechnung gestellt.
- Redshift Spectrum – Wenn Sie Amazon Redshift Serverless nutzen und Abfragen ausführen, fällt für Data-Lake-Abfragen keine separate Gebühr an. Bei Abfragen zu Daten, die in Amazon S3 gespeichert sind, entspricht die Gebühr nach Transaktionszeit der für Abfragen von lokalen Daten.
- Verbundabfragen – Verbundabfragen werden nach den in einem bestimmten Zeitintervall genutzten RPUs berechnet, genau wie Abfragen im Data Warehouse oder Data Lake.
- Speicher – Der Speicher wird separat nach GB/Monat in Rechnung gestellt.
- Mindestgebühr – Die Mindestgebühr gilt für 60 Sekunden Ressourcennutzung, gemessen auf Sekundenbasis.
- Snapshot-Fakturierung – Die Snapshot-Fakturierung ändert sich nicht. Die Fakturierung erfolgt je nach Speicher in GB/Monat. Sie können Ihr Data Warehouse kostenlos auf bestimmte Punkte in den letzten 24 Stunden zurücksetzen, mit einer Granularität von 30 Minuten. Weitere Informationen finden Sie unter Amazon Redshift – Preise.

Bewährte Methoden für Amazon Redshift Serverless, um die Abrechnung vorhersehbar zu halten

Es gibt einige bewährte Methoden und integrierte Einstellungen, die dazu beitragen, Ihre Abrechnung konsistent zu halten.

- Stellen Sie sicher, dass Sie jede Transaktion beenden. Wenn Sie eine Aktion mit `BEGIN` starten, müssen Sie sie auch mit `END` beenden.
- Verwenden Sie die bewährten Methoden zur Fehlerbehebung, um ordnungsgemäß auf Fehler zu reagieren und jede Transaktion zu beenden. Die Minimierung offener Transaktionen hilft, unnötige RPU-Nutzung zu vermeiden.
- `SESSION TIMEOUT` hilft durch Beendigung offener Transaktionen und inaktiver Sitzungen. Es führt bei Sitzungen, die länger als 3 600 Sekunden (1 Stunde) inaktiv sind, zu einem Timeout. Es

führt bei Transaktionen, die länger als 21 600 Sekunden (6 Stunden) offen und inaktiv sind, zu einem Timeout. Diese Zeitüberschreitungseinstellung kann explizit für einen bestimmten Benutzer geändert werden, z. B. wenn Sie eine Sitzung für eine lang laufende Abfrage geöffnet lassen möchten. Das Thema CREATE USER zeigt, wie `SESSION TIMEOUT` für einen Benutzer eingestellt wird.

- In den meisten Fällen empfehlen wir, den Wert `SESSION TIMEOUT` nicht zu erweitern, es sei denn, Sie haben einen Anwendungsfall, der dies ausdrücklich erfordert. Wenn die Sitzung bei einer offenen Transaktion inaktiv bleibt, kann dies zu einem Fall führen, in dem RPUs verwendet werden, bis die Sitzung geschlossen wird. Dies führt zu unnötigen Kosten.
- Amazon Redshift Serverless hat einen Zeitraum von maximal 86 399 Sekunden (24 Stunden) für eine laufende Abfrage. Die maximale Inaktivitätsdauer für eine offene Transaktion, bevor Amazon Redshift Serverless die mit der Transaktion verknüpfte Sitzung beendet, beträgt sechs Stunden. Weitere Informationen finden Sie unter Kontingente für Objekte von Amazon Redshift Serverless.

Verbinden mit Amazon Redshift Serverless

Sobald Sie Ihre Amazon-Redshift-Serverless-Instance eingerichtet haben, können Sie eine Verbindung mit verschiedenen Methoden herstellen. Diese sind unten beschrieben. Wenn Sie mehrere Teams oder Projekte haben und die Kosten separat verwalten möchten, können Sie separate AWS-Konten verwenden.

Eine Liste, AWS-Regionen wo Amazon Redshift Serverless verfügbar ist, finden Sie in den Endpunkten, die für die Redshift Serverless API aufgeführt sind. Allgemeine Amazon Web Services-Referenz

Amazon Redshift Serverless stellt eine Verbindung zur serverlosen Umgebung AWS-Konto in Ihrer aktuellen Umgebung her. AWS-Region Amazon Redshift Serverless wird in einer VPC innerhalb der Portbereiche 5431–5455 und 8191–8215 ausgeführt. Der Standardwert ist 5439. Derzeit können Sie Ports nur mit der API-Operation `UpdateWorkgroup` und der Operation ändern. AWS CLI `update-workgroup`

Verbinden mit Amazon Redshift Serverless

Sie können eine Verbindung mit einer Datenbank (namens `dev`) in Amazon Redshift Serverless mit der folgenden Syntax herstellen.

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

Die folgende Verbindungszeichenfolge gibt beispielsweise die Region us-east-1 an.

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

Verbinden mit Amazon Redshift Serverless über JDBC-Treiber

Sie können eine der folgenden Methoden verwenden, um mit dem von Amazon RedShift bereitgestellten JDBC-Treiber Version 2 eine Verbindung mit Amazon Redshift Serverless mit Ihrem bevorzugten SQL-Client herzustellen.

Verwenden Sie die folgende Syntax, um eine Verbindung mit Anmeldeinformationen für die Datenbankauthentifizierung unter Verwendung des JDBC-Treibers Version 2.1.x oder höher herzustellen. Die Portnummer ist optional; falls nicht enthalten, verwendet Amazon Redshift Serverless standardmäßig die Portnummer 5439. Sie können zu einem anderen Port aus dem Portbereich 5431–5455 oder 8191–8215 wechseln. Verwenden Sie die AWS CLI und die Amazon-Redshift-API, um den Standardport für einen Serverless-Endpunkt zu ändern.

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

Die folgende Verbindungszeichenfolge gibt beispielsweise die Arbeitsgruppen-Standardeinstellung, die Konto-ID 123456789012 und die Region us-east-2 an.

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

Verwenden Sie die folgende Syntax, um eine Verbindung mit IAM über den JDBC-Treiber Version 2.1.x oder höher herzustellen. Die Portnummer ist optional; falls nicht enthalten, verwendet Amazon Redshift Serverless standardmäßig die Portnummer 5439. Sie können zu einem anderen Port aus dem Portbereich 5431–5455 oder 8191–8215 wechseln. Um den Standardport für einen serverlosen Endpunkt zu ändern, verwenden Sie die AWS CLI Amazon Redshift Redshift-API.

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

Die folgende Verbindungszeichenfolge gibt beispielsweise die Arbeitsgruppen-Standardeinstellung, die Konto-ID 123456789012 und die Region us-east-2 an.

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

Verwenden Sie die folgende Syntax für ODBC.

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

Wenn Sie eine ältere JDBC-Treiberversion verwenden als 2.1.0.9 und eine Verbindung mit IAM herstellen, müssen Sie die folgende Syntax verwenden.

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

Die folgende Verbindungszeichenfolge gibt beispielsweise den Arbeitsgruppen-Standard und den Wert us-east-1 an. AWS-Region

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

Weitere Informationen zu Treibern finden Sie unter Konfigurieren von Verbindungen in Amazon Redshift.

So finden Sie die JDBC- und die ODBC-Verbindungszeichenfolge

Sie benötigen die JDBC- oder ODBC-Verbindungszeichenfolge, um mit Ihrem SQL-Client-Tool eine Verbindung zu Ihrer Arbeitsgruppe herzustellen. Sie finden die Verbindungszeichenfolge in der Amazon-Redshift-Serverless-Konsole auf der Detailseite einer Arbeitsgruppe.

So finden Sie die Verbindungszeichenfolge für eine Arbeitsgruppe

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Redshift Serverless aus.
3. Wählen Sie im Navigationsmenü Arbeitsgruppenkonfiguration und dann den Namen der Arbeitsgruppe in der Liste aus, um die zugehörigen Details anzuzeigen.
4. Die JDBC-URL- und ODBC-URL-Verbindungszeichenfolgen finden Sie zusammen mit zusätzlichen Details im Abschnitt Allgemeine Informationen. Jede Zeichenfolge basiert auf der

AWS Region, in der die Arbeitsgruppe ausgeführt wird. Wählen Sie das Symbol neben der entsprechenden Verbindungszeichenfolge aus, um die Verbindungszeichenfolge zu kopieren.

Verbinden mit Amazon Redshift Serverless über die Daten-API

Sie können die Amazon-Redshift-Daten-API auch verwenden, um eine Verbindung mit Amazon Redshift Serverless herzustellen. Verwenden Sie in Ihren AWS CLI Aufrufen den `workgroup-name` Parameter anstelle des `cluster-identifier` Parameters.

Weitere Informationen zur Daten-API finden Sie unter Verwenden der Amazon Redshift Data API. Beispielcode, der die Daten-API in Python aufruft, und andere Beispiele finden Sie unter Erste Schritte mit der Redshift Data API und suchen Sie in den `use-cases` Ordnern `quick-start` und unter. GitHub

Verbinden mit Amazon Redshift Serverless über SSL

Konfigurieren einer sicheren Verbindung zu Amazon Redshift Serverless

Um SSL-Verbindungen zu unterstützen, erstellt und installiert Redshift Serverless für jede Arbeitsgruppe ein AWS Certificate Manager (ACM) ausgestelltes SSL-Zertifikat. ACM-Zertifikaten wird von den meisten Betriebssystemen, Webbrowsern und Clients öffentlich vertraut. Möglicherweise müssen Sie ein Zertifikatspaket herunterladen, wenn Ihre SQL-Clients oder -Anwendungen über SSL eine Verbindung zu Redshift Serverless herstellen und die `sslmode` Verbindungsoption auf `requireverify-ca`, oder gesetzt ist. `verify-full` Wenn Ihr Client ein Zertifikat benötigt, stellt Redshift Serverless ein Bundle-Zertifikat wie folgt bereit:

- Laden Sie das Paket von https://s3.amazonaws.com/redshift-downloads/ amazon-trust-ca-bundle .crt herunter.
  - Die erwartete MD5-Prüfsummennummer ist 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - Die sha256-Prüfsummennummer ist 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  Verwenden Sie nicht das vorherige Zertifikatpaket, das auf `https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt` zu finden ist.
- Laden Sie das Paket in China AWS-Region von https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt herunter.
  - Die erwartete MD5-Prüfsummennummer ist 418dea9b6d5d5de7a8f1ac42e164cdcf.

- Die sha256-Prüfsummennummer ist 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

Verwenden Sie nicht vorherige Zertifikatpakete, die auf `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` und `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem` zu finden sind.

> **Important**
>
> Redshift Serverless hat die Art und Weise geändert, wie SSL-Zertifikate verwaltet werden. Möglicherweise müssen Sie Ihre aktuellen Trust-Root-CA-Zertifikate aktualisieren, um weiterhin über SSL eine Verbindung zu Ihren Arbeitsgruppen herstellen zu können. Weitere Informationen zu ACM-Zertifikaten für SSL-Verbindungen finden Sie unter. Umstellung auf ACM-Zertifikate für SSL-Verbindungen

Standardmäßig akzeptieren Arbeitsgruppendatenbanken eine Verbindung, unabhängig davon, ob sie SSL verwendet oder nicht.

Um eine neue Arbeitsgruppe zu erstellen, die nur SSL-Verbindungen akzeptiert, verwenden Sie den `create-workgroup` Befehl und setzen Sie den `require_ssl` Parameter auf. `true` Um das folgende Beispiel zu verwenden, *`yourNamespaceName`*ersetzen Sie es durch den Namen Ihres Namespaces und *`yourWorkgroupName`*durch den Namen Ihrer Arbeitsgruppe.

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

Um eine bestehende Arbeitsgruppe so zu aktualisieren, dass sie nur SSL-Verbindungen akzeptiert, verwenden Sie den `update-workgroup` Befehl und setzen Sie den `require_ssl` Parameter auf. `true` Beachten Sie, dass Redshift Serverless Ihre Arbeitsgruppe neu startet, wenn Sie den Parameter aktualisieren. `require_ssl` Um das folgende Beispiel zu verwenden, *`yourWorkgroupName`*ersetzen Sie es durch den Namen Ihrer Arbeitsgruppe.

```
aws redshift-serverless update-workgroup \
--workgroup-name yourWorkgroupName \
```

```
--config-parameters parameterKey=require_ssl,parameterValue=true
```

Amazon Redshift unterstützt das Elliptic Curve Diffie–Hellman Ephemeral (ECDHE) Key Agreement-Protokoll. Mit ECDHE besitzen sowohl der Client als auch der Server ein öffentlich-privates Elliptic Curve-Schlüsselpaar, das verwendet wird, um ein gemeinsames Geheimnis über einen nicht sicheren Kanal einzurichten. Sie müssen nichts in Amazon Redshift konfigurieren, um ECDHE zu aktivieren. Wenn Sie sich von einem SQL-Client-Tool aus verbinden, das ECDHE verwendet, um die Kommunikation zwischen dem Client und dem Server zu verschlüsseln, verwendet Amazon Redshift die angegebene Verschlüsselungsliste, um die entsprechende Verbindung herzustellen. Weitere Informationen finden Sie unter Diffie-Hellman-Schlüsselaustausch auf Wikipedia und Ciphers (Verschlüsselungsverfahren) auf der OpenSSL-Website.

Herstellen einer Verbindung mit Amazon Redshift Serverless von einem von Amazon Redshift verwalteten VPC-Endpunkt aus

Verbinden mit Amazon Redshift Serverless von anderen VPC-Endpunkten

Informationen zur Einrichtung oder Konfiguration eines verwalteten VPC-Endpoints für eine Amazon Redshift Serverless-Arbeitsgruppe finden Sie unter Arbeiten mit von Redshift verwalteten VPC-Endpunkten.

Verbinden mit Amazon Redshift Serverless über einen Redshift-VPC-Endpunkt in einem anderen Konto oder einer anderen Region

Verbinden mit Amazon Redshift Serverless über einen VPC-Kreuzendpunkt

Amazon Redshift Serverless wird in einer VPC bereitgestellt. Sie können den Zugriff auf eine VPC in einem anderen Konto gewähren, um in Ihrem Konto auf Amazon Redshift Serverless zuzugreifen. Dies ist einer Verbindung über einen verwalteten VPC-Endpunkt vergleichbar. In diesem Fall stammt die Verbindung jedoch beispielsweise aus einem Datenbank-Client in einem anderen Konto. Es gibt einige Operationen, die Sie ausführen können:

- Ein Datenbankbesitzer kann einem anderen Konto in derselben Region Zugriff auf eine VPC gewähren, die Amazon Redshift Serverless enthält.
- Ein Datenbankbesitzer kann den Zugriff auf Amazon Redshift Serverless widerrufen.

Der Hauptvorteil des kontoübergreifenden Zugriffs liegt in einer einfacheren Datenbankzusammenarbeit. Benutzer müssen nicht in dem Konto bereitgestellt werden, das die

Datenbank enthält, um auf sie zugreifen zu können. Dies reduziert die Zahl der Konfigurationsschritte und spart Zeit.

Erforderliche Berechtigungen für die Gewährung des Zugriffs auf eine VPC in einem anderen Konto

Um Zugriff zu gewähren oder den gewährten Zugriff zu ändern, benötigt die gewährende Person eine zugewiesene Berechtigungsrichtlinie mit den folgenden Berechtigungen:

- redshift-serverlos: PutResourcePolicy
- redshift-serverlos: GetResourcePolicy
- redshift-serverlos: DeleteResourcePolicy
- ec2: CreateVpcEndpoint
- ec2: ModifyVpcEndpoint

Möglicherweise benötigen Sie weitere Berechtigungen, die in der AWS verwalteten Richtlinie AmazonRedshiftFullAccessangegeben sind. Weitere Informationen finden Sie unter Gewähren von Berechtigungen für Amazon Redshift Serverless.

Der Gewährungsempfänger benötigt eine zugewiesene Berechtigungsrichtlinie mit den folgenden Berechtigungen:

- redshift-serverlos: ListWorkgroups
- redshift-serverlos: CreateEndpointAccess
- redshift-serverlos: UpdateEndpointAccess
- redshift-serverlos: GetEndpointAccess
- redshift-serverlos: ListEndpointAccess
- redshift-serverlos: DeleteEndpointAccess

Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Dies ist ein Beispiel für eine Ressourcenrichtlinie zur Konfiguration eines VPC-übergreifenden Zugriffs:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountCrossVPCAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                   "123456789012",
                   "234567890123"
                ]
             },
            "Action": [
                "redshift-serverless:CreateEndpointAccess",
                "redshift-serverless:UpdateEndpointAccess",
                "redshift-serverless:DeleteEndpointAccess",
                "redshift-serverless:GetEndpointAccess"
            ],
            "Condition": {
                "ArnLike": {
                    "redshift-serverless:AuthorizedVpc": [
                        "arn:aws:ec2:us-east-1:123456789012:vpc/*",
                        "arn:aws:ec2:us-east-1:234567890123:vpc/vpc-456",
                        "arn:aws:ec2:us-east-1:234567890123:vpc/vpc-987"
                        ]
                    }
                }
            }
        }
    ]
}
```

Die Verfahren in diesem Abschnitt setzen voraus, dass der ausführende Benutzer die entsprechenden zugewiesenen Berechtigungen besitzt, z. B. über eine zugewiesene IAM-Rolle, die diese Berechtigungen auflistet. Die Verfahren setzen auch voraus, dass der Arbeitsgruppe eine IAM-Rolle mit entsprechenden Ressourcenberechtigungen angefügt ist.

Gewährung des VPC-Zugriffs auf andere Konten über die Konsole

Dieses Verfahren zeigt die Schritte für die Konfiguration des Datenbankzugriffs, wenn Sie der Datenbankbesitzer sind und Zugriff auf die Datenbank gewähren möchten.

Gewährung des Zugriffs über das Besitzerkonto

1. In den Eigenschaften für die Amazon-Redshift-Serverless-Arbeitsgruppe finden Sie auf der Registerkarte Datenzugriff eine Liste mit dem Namen Gewährte Konten. Sie enthält die Konten und VPCs, denen Zugriff auf die Arbeitsgruppe gewährt wurde. Suchen Sie die Liste und wählen Sie Zugriff gewähren aus, um der Liste ein Konto hinzuzufügen.
2. Anschließend wird ein Fenster angezeigt, in das Sie Informationen zum Gewährungsempfänger eingeben können. Geben Sie die AWS -Konto-ID ein. Dies ist die 12-stellige ID des Kontos, auf das Sie Zugriff gewähren möchten.
3. Sie können dem Gewährungsempfänger Zugriff auf alle VPCs oder auf bestimmte VPCs gewähren. Wenn Sie nur bestimmten VPCs Zugriff gewähren, können Sie die IDs hinzufügen, indem Sie jede einzelne ID eingeben und VPC hinzufügen auswählen.
4. Wenn Sie fertig sind, wählen Sie Änderungen speichern aus.

Wenn Sie die Änderungen speichern, wird das Konto in der Liste Gewährte Konten angezeigt. Der Eintrag zeigt die Konto-ID und die Liste der VPCs an, denen Zugriff gewährt wurde.

Der Datenbankbesitzer kann den Zugriff auf ein Konto auch widerrufen. Der Besitzer kann den Zugriff jederzeit widerrufen.

Widerrufen des Zugriffs auf ein Konto

1. Sie können mit der Liste der gewährten Konten beginnen. Wählen Sie zunächst ein oder mehrere Konten aus.
2. Wählen Sie Zugriff widerrufen aus.

Nach der Gewährung des Zugriffs kann ein Datenbankadministrator des Gewährungsempfängers in der Konsole überprüfen, ob der Zugriff vorhanden ist.

Überprüfen über die Konsole, ob Ihnen Zugriff auf ein anderes Konto gewährt wurde

1. In den Eigenschaften für die Amazon-Redshift-Serverless-Arbeitsgruppe finden Sie auf der Registerkarte Datenzugriff eine Liste mit dem Namen Autorisierte Konten. Anschließend werden die Konten angezeigt, auf die der Zugriff über diese Arbeitsgruppe möglich ist. Der Gewährungsempfänger kann die Endpunkt-URL der Arbeitsgruppe nicht verwenden, um direkt auf die Arbeitsgruppe zuzugreifen. Um auf die Arbeitsgruppe zuzugreifen, wechseln Sie als Gewährungsempfänger zum Abschnitt Endpunkt und wählen Endpunkt erstellen aus.

2. Anschließend geben Sie als Gewährungsempfänger einen Endpunktnamen und eine VPC für den Zugriff auf die Arbeitsgruppe an.
3. Nach erfolgreicher Erstellung des Endpunkts wird er im Abschnitt Endpunkt angezeigt und erhält eine Endpunkt-URL. Über diese Endpunkt-URL können Sie auf die Arbeitsgruppe zuzugreifen.

Gewähren von Zugriff auf andere Konten über CLI-Befehle

Das Konto, das den Zugriff gewährt, muss zunächst den Zugriff auf ein anderes Konto gewähren, um eine Verbindung über `put-resource-policy` herzustellen. Der Datenbankbesitzer kann `put-resource-policy` aufrufen, um ein anderes Konto zur Erstellung von Verbindungen mit der Arbeitsgruppe zu autorisieren. Das Konto des Gewährungsempfängers kann dann `create-endpoint-authorization` verwenden, um über die zugelassenen VPCs Verbindungen mit der Arbeitsgruppe herzustellen.

Im Folgenden werden die Eigenschaften für `put-resource-policy` gezeigt, die Sie aufrufen können, um den Zugriff auf ein bestimmtes Konto und eine bestimmte VPC zuzulassen.

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

Nach dem Aufruf des Befehls können Sie `get-resource-policy` unter Angabe von `resource-arn` aufrufen, um die Konten und VPCs mit Zugriff auf die Ressource anzuzeigen.

Der folgende Aufruf kann vom Gewährungsempfänger ausgeführt werden. Anschließend werden Informationen zum gewährten Zugriff angezeigt. Insbesondere wird eine Liste mit den VPCs zurückgegeben, denen Zugriff gewährt wurde.

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

So kann der Gewährungsempfänger Informationen zu Endpunktautorisierungen aus dem gewährenden Konto erhalten. Das `owner-account` ist das teilende Konto. Wenn Sie dies ausführen, werden die `CrossAccountVpcs` für jede Arbeitsgruppe zurückgegeben. Dies ist eine Liste der zulässigen VPCs. Zur Referenz werden im Folgenden alle Eigenschaften aufgeführt, die für eine Arbeitsgruppe verfügbar sind:

```
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

Zur Erinnerung: Die Cluster-Verschiebung ist keine Voraussetzung für die Konfiguration von zusätzlichen Redshift-Netzwerk-Features, wie beispielsweise den Features, die für die Notfallwiederherstellung oder andere Zwecke verwendet werden. Sie ist außerdem für Folgendes nicht erforderlich:

- Verbindung von einer konto- oder regionsübergreifenden VPC zu Redshift herstellen — Sie können eine Verbindung von einer AWS Virtual Private Cloud (VPC) zu einer anderen herstellen, die eine Redshift-Datenbank enthält, wie in diesem Abschnitt beschrieben.
- Einrichtung eines benutzerdefinierten Domain-Namens – Sie können für Ihren Amazon-Redshift-Cluster oder Ihre Amazon-Redshift-Serverless-Arbeitsgruppe einen benutzerdefinierten Domain-Namen (auch als benutzerdefinierte URL bezeichnet) erstellen, um den Endpunktnamen einprägsamer und einfacher zu gestalten. Weitere Informationen finden Sie unter Verwendung eines benutzerdefinierten Domain-Namens für Client-Verbindungen.

Konfiguration geeigneter Netzwerkverkehrseinstellungen für Amazon Redshift Serverless

Verbindung zu Amazon Redshift Serverless bei öffentlicher Zugänglichkeit

Anweisungen zum Einrichten Ihrer Einstellungen für den Netzwerkverkehr finden Sie unter Öffentlicher Zugriff mit standardmäßiger oder benutzerdefinierter Sicherheitsgruppenkonfiguration. Dies schließt einen Anwendungsfall ein, bei dem der Cluster öffentlich zugänglich ist.

Verbindung zu Amazon Redshift Serverless ohne öffentliche Zugänglichkeit

Anweisungen zum Einstellen der Einstellungen für den Netzwerkverkehr finden Sie unter Privater Zugriff mit standardmäßiger oder benutzerdefinierter Sicherheitsgruppenkonfiguration. Dies schließt einen Anwendungsfall ein, bei dem der Cluster nicht für das Internet verfügbar ist.

Definieren von Datenbankrollen, die Verbundbenutzern in Amazon Redshift Serverless zugewiesen werden sollen

Sie können in Ihrer Organisation Rollen definieren, die festlegen, welche Datenbankrollen in Amazon Redshift Serverless zugewiesen werden. Weitere Informationen finden Sie unter Definieren von Datenbankrollen, die Verbundbenutzern in Amazon Redshift Serverless zugewiesen werden sollen.

Weitere Ressourcen

Weitere Informationen zu sicheren Verbindungen mit Amazon Redshift Serverless, einschließlich der Erteilung von Berechtigungen, der Autorisierung des Zugriffs auf zusätzliche Services und der Erstellung von IAM-Rollen, finden Sie unter Identity and Access Management in Amazon Redshift Serverless.

Definieren von Datenbankrollen, die Verbundbenutzern in Amazon Redshift Serverless zugewiesen werden sollen

Wenn Sie Teil einer Organisation sind, verfügen Sie über eine Reihe von zugeordneten Rollen. Zum Beispiel gibt es Rollen für Ihre berufliche Funktion, wie Programmierer und Manager. Ihre Rollen bestimmen, auf welche Anwendungen und Daten Sie zugreifen können. Die meisten Organisationen nutzen einen Identitätsanbieter wie Microsoft Active Directory, um Benutzern und Gruppen Rollen zuzuweisen. Rollen werden zunehmend zur Kontrolle des Zugriffs auf Ressourcen verwendet, da Organisationen nicht mehr so viele einzelne Benutzer verwalten müssen.

Vor Kurzem wurde die rollenbasierte Zugriffskontrolle in Amazon Redshift Serverless eingeführt. Mithilfe von Datenbankrollen können Sie den Zugriff auf Daten und Objekte wie beispielsweise Schemas oder Tabellen sichern. Sie können Rollen auch verwenden, um eine Reihe von höheren Berechtigungen zu definieren, z. B. für Systemüberwacher oder Datenbankadministratoren. Nachdem Sie Datenbankrollen Ressourcenberechtigungen erteilt haben, müssen Sie jedoch einen weiteren Schritt ausführen. Dieser besteht darin, die Rollen eines Benutzers aus der Organisation mit den Datenbankrollen zu verbinden. Sie können jedem Benutzer die entsprechenden Datenbankrollen bei der ersten Anmeldung zuweisen, indem Sie SQL-Anweisungen ausführen. Dies bedeutet jedoch einen großen Aufwand. Eine einfachere Methode besteht darin, die Datenbankrollen zu definieren, um sie zuzuweisen und an Amazon Redshift Serverless zu übergeben. Dies hat den Vorteil, dass die Erstanmeldung vereinfacht wird.

Sie können Rollen mit `GetCredentials` an Amazon Redshift Serverless übergeben. Wenn sich ein Benutzer zum ersten Mal bei einer Datenbank in Amazon Redshift Serverless anmeldet, wird ein zugeordneter Datenbankbenutzer erstellt und den entsprechenden Datenbankrollen zugeordnet. In diesem Thema wird der Vorgang zum Übergeben von Rollen an Amazon Redshift Serverless beschrieben.

Das Übergeben von Datenbankrollen hat zwei Hauptanwendungsfälle:

- Wenn sich ein Benutzer über einen externen Identitätsanbieter anmeldet, in der Regel mit konfiguriertem Verbund, und die Rollen mithilfe eines Sitzungs-Tags weitergibt.
- Wenn sich ein Benutzer mit IAM-Anmeldeinformationen anmeldet und seine Rollen mithilfe eines Tag-Schlüssels und -Werts übergeben werden.

Weitere Informationen zur rollenbasierten Zugriffskontrolle finden Sie unter Rollenbasierte Zugriffskontrolle (RBAC).

Konfigurieren von Datenbankrollen

Bevor Sie Rollen an Amazon Redshift Serverless übergeben können, müssen Sie Datenbankrollen in Ihrer Datenbank konfigurieren und ihnen entsprechende Berechtigungen für Datenbankressourcen gewähren. In einem einfachen Szenario können Sie beispielsweise eine Datenbankrolle mit dem Namen Verkauf erstellen und ihr Zugriff zum Abfragen von Tabellen mit Verkaufsdaten gewähren. Weitere Informationen zum Erstellen von Datenbankrollen und zum Erteilen von Berechtigungen finden Sie unter CREATE ROLE und GRANT.

Anwendungsfälle für die Definition von Datenbankrollen, die Verbundbenutzern zugewiesen werden sollen

In diesen Abschnitten werden einige Anwendungsfälle beschrieben, in denen die Übergabe von Datenbankrollen an Amazon Redshift Serverless den Zugriff auf Datenbankressourcen vereinfachen kann.

Anmelden mithilfe eines Identitätsanbieters

Der erste Anwendungsfall setzt voraus, dass Ihre Organisation über Benutzeridentitäten in einem Service zur Identitäts- und Zugriffsverwaltung verfügt. Dieser Dienst kann cloudbasiert sein, beispielsweise JumpCloud oder Okta, oder lokal, wie Microsoft Active Directory. Das Ziel besteht darin, die Rollen eines Benutzers vom Identitätsanbieter automatisch Ihren Datenbankrollen zuzuordnen, wenn der Benutzer sich bei einem Client wie beispielsweise dem Query Editor V2 oder mit einem JDBC-Client anmeldet. Um dies einzurichten, müssen Sie einige Konfigurationsaufgaben ausführen. Diese umfassen u. a. folgende:

1. Konfigurieren Sie die Verbundintegration mit Ihrem Identitätsanbieter (IDP) über eine Vertrauensstellung. Dies ist eine Grundvoraussetzung. Wenn Sie dies einrichten, ist der Identitätsanbieter dafür verantwortlich, den Benutzer über eine SAML-Assertion zu authentifizieren und Anmeldeinformationen bereitzustellen. Weitere Informationen finden Sie unter Integration von SAML-Lösungsanbietern von Drittanbietern mit. AWS Weitere Informationen finden Sie auch unter Verbundzugriff auf Amazon Redshift Query Editor V2 mit Active Directory Federation Services (AD FS) oder Single-Sign-On-Verbundzugriff auf Amazon Redshift Query Editor V2 mit Okta.
2. Der Benutzer muss über die folgenden Richtlinienberechtigungen verfügen:
   - `GetCredentials` – Stellt Anmeldeinformationen für die temporäre Autorisierung zur Anmeldung bei Amazon Redshift Serverless bereit.
   - `sts:AssumeRoleWithSAML`— Stellt einen Mechanismus zur Verknüpfung eines Unternehmensidentitätsspeichers oder -verzeichnisses mit dem rollenbasierten Zugriff bereit. AWS
   - `sts:TagSession` – Genehmigung für die Aktion TagSession auf dem Prinzipal des Identitätsanbieters.

   In diesem Fall gibt `AssumeRoleWithSAML` einen Satz an Sicherheitsanmeldeinformationen für Benutzer zurück, die über eine authentifizierte SAML-Antwort authentifiziert wurden. Dieser Vorgang bietet einen Mechanismus zum Verknüpfen eines Identitätsspeichers oder -verzeichnisses mit einem AWS rollenbasierten Zugriff ohne benutzerspezifische

Anmeldeinformationen. Im Fall von Benutzern mit der Berechtigung `AssumeRoleWithSAML` ist der Identitätsanbieter für die Verwaltung der SAML-Assertion verantwortlich, die zum Übergeben der Rolleninformationen verwendet wird.

Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

3. Sie konfigurieren das Tag `RedshiftDbRoles` mit den durch Doppelpunkte getrennten Rollenwerten im Format Rolle1:Rolle2. z. B. `manager:engineer`. Diese können von einer in Ihrem Identitätsanbieter konfigurierten Sitzungs-Tag-Implementierung abgerufen werden. Die SAML-Authentifizierungsanfrage übergibt die Rollen programmgesteuert. Weitere Informationen zum Übergeben von Sitzungs-Tags finden Sie unter Übergeben von Sitzungs-Tags in AWS STS.

   Wenn Sie einen Rollennamen übergeben, der in der Datenbank nicht vorhanden ist, wird er ignoriert.

In diesem Anwendungsfall werden die Rollen von Benutzern, die sich mithilfe einer Verbundidentität anmelden, in der Autorisierungsanfrage über den Schlüssel und Wert des Sitzungs-Tags übergeben. Daraufhin übergibt `GetCredentials` die Rollen nach der Autorisierung an die Datenbank. Nach einer erfolgreichen Verbindung werden die Datenbankrollen zugeordnet und der Benutzer kann der jeweiligen Rolle entsprechende Datenbankaufgaben ausführen. Der wesentliche Teil des Vorgangs besteht darin, dass dem `RedshiftDbRoles`-Sitzungs-Tag die Rollen in der ersten Autorisierungsanfrage zugewiesen werden. Weitere Informationen zum Übergeben von Sitzungs-Tags finden Sie unter Übergeben von Sitzungs-Tags mithilfe von SAML. AssumeRoleWith

Anmelden mithilfe von IAM-Anmeldeinformationen

Im zweiten Anwendungsfall können Rollen für einen Benutzer übergeben werden und dieser kann über IAM-Anmeldeinformationen auf eine Datenbank-Client-Anwendung zugreifen.

1. Dem Benutzer, der sich in diesem Fall anmeldet, müssen Richtlinienberechtigungen für die folgenden Aktionen zugewiesen werden:
   - `tag:GetResources` – Gibt mit Tags versehene Ressourcen zurück, die spezifischen Tags zugeordnet sind.
   - `tag:GetTagKeys` – Gibt die aktuell verwendeten Tag-Schlüssel zurück.

Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

2. Für den Zugriff auf den Datenbankservice, wie beispielsweise Amazon Redshift Serverless, sind auch Berechtigungen erforderlich.
3. Konfigurieren Sie für diesen Anwendungsfall die Tag-Werte für Ihre Rollen in AWS Identity and Access Management. Sie können sich dafür entscheiden, Tags zu bearbeiten und einen Tag-Schlüssel zu erstellen, der RedshiftDbRolesmit einer zugehörigen Tag-Wert-Zeichenfolge aufgerufen wird, die die Rollen enthält. Zum Beispiel manager:engineer.

Wenn sich ein Benutzer anmeldet, wird seine Rolle der Autorisierungsanfrage hinzugefügt und an die Datenbank übergeben. Sie wird einer vorhandenen Datenbankrolle zugeordnet.

Weitere Ressourcen

Wie in den Anwendungsfällen erwähnt, können Sie die Vertrauensstellung zwischen Ihrem IdP und AWS konfigurieren. Weitere Informationen finden Sie unter Konfigurieren des SAML-2.0-Identitätsanbieters mit Vertrauensstellung für die vertrauende Seite und Hinzufügen von Ansprüchen.

Identity and Access Management in Amazon Redshift Serverless

Für den Zugriff auf Amazon Redshift sind Anmeldeinformationen erforderlich, mit denen Sie Ihre Anfragen authentifizieren AWS können. Diese Anmeldeinformationen müssen über Berechtigungen für den Zugriff auf AWS Ressourcen wie Amazon Redshift Serverless verfügen.

In den folgenden Abschnitten erfahren Sie, wie Sie AWS Identity and Access Management (IAM) und Amazon Redshift verwenden können, um Ihre Ressourcen zu schützen, indem Sie kontrollieren, wer darauf zugreifen kann. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Amazon Redshift Serverless Berechtigungen gewähren

Für den Zugriff auf andere AWS Dienste benötigt Amazon Redshift Serverless Berechtigungen.

Autorisieren von Amazon Redshift Serverless, für Sie auf andere AWS Dienste zuzugreifen

Für einige Amazon Redshift-Funktionen muss Amazon Redshift in Ihrem Namen auf andere AWS Dienste zugreifen. Damit Ihre Amazon-Redshift-Serverless-Instance in Ihrem Namen aktiv werden kann, geben Sie Sicherheitsanmeldeinformationen für sie an. Die bevorzugte Methode zur Bereitstellung von Sicherheitsanmeldedaten ist die Angabe einer AWS Identity and Access Management (IAM-) Rolle. Sie können auch eine IAM-Rolle über die Amazon-Redshift-Konsole erstellen und als Standard festlegen. Weitere Informationen finden Sie unter Erstellen einer IAM-Rolle als Standard für Amazon Redshift.

Um auf andere AWS Dienste zuzugreifen, erstellen Sie eine IAM-Rolle mit den entsprechenden Berechtigungen. Sie müssen die Rolle auch Amazon Redshift Serverless zuordnen. Geben Sie außerdem entweder den Amazon-Ressourcennamen (ARN) der Rolle an, wenn Sie den Amazon-Redshift-Befehl ausführen, oder geben Sie das `default`-Schlüsselwort an.

Wenn Sie die Vertrauensstellung für die IAM-Rolle in https://console.aws.amazon.com/iam/ ändern, stellen Sie sicher, dass sie `redshift-serverless.amazonaws.com` und `redshift.amazonaws.com` als Prinzipaldienstnamen enthält. Informationen zur Verwaltung von IAM-Rollen für den Zugriff auf andere AWS Dienste in Ihrem Namen finden Sie unter. Amazon Redshift autorisieren, in Ihrem Namen auf andere AWS Dienste zuzugreifen

Erstellen einer IAM-Rolle als Standard für Amazon Redshift

Wenn Sie IAM-Rollen über die Amazon Redshift-Konsole erstellen, erstellt Amazon Redshift programmgesteuert die Rollen in Ihrem. AWS-Konto Amazon Redshift fügt ihnen auch automatisch bestehende AWS verwaltete Richtlinien hinzu. Bei dieser Methode können Sie in der Amazon-Redshift-Konsole bleiben und müssen zur Rollenerstellung nicht zur IAM-Konsole wechseln.

Bei der IAM-Rolle, die Sie über die Konsole für Ihren Cluster erstellen, ist die verwaltete Richtlinie `AmazonRedshiftAllCommandsFullAccess` automatisch angefügt. Diese IAM-Rolle ermöglicht es Amazon Redshift, Daten für AWS Ressourcen in Ihrem IAM-Konto zu kopieren, zu entladen, abzufragen und zu analysieren. Zu den entsprechenden Befehlen gehören COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL und CREATE LIBRARY. Weitere Informationen zum Erstellen einer IAM-Roll als Standard für Amazon Redshift finden Sie unter Erstellen einer IAM-Rolle als Standard für Amazon Redshift.

Um mit der Erstellung einer IAM-Rolle als Standard für Amazon Redshift zu beginnen, öffnen Sie die AWS Management Console, wählen Sie die Amazon Redshift Redshift-Konsole aus und wählen Sie dann im Menü Redshift Serverless aus. Über das Serverless-Dashboard können Sie eine neue Arbeitsgruppe erstellen. In den Schritten zur Erstellung können Sie eine IAM-Rolle auswählen oder eine neue IAM-Rolle konfigurieren.

Wenn Sie bereits über eine Amazon Redshift Serverless-Arbeitsgruppe verfügen und IAM-Rollen für diese konfigurieren möchten, öffnen Sie die. AWS Management Console Wählen Sie die Amazon Redshift Redshift-Konsole und dann Redshift Serverless. Wählen Sie auf der Amazon Redshift Serverless-Konsole die Namespace-Konfiguration für eine bestehende Arbeitsgruppe aus. Unter Sicherheit und Verschlüsselung können Sie die Berechtigungen bearbeiten.

Zuweisen von IAM-Rollen zu einem Namespace

Jede IAM-Rolle ist eine AWS Identität mit Berechtigungsrichtlinien, die festlegen, welche Aktionen jede Rolle AWS ausführen kann. Die Rolle sollte von jedem übernommen werden können, der sie benötigt. Darüber hinaus ist jeder Namespace eine Sammlung von Objekten, wie Tabellen und Schemata, und Benutzern. Wenn Sie Amazon Redshift Serverless verwenden, können Sie Ihrem Namespace mehrere IAM-Rollen zuordnen. Dies erleichtert die adäquate Strukturierung Ihrer Berechtigungen für eine Sammlung von Datenbankobjekten, sodass Rollen Aktionen sowohl für interne als auch für externe Daten ausführen können. Zum Beispiel, damit Sie einen `COPY`-Befehl in einer Amazon-Redshift-Datenbank ausführen können, um Daten von Amazon S3 abzurufen und eine Redshift-Tabelle auszufüllen.

Sie können einem Namespace über die Konsole mehrere Rollen zuordnen, wie zuvor in diesem Abschnitt beschrieben. Außerdem können Sie den API-Befehl `CreateNamespace` oder den CLI-Befehl `create-namespace` verwenden. Mit dem API- oder CLI-Befehl können Sie dem Namespace IAM-Rollen zuweisen, indem Sie `IAMRoles` mit einer oder mehreren Rollen ausfüllen. Insbesondere fügen Sie der Sammlung ARNs für bestimmte Rollen hinzu.

Verwalten von mit einem Namespace verknüpften IAM-Rollen

Auf der können AWS Management Console Sie die Berechtigungsrichtlinien für Rollen in AWS Identity and Access Management verwalten. Sie können IAM-Rollen für den Namespace verwalten, indem Sie die unter Namespace configuration (Namespace-Konfiguration) verfügbaren Einstellungen verwenden. Weitere Informationen zu Namespaces und deren Verwendung in Amazon Redshift Serverless finden Sie unter Übersicht über Arbeitsgruppen und Namespaces in Amazon Redshift Serverless.

Erste Schritte mit IAM-Anmeldeinformationen für Amazon Redshift

Wenn Sie sich zum ersten Mal bei der Amazon-Redshift-Konsole anmelden und Amazon Redshift Serverless zum ersten Mal ausprobieren, empfehlen wir, dass Sie sich als Benutzer mit einer angefügten IAM-Rolle anmelden, die über die erforderlichen Richtlinien verfügt. Nachdem Sie mit dem Erstellen einer Instance von Amazon Redshift Serverless begonnen haben, zeichnet Amazon Redshift den IAM-Rollennamen auf, den Sie bei der Anmeldung verwendet haben. Sie können dieselben Anmeldeinformationen verwenden, um sich bei der Amazon-Redshift-Konsole und der Konsole von Amazon Redshift Serverless anzumelden.

Beim Erstellen der Amazon-Redshift-Serverless-Instance können Sie eine Datenbank erstellen. Verwenden Sie den Abfrage-Editor v2, um mit der Option für temporäre Anmeldeinformationen eine Verbindung zur Datenbank herzustellen.

Um einen neuen Admin-Benutzernamen und ein neues Passwort permanent für die Datenbank hinzuzufügen, wählen Sie Customize admin user credentials (Anpassen von Administratoranmeldeinformationen) aus und geben Sie einen neuen Benutzernamen und ein Passwort für den Administrator ein.

Verwenden Sie eine IAM-Rolle, um mit der Verwendung von Amazon Redshift Serverless zu beginnen und zum ersten Mal eine Arbeitsgruppe und einen Namespace in der Konsole zu erstellen. Stellen Sie sicher, dass diese Rolle entweder über die Administratorberechtigung `arn:aws:iam::aws:policy/AdministratorAccess` oder die vollständige Amazon-Redshift-Berechtigung `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess` verfügt, die der IAM-Richtlinie angefügt ist.

In den folgenden Szenarien wird beschrieben, wie Ihre IAM-Anmeldeinformationen von Amazon Redshift Serverless verwendet werden, wenn Sie mit der Nutzung der Amazon-Redshift-Serverless-Konsole beginnen:

- Wenn Sie Use default settings (Standardeinstellungen verwenden) angeben, wandelt Amazon Redshift Serverless Ihre aktuelle IAM-Identität in einen Datenbank-Superuser um. Sie können dieselbe IAM-Identität mit der Amazon-Redshift-Serverless-Konsole verwenden, um Superuser-Aktionen in Ihrer Datenbank in Amazon Redshift Serverless durchzuführen.
- Wen Sie Customize settings (Einstellungen anpassen) auswählen, ohne einen Admin user name (Administrator-Benutzernamen) und ein Passwort anzugeben, verwendet Amazon Redshift Serverless Ihre aktuellen IAM-Anmeldeinformationen als Standard-Administratoranmeldeinformationen.

- Wenn Sie Customize settings (Einstellungen anpassen) auswählen und einen Admin unser name (Administrator-Benutzernamen) und ein Passwort angeben, wandelt Amazon Redshift Serverless Ihre aktuelle IAM-Identität in einen Datenbank-Superuser um. Amazon Redshift Serverless erstellt auch eine weitere dauerhafte Kombination aus Benutzername und Passwort für einen Superuser. Sie können entweder Ihre aktuelle IAM-Identität oder das erstellte Paar aus Benutzername und Passwort verwenden, um sich als Superuser in Ihrer Datenbank anzumelden.

Verwalten des Zugriffs auf Datenbankobjekte von Amazon Redshift Serverless mit Datenbankrollenberechtigungen

Dieses Verfahren zeigt, wie Sie die Berechtigung erteilen, eine Tabelle über eine Amazon-Redshift-Datenbankrolle abzufragen. Die Rolle wird mithilfe eines Tags zugewiesen, das einem Benutzer in IAM angefügt ist und bei der Anmeldung an Amazon Redshift übergeben wird. Es ist eine beispielhafte Erklärung der unter Definieren von Datenbankrollen, die Verbundbenutzern in Amazon Redshift Serverless zugewiesen werden sollen genannten Konzepte. Der Vorteil dieser Schritte besteht darin, dass Sie einem Benutzer eine Datenbankrolle zuordnen können und seine Berechtigungen nicht für jedes Datenbankobjekt festlegen müssen. Es vereinfacht die Verwaltung der Fähigkeit des Benutzers, Daten abzufragen, zu ändern oder zu Tabellen hinzuzufügen sowie andere Aktionen auszuführen.

Das Verfahren setzt voraus, dass Sie bereits eine Datenbank von Amazon Redshift Serverless eingerichtet haben und dass Sie in der Datenbank Berechtigungen gewähren können. Außerdem wird vorausgesetzt, dass Sie berechtigt sind, einen IAM-Benutzer in der AWS Konsole zu erstellen, eine IAM-Rolle zu erstellen und Richtlinienberechtigungen zuzuweisen.

1. Erstellen Sie einen IAM-Benutzer mithilfe der IAM-Konsole. Später stellen Sie mit diesem Benutzer eine Verbindung mit der Datenbank her.
2. Erstellen Sie eine Redshift-Datenbankrolle mit dem Abfrage-Editor v2 oder einem anderen SQL-Client. Weitere Informationen zum Erstellen von Datenbankrollen finden Sie unter CREATE ROLE.

   ```
   CREATE ROLE urban_planning;
   ```

   Fragen Sie die Systemansicht SVV_ROLES ab, um zu überprüfen, ob Ihre Rolle erstellt wurde. Es werden außerdem Systemrollen zurückgegeben.

```
SELECT * from SVV_ROLES;
```

3. Erteilen Sie der von Ihnen erstellten Datenbankrolle die Berechtigung, Daten aus einer Tabelle auszuwählen. (Der IAM-Benutzer, den Sie erstellt haben, meldet sich irgendwann an und wählt mithilfe der Datenbankrolle Datensätze aus der Tabelle aus.) Der Rollenname und der Tabellenname im folgenden Codebeispiel sind Beispiele. Hier wird die Berechtigung erteilt, Daten aus einer Tabelle mit dem Namen `cities` auszuwählen.

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

4. Verwenden Sie die AWS Identity and Access Management Konsole, um eine IAM-Rolle zu erstellen. Diese Rolle erteilt die Berechtigung zur Verwendung des Abfrage-Editors v2. Erstellen Sie eine neue IAM-Rolle und wählen Sie für den Typ der vertrauenswürdigen Entität AWS -Konto aus. Klicken Sie dann auf Konto hinzufügen. Erteilen Sie der Rolle die folgende Richtlinienberechtigungen:

   - `AmazonRedshiftReadOnlyAccess`
   - `tag:GetResources`
   - `tag:GetTagKeys`
   - Alle Aktionen für sqlworkbench, einschließlich `sqlworkbench:ListDatabases` und `sqlworkbench:UpdateConnection`.

5. Fügen Sie in der IAM-Konsole dem IAM-Benutzer, den Sie zuvor erstellt haben, ein Tag mit dem Schlüssel `RedshiftDbRoles` hinzu. Der Wert des Tags sollte mit der Datenbankrolle übereinstimmen, die Sie im ersten Schritt erstellt haben. Im Beispiel ist dies `urban_planning`.

Nachdem Sie diese Schritte ausgeführt haben, weisen Sie dem Benutzer, den Sie in der IAM-Konsole erstellt haben, die IAM-Rolle zu. Wenn sich der Benutzer mit dem Abfrage-Editor v2 bei der Datenbank anmeldet, wird sein Datenbankrollenname im Tag an Amazon Redshift übergeben und mit ihm verknüpft. Somit kann er mithilfe der Datenbankrolle die entsprechenden Tabellen abfragen. Zur Veranschaulichung kann der Benutzer in diesem Beispiel die Tabelle `cities` über die Datenbankrolle `urban_planning` abfragen.

Migrieren eines bereitgestellten Clusters zu Amazon Redshift Serverless

Um von einem bereitgestellten Cluster zu Amazon Redshift Serverless zu migrieren, beachten Sie die folgenden Schritte.

Erstellen eines Snapshots Ihres bereitgestellten Clusters

Um Daten von Ihrem bereitgestellten Cluster zu Amazon Redshift Serverless zu übertragen, erstellen Sie einen Snapshot Ihres bereitgestellten Clusters und stellen diesen dann in Amazon Redshift Serverless wieder her. Amazon Redshift wandelt verschachtelte Schlüssel automatisch in zusammengesetzte Schlüssel um, wenn Sie einen Snapshot bereitgestellter Cluster in einem Serverless-Namespace wiederherstellen.

> **Note**
>
> Bevor Sie Ihre Daten zu einer Serverless-Arbeitsgruppe migrieren, stellen Sie sicher, dass die Anforderungen Ihres bereitgestellten Clusters mit der RPU-Menge kompatibel sind, die Sie in Amazon Redshift Serverless auswählen.

So erstellen Sie einen Snapshot Ihres bereitgestellten Clusters

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster), Snapshots und wählen Sie dann Create snapshot (Snapshot erstellen) aus.
3. Geben Sie die Eigenschaften der Snapshot-Definition ein und wählen Sie dann Create snapshot (Snapshot erstellen) aus. Es kann einige Zeit dauern, bis der Snapshot verfügbar ist.

So stellen Sie einen Snapshot bereitgestellter Cluster in einem Serverless-Namespace wieder her:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Navigieren Sie auf der Konsole für bereitgestellte Amazon Redshift-Cluster zur Seite Clusters (Cluster), Snapshots.

3. Wählen Sie einen Snapshot zum Verwenden aus.
4. Wählen Sie Restore snapshot (Snapshot wiederherstellen), Restore to serverless namespace (In Serverless-Namespace wiederherstellen).
5. Wählen Sie einen Namespace, in dem Sie Ihren Snapshot wiederherstellen möchten.
6. Bestätigen Sie, dass Sie von Ihrem Snapshot aus wiederherstellen möchten. Diese Aktion ersetzt alle Datenbanken auf Ihrem Serverless-Endpunkt durch die Daten aus Ihrem bereitgestellten Cluster. Wählen Sie Restore (Wiederherstellen) aus.

Weitere Informationen zu bereitgestellten Cluster-Snapshots finden Sie unter Amazon-Redshift-Snapshots.

Herstellen einer Verbindung mit Amazon Redshift Serverless über einen Treiber

Um mit Ihrem bevorzugten SQL-Client eine Verbindung zu Amazon Redshift Serverless herzustellen, können Sie den von Amazon Redshift bereitgestellten JDBC-Treiber Version 2 verwenden. Wir empfehlen, eine Verbindung mit der JDBC-Treiberversion 2.1.x oder höher herzustellen. Der Portnummer ist optional. Wenn Sie keine Angaben machen, verwendet Amazon Redshift Serverless standardmäßig die Portnummer 5439. Sie können zu einem anderen Port aus dem Portbereich 5431–5455 oder 8191–8215 wechseln. Verwenden Sie die AWS CLI und die Amazon-Redshift-API, um den Standardport für einen Serverless-Endpunkt zu ändern.

Den genauen Endpunkt für den JDBC-, ODBC- oder Python-Treiber finden Sie unter Arbeitsgruppenkonfiguration in Amazon Redshift Serverless. Sie können auch den Amazon Redshift Serverless API-Vorgang `GetWorkgroup` oder den AWS CLI Vorgang verwenden, `get-workgroups` um Informationen über Ihre Arbeitsgruppe zurückzugeben und dann eine Verbindung herzustellen.

Verbinden mit passwortbasierter Authentifizierung

Um eine Verbindung mit passwortbasierter Authentifizierung herzustellen, verwenden Sie die folgende Syntax.

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

Verwenden Sie die folgende Syntax, um eine Verbindung über den Amazon-Redshift-Python-Treiber herzustellen.

```
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
```

Herstellen einer Verbindung über IAM

Wenn Sie sich lieber mit IAM anmelden möchten, verwenden Sie den folgenden Treiberendpunkt. Mit diesem Treiberendpunkt können Sie eine Verbindung zu einer bestimmten Datenbank herstellen und die `GetCredentials`-API-Operation von Amazon Redshift Serverless verwenden.

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

Dieser Treiberendpunkt unterstützt die Anpassung von `dbUser`, `dbGroup` und `auto-create` nicht. Standardmäßig erstellt der Treiber automatisch Datenbankbenutzer bei der Anmeldung und weist sie Gruppen gemäß den Benutzergruppen zu, die Sie in IAM definiert haben. Hinweis: Gruppennamen, die Sie in IAM angeben, dürfen nur Kleinbuchstaben, Ziffern, Unterstriche (_), Pluszeichen (+), Punkte (.), At-Zeichen (@) oder Bindestriche (-) enthalten. Andernfalls stellt der Treiber möglicherweise keine Verbindung zu `dbGroup` her.

Stellen Sie sicher, dass Ihre AWS Identität über die richtige IAM-Richtlinie für die Aktion verfügt. `RedshiftServerlessGetCredentials` Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie, die einer AWS Identität die richtigen Berechtigungen für die Verbindung mit Amazon Redshift Serverless gewährt. Weitere Informationen zu IAM-Berechtigungen finden Sie unter IAM-Identitätsberechtigungen hinzufügen.

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

```
            "Resource": "*"
        }
    ]
}
```

Herstellen einer Verbindung über IAM mit dbUser und dbGroups

Wenn Sie benutzerdefinierte dbUser- und dbGroups-Verbindungsoptionen verwenden möchten, verwenden Sie den folgenden Treiberendpunkt. Wie der andere Serverless-Treiberendpunkt von Amazon Redshift auch erstellt diese Syntax automatisch Datenbankbenutzer bei der Anmeldung. Dieser Treiberendpunkt verwendet die API-Operation `GetCredentials` in Amazon Redshift Serverless. dbUser muss mit einem Buchstaben beginnen, darf nur alphanumerische Zeichen, Unterstriche (_), Pluszeichen (+), Punkte (.), At-Zeichen (@) oder Bindestriche (-) enthalten und muss weniger als 128 Zeichen lang sein. dbGroups darf nur Kleinbuchstaben, Zahlen, Unterstriche (_), Pluszeichen (+), Punkte (.), At-Zeichen (@) oder Bindestriche enthalten.

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

Verwenden Sie die folgende Syntax, um eine Verbindung über den Amazon-Redshift-Python-Treiber herzustellen.

```
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
```

Herstellen einer Verbindung über ODBC

Um eine Verbindung über ODBC herzustellen, verwenden Sie die folgende Syntax.

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

Verwenden des Amazon-Redshift-Serverless-SDK

Wenn Sie Verwaltungsskripte mit dem Amazon-Redshift-SDK geschrieben haben, müssen Sie das neue Amazon-Redshift-Serverless-SDK verwenden, um Amazon Redshift Serverless und zugehörige Ressourcen zu verwalten. Weitere Informationen zu verfügbaren API-Operationen finden Sie im API-Referenzhandbuch zu Amazon Redshift Serverless.

Übersicht über Arbeitsgruppen und Namespaces in Amazon Redshift Serverless

Wenn Sie Workloads isolieren und verschiedene Ressourcen in Amazon Redshift Serverless verwalten möchten, können Sie Namespaces und Arbeitsgruppen erstellen und Speicher- und Rechenressourcen separat verwalten.

Übersicht über Arbeitsgruppen und Namespaces in Amazon Redshift Serverless

Ein Namespace ist eine Sammlung von Datenbankobjekten und Benutzern. Der speicherbezogene Namespace gruppiert Schemas, Tabellen, Benutzer oder AWS Key Management Service Schlüssel zum Verschlüsseln von Daten. Zu den Speichereigenschaften gehören der Datenbankname und das Passwort des Administrators, Berechtigungen sowie Verschlüsselung und Sicherheit. Andere Ressourcen, die unter Namespaces gruppiert sind, umfassen Datashares, Wiederherstellungspunkte und Nutzungslimits. Sie können diese Speichereigenschaften mithilfe der Amazon Redshift Serverless-Konsole AWS Command Line Interface, der oder der Amazon Redshift Serverless APIs für die jeweilige Ressource konfigurieren.

Eine Arbeitsgruppe ist eine Sammlung von Rechenressourcen. Die rechenbezogene Arbeitsgruppe gruppiert Rechenressourcen wie RPUs, VPC-Subnetzgruppen und Sicherheitsgruppen.
Zu den Eigenschaften der Arbeitsgruppe gehören Netzwerk- und Sicherheitseinstellungen.
Andere Ressourcen, die unter Arbeitsgruppen gruppiert sind, umfassen Zugriffs- und Nutzungsbeschränkungen. Sie können diese Recheneigenschaften mit der Amazon Redshift Serverless-Konsole AWS Command Line Interface, den oder den Amazon Redshift Serverless APIs konfigurieren.

Sie können einen oder mehrere Namespaces und Arbeitsgruppen erstellen. Jedem Namespace kann nur eine Arbeitsgruppe zugeordnet sein. Umgekehrt kann jede Arbeitsgruppe nur einem Namespace zugeordnet werden.

Erste Schritte mit Amazon Redshift Serverless mit der Konsole

Das Einrichten von Amazon Redshift Serverless umfasst mehrere Konfigurationsschritte. Wenn Sie die Schritte zum Einrichten von Amazon Redshift Serverless ausführen, erstellen Sie einen Namespace und eine Arbeitsgruppe und verknüpfen sie miteinander. Um mit dem Einrichten der Konfiguration von Amazon Redshift Serverless mit der Amazon-Redshift-Serverless-Konsole zu beginnen, können Sie Get started with Amazon Redshift Serverless (Erste Schritte mit Amazon Redshift Serverless) auswählen, um Amazon Redshift Serverless einzurichten und damit zu interagieren. Sie können eine Umgebung mit Standardeinstellungen auswählen, was eine schnellere Einrichtung ermöglicht, oder die Einstellungen explizit gemäß den Anforderungen Ihres Unternehmens konfigurieren. Während dieses Vorgangs geben Sie Einstellungen für Ihre Arbeitsgruppe und den Namespace an.

Nachdem Sie die Umgebung eingerichtet haben, können Sie sich mithilfe von Eigenschaften von Arbeitsgruppen und Eigenschaften von Namespaces mit den Einstellungen vertraut machen.

Verwaltung von Arbeitsgruppen und Namespaces mithilfe der Amazon Redshift Serverless AWS Command Line Interface API

Neben der Verwendung der AWS Konsole können Sie auch die AWS CLI oder die Amazon Redshift Serverless API verwenden, um mit Arbeitsgruppen und Namespaces zu interagieren. In der folgenden Tabelle werden die API- und CLI-Operationen aufgeführt, die Sie für die Verwaltung von Snapshots und Wiederherstellungspunkten verwenden können.

API-Operation	CLI-Befehl	Beschreibung
CreateNamespace	create-namespace	Erstellt einen Namespace . Standardmäßig erstellt Amazon Redshift Serverless Namespaces mit einem AWS Key Management Service Standardschlüssel, aber Sie können einen anderen Schlüssel angeben, um Ihre Daten zu verschlüsseln. Sie können einen Namespace auch durch die Wiederher stellung eines Snapshots

API-Operation	CLI-Befehl	Beschreibung
		erstellen. Weitere Informationen finden Sie unter Arbeiten mit Snapshots und Wiederherstellungspunkten.
UpdateNamespace	update-namespace	Aktualisiert einen Namespace.
GetNamespace	get-namespace	Ruft Informationen zu einem Namespace ab.
ListNamepaces	list-namespaces	Ruft Informationen zu einer Liste von Namespaces ab.
DeleteNamespace	delete-namespace	Löscht einen Namespace.
CreateWorkgroup	create-workgroup	Erstellt eine Arbeitsgruppe. Stellen Sie beim Erstellen einer Arbeitsgruppe sicher, dass bereits ein Namespace vorhanden ist, den Sie der Arbeitsgruppe zuordnen können. Sie können beim Erstellen der Arbeitsgruppe Rechenressourcen wie Subnetze, Sicherheitsgruppen und RPUs angeben.
UpdateWorkgroup	update-workgroup	Aktualisiert eine Arbeitsgruppe.
GetWorkgroup	get-workgroup	Ruft Informationen zu einer Arbeitsgruppe ab.
ListWorkgroups	list-workgroups	Ruft Informationen zu einer Liste von Arbeitsgruppen ab.
DeleteWorkgroup	delete-workgroup	Löscht eine Arbeitsgruppe.

Verwalten von Amazon Redshift Serverless mithilfe der Konsole

Wenn Sie Data Warehouses in Amazon Redshift Serverless erstellen, bearbeiten oder löschen möchten, verwenden Sie Serverless dashboard (Serverless-Dashboard) auf der Amazon-Redshift-Konsole. Der Zugriff auf einzelne Konsoleneinstellungen hängt von Ihrer IAM-Rolle und Ihren Berechtigungen ab.

Weitere Informationen zur Einrichtung von Amazon Redshift Serverless finden Sie unter Ersteinrichtung von Amazon Redshift Serverless. Informationen zum Erstellen und Konfigurieren von Arbeitsgruppen finden Sie unter Arbeiten mit Arbeitsgruppen. Informationen zum Konfigurieren von Namespaces finden Sie unter Arbeiten mit Namespaces.

Ersteinrichtung von Amazon Redshift Serverless

Wenn Sie zum ersten Mal Serverless dashboard (Serverless-Dashboard) auswählen, werden Sie durch die Schritte zum Einrichten von Amazon Redshift Serverless geführt. Unter Get started with the serverless experience (Erste Schritte mit der Serverless-Umgebung) können Sie anhand eines Beispieldatensatzes ein Data Warehouse in Amazon Redshift Serverless einrichten. Amazon Redshift Serverless lädt den Beispieldatensatz während des Erstellungsprozesses automatisch. Sie können die Daten sofort abfragen, nachdem das Data Warehouse erstellt wurde. Weitere Informationen zur Ersteinrichtung von Amazon Redshift Serverless finden Sie unter Ersteinrichtung von Amazon Redshift Serverless.

Arbeiten mit Arbeitsgruppen

Wenn Sie Workloads isolieren und Ressourcen in Amazon Redshift Serverless verwalten möchten, können Sie Arbeitsgruppen und Namespaces erstellen. Die rechenbezogene Arbeitsgruppe gruppiert Rechenressourcen wie RPUs und VPC-Subnetzgruppen. Wenn Sie noch keine Arbeitsgruppe und keinen Namespace erstellt haben und nach Anleitungen zu den ersten Schritten mit Amazon Redshift Serverless suchen, informieren Sie sich unter Ersteinrichtung von Amazon Redshift Serverless.

Erstellen einer Arbeitsgruppe mit einem Namespace

Diese Schritte setzen voraus, dass Sie die Erstkonfiguration für Amazon Redshift Serverless abgeschlossen haben. Wenn Sie noch keine Arbeitsgruppe und keinen Namespace erstellt haben und nach Anleitungen zu den ersten Schritten mit Amazon Redshift Serverless suchen, informieren Sie sich unter Ersteinrichtung von Amazon Redshift Serverless.

Gehen Sie folgendermaßen vor, um eine Arbeitsgruppe zu erstellen:

1. Wählen Sie das Serverless dashboard (Serverless-Dashboard) aus. Wählen Sie dann Create workgroup (Arbeitsgruppe erstellen) aus.
2. Geben Sie einen Namen für die Arbeitsgruppe an.
3. Wählen Sie eine Virtual Private Cloud (VPC) für Amazon Redshift Serverless aus. Dadurch wird die Arbeitsgruppe einem bestimmten virtuellen Netzwerk in Ihrer Umgebung zugewiesen. AWS Weitere Informationen zu VPCs finden Sie unter Übersicht über VPCs und Subnetze.
4. Wählen Sie eine oder mehrere VPC security groups (VPC-Sicherheitsgruppen) aus. Weitere Informationen finden Sie unter Kontrollieren des Datenverkehrs zu Ressourcen mithilfe von Sicherheitsgruppen.
5. Geben Sie unter Subnet (Subnetz) ein oder mehrere Subnetze an, die Sie Ihrer Datenbank zuordnen möchten. Diese Subnetze sind in der VPC enthalten, die Sie zuvor ausgewählt haben, und müssen sich in drei verschiedenen Availability Zones befinden. Weitere Informationen finden Sie unter Überlegungen zur Verwendung von Amazon Redshift Serverless.
6. Wählen Sie die RPU-Basiskapazität entsprechend Ihren Anforderungen aus.

Einen Namespace auswählen

1. Sie können entweder Create new namespace (Neuen Namespace erstellen) auswählen und den Namespace-Namen eingeben oder auf Add to an existing namespace (Einem vorhandenen Namespace hinzufügen) klicken und den Namespace aus der Dropdown-Liste auswählen.
2. Geben Sie für Database name and password (Datenbankname und Passwort) den Namen der ersten Datenbank an. Sie können auch einen anderen Administrator als Ihren Standardkonsolenadministrator angeben, indem Sie die Admin user credentials (Administrator-Anmeldeinformationen) ändern.
3. Wählen Sie für Permissions (Berechtigungen) die Option Associate IAM role (IAM-Rolle zuweisen) aus, um bestimmte IAM-Rollen mit Ihrem Namespace und der Arbeitsgruppe zu verknüpfen. Weitere Informationen zum Verknüpfen von IAM-Rollen mit Amazon Redshift finden Sie unter Identity and Access Management in Amazon Redshift.
4. Sie können Ihre Verschlüsselungseinstellungen anpassen, indem Sie einen neuen Schlüssel erstellen oder einen anderen Schlüssel als den Standardschlüssel auswählen. Wählen Sie unter Audit logging (Prüfungsprotokollierung) die Protokolle aus, die exportiert werden sollen. Jeder Protokolltyp gibt verschiedene Metadaten an. Klicken Sie auf Continue (Weiter), um Ihre Einstellungen zu überprüfen.

Überprüfen von Arbeitsgruppeneinstellungen

1. Überprüfen Sie die Einstellungen unter Review and create (Überprüfen und erstellen). Hier werden die Einstellungen angezeigt, die Sie in den vorherigen Schritten ausgewählt haben.
2. Wählen Sie Speichern.

Nachdem Sie die Arbeitsgruppe erstellt haben, wird sie der Liste Workgroups (Arbeitsgruppen) hinzugefügt.

Erstellen einer Vorschau-Arbeitsgruppe

Sie können eine Amazon-Redshift-Serverless-Arbeitsgruppe in der Vorschau erstellen, um neue Funktionen von Amazon Redshift Serverless zu testen. Sie können diese Funktionen nicht in der Produktion verwenden und Ihre Vorschau-Arbeitsgruppe auch nicht in eine Produktionsarbeitsgruppe verschieben. Weitere Informationen zu den Bedingungen für Vorschauversionen finden Sie unter Betas und Vorversionen in den AWS -Servicebedingungen.

Die folgenden Funktionen sind zurzeit in Vorschau-Arbeitsgruppen verfügbar:

- Arbeiten mit Null-ETL-Integrationen

So erstellen Sie eine Arbeitsgruppe in der Vorschau

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Serverless-Dashboard und anschließend Arbeitsgruppenkonfiguration aus. Die Arbeitsgruppen für Ihr aktuelles Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jeder Arbeitsgruppe wird in Spalten in der Liste angezeigt.
3. Ein Banner auf der Seite Arbeitsgruppenkonfiguration stellt eine Vorschau der Arbeitsgruppen vor. Wählen Sie die Schaltfläche Create preview workgroup (Vorschau-Arbeitsgruppe erstellen) aus, um die Seite zum Erstellen von Arbeitsgruppen zu öffnen.
4. Geben Sie Eigenschaften für Ihre Arbeitsgruppe ein. Wir empfehlen, einen Namen für die Arbeitsgruppe zu verwenden, der darauf hinweist, dass sich diese in der Vorschau befindet. Wählen Sie Optionen für Ihre Arbeitsgruppe, einschließlich Optionen mit der Bezeichnung - preview (Vorschau), für die zu testenden Funktionen. Durchlaufen Sie die weiteren Seiten, um Optionen für Ihre Arbeitsgruppe und den Namespace einzugeben. Allgemeine Informationen zum

Erstellen von Arbeitsgruppen finden Sie unter the section called “Erstellen einer Arbeitsgruppe mit einem Namespace”.

5. Wählen Sie Vorschau-Arbeitsgruppe erstellen, um eine Arbeitsgruppe in der Vorschau zu erstellen.
6. Wenn Ihre Vorschau-Arbeitsgruppe verfügbar ist, verwenden Sie Ihren SQL-Client, um Daten zu laden und abzufragen.

Informationen zur Vorschau in bereitgestellten Clustern finden Sie unter Erstellen eines Vorschau-Clusters.

Anzeigen von Eigenschaften für eine Arbeitsgruppe

In Amazon Redshift Serverless ist eine Arbeitsgruppe eine Sammlung von Ressourcen, die verwendet werden können. Wenn Sie Amazon Redshift Serverless wählen, können Sie in der AWS Konsole im Navigationsmenü die Option Arbeitsgruppenkonfiguration auswählen, um eine Liste anzuzeigen. Sie können das Feld Search (Suchen) verwenden, um Arbeitsgruppen zu finden, die Ihren Suchkriterien entsprechen. Für jeden Arbeitsgruppeneintrag werden einige Eigenschaften angezeigt:

- Workgroup (Arbeitsgruppe) – Der Name der Arbeitsgruppe. Sie können den Namen auswählen, um die Eigenschaften der Arbeitsgruppe anzuzeigen und zu bearbeiten.
- Status – Zeigt an, ob die Arbeitsgruppe verfügbar ist.
- Namespace – Der Namespace, der der Arbeitsgruppe zugeordnet ist. Jeder Arbeitsgruppe ist ein Namespace zugeordnet.
- Creation date (Erstellungsdatum) – Das Datum, an dem die Arbeitsgruppe erstellt wurde.
- Tags – Mit der Arbeitsgruppe verknüpfte Tags.

Eigenschaften von Arbeitsgruppen

Sie können Arbeitsgruppen auflisten, indem Sie Workgroup configuration (Arbeitsgruppenkonfiguration) im linken Menü auswählen. Dann können Sie eine Arbeitsgruppe aus der Liste auswählen. In verschiedenen Bereichen werden Eigenschaften für die Arbeitsgruppe angezeigt. Sie können auch Aktionen ausführen. Im Abschnitt General information (Allgemeine Informationen) wird Folgendes angezeigt:

- Workgroup (Arbeitsgruppe) – Der Name der Arbeitsgruppe.

- Namespace – Der Namespace, der der Arbeitsgruppe zugeordnet ist. Sie können die Option auswählen, um sich die entsprechenden Eigenschaften anzeigen zu lassen. Eine Arbeitsgruppe ist einem einzelnen Namespace zugeordnet.
- Date created (Erstellungsdatum) – Der Zeitpunkt, an dem die Arbeitsgruppe erstellt wurde.
- Status – Gibt an, ob die Arbeitsgruppenressourcen verfügbar sind. Wenn sie verfügbar sind, können Sie sich über einen Client mit der Amazon-Redshift-Serverless-Instance verbinden, um Daten abzufragen oder Datenbankressourcen zu erstellen, oder Sie können eine Verbindung mit dem Abfrage-Editor v2 herstellen.
- Endpoint (Endpunkt) – Die URL.
- JDBC URL (JDBC–URL) – Die URL zum Herstellen von JDBC-Clientverbindungen. Sie können diese URL verwenden, um eine Verbindung mit einem JDBC-Treiber für Amazon Redshift herzustellen. Weitere Informationen finden Sie unter Konfigurieren einer Verbindung für JDBC-Treiberversion 2.1 für Amazon Redshift.
- ODBC URL (ODBC–URL) – Die URL zum Herstellen von ODBC-Clientverbindungen. Hier sind Eigenschaften wie Datenbank und Benutzer-ID sowie ihre Werte enthalten.
- Arbeitsgruppenversion und Patch-Version – Amazon Redshift Serverless veröffentlicht regelmäßig neue Versionen und Patches. Sie können mit den Arbeitsgruppenversions- und Patch-Versionsnummern Softwareupdates für Ihre Amazon-Redshift-Serverless-Arbeitsgruppe nachverfolgen. Weitere Informationen zu Änderungen und Funktionen in bestimmten Patches finden Sie unter Cluster-Versionen für Amazon Redshift.

Die Registerkarte Data access (Datenzugriff) enthält mehrere Bereiche:

- Network and security (Netzwerk und Sicherheit) – Sie können Netzwerkeigenschaften sehen, wie zum Beispiel den Bezeichner Virtual Private Cloud (VPC), die Liste VPC Security Group ((VPC-Sicherheitsgruppe), Enhanced VPC routing (Erweitertes VPC-Routing) und die Einstellung Publicly accessible (Öffentlich zugänglich). Wenn Sie Edit (Bearbeiten) auswählen, können Sie diese Einstellungen ändern. Darüber hinaus können Sie Turn on enhanced VPC Routing (Erweitertes VPC-Routing aktivieren) auswählen. Mit dieser Einstellung wird der Netzwerkverkehr zwischen Ihrer Serverless-Datenbank und Datenrepositorys über eine VPC weitergeleitet, um den Datenschutz und die Sicherheit zu erhöhen. Sie können auch Turn on Public Accessible (Öffentliche Zugänglichkeit aktivieren), wodurch die Datenbank von außerhalb der VPC öffentlich zugänglich ist, sodass Instances und Geräte eine Verbindung herstellen können.

- Redshift managed VPC endpoints (Von Redshift verwaltete VPC-Endpunkte) – Sie können verwaltete VPC-Endpunkte erstellen, um von einer anderen VPC aus auf Amazon Redshift Serverless zuzugreifen.

Die Registerkarte Limits enthält Einstellungen zur Kontrolle von Kapazitäts- und Nutzungslimits für Amazon Redshift Serverless. Sie umfasst die folgenden Bereiche:

- Base capacity in Redshift processing units (RPUs) (Basiskapazität in Redshift Processing Units (RPUs)) – Sie können die Basiskapazität der Rechenressourcen festlegen, die zur Verarbeitung Ihrer Workload verwendet werden. Weitere Informationen finden Sie unter Grundlegendes zur Amazon-Redshift-Serverless-Kapazität.
- Nutzungslimits – Sie können bis zu vier Limits für die maximale Zahl von Rechenressourcen einrichten, die Ihre Amazon-Redshift-Serverless-Instance in einem bestimmten Zeitraum verwenden kann. Außerdem können Sie Aktionen auswählen, die Amazon Redshift Serverless ausführen soll, wenn diese Limits erreicht werden. Beispielsweise können Sie für Ihre Arbeitsgruppe zwei Limits festlegen, ein Limit von 500 RPU-Stunden und ein Limit von 900 RPU-Stunden. Sie können Amazon Redshift Serverless eine Warnung senden lassen, wenn das erste Limit von 500 RPU-Stunden erreicht wird, und Benutzerabfragen deaktivieren lassen, wenn das zweite Limit von 900 Stunden erreicht ist. Diese Limits helfen Ihnen, die Kosten zu kontrollieren und planbarer zu machen.
- Query limits (Abfragelimits) – Sie können Grenzwerte für Abfragen festlegen, z. B. die Einstellung für eine Zeitüberschreitung. Diese Grenzwerte helfen Ihnen, Kosten und Leistung zu optimieren.

Auf der Registerkarte Registerkarten finden Sie den Bereich Tags mit allen Tags, die Sie für Ihre Arbeitsgruppe erstellt haben. Weitere Informationen über das Markieren von -Ressourcen mit Tags finden Sie unter Markieren von Ressourcen – Übersicht.

Löschen von Arbeitsgruppen

Sie können eine Arbeitsgruppe über die Konsole löschen. Stellen Sie zuvor sicher, dass Ihre Daten gesichert und Snapshots vorhanden sind. Ressourcen, die als Teil der Arbeitsgruppe gelöscht wurden, können in vielen Fällen nicht abgerufen werden.

Führen Sie folgende Schritte aus:

1. Klicken Sie auf Amazon Redshift Serverless, wählen Sie Workgroup configuration (Arbeitsgruppenkonfiguration) und Delete Amazon Redshift Serverless instance (Amazon-Redshift-Serverless-Instance löschen) aus.

2. Ein Dialogfeld wird geöffnet. Wenn Sie die Arbeitsgruppe löschen möchten, werden alle Nutzungslimits aufgehoben, alle VPC-Endpunkte werden entfernt und der Zugriff auf VPC-Endpunkte wird deaktiviert.

   Geben Sie delete (löschen) ein und wählen Sie zur Bestätigung Delete (Löschen) aus.

Nachdem Sie die Schritte abgeschlossen haben, lautet der Status der Arbeitsgruppe Deleting (Wird gelöscht) und das Banner zeigt an, dass die Arbeitsgruppe gelöscht wird. Während der Löschvorgang läuft, werden einige Funktionen unter dem Serverless Dashboard deaktiviert. Sie können jedoch bereitgestellte Cluster im Provisioned clusters dashboard (Dashboard für bereitgestellte Cluster) konfigurieren.

Nachdem Sie die Arbeitsgruppe gelöscht haben, wird sie nicht mehr mit dem Namespace angezeigt. Sie können die Schaltfläche Create workgroup (Arbeitsgruppe erstellen) auswählen, um eine neue Arbeitsgruppe zu erstellen.

Sie können eine vorhandene Arbeitsgruppe löschen und eine neue Arbeitsgruppe mit einer anderen Konfiguration mit demselben Namespace verknüpfen. Wählen Sie beim Erstellen der neuen Arbeitsgruppe die Basiskapazität aus, die für die Größe der Daten funktioniert, die mit dem Namespace verknüpft sind.

Sie können eine Arbeitsgruppe mit einem Namespace verknüpfen, der mit einem vom Kunden verwalteten Schlüssel (CMK) erstellt wurde. Weitere Informationen zu finden Sie unter Konzepte AWS KMS.AWS KMS

Arbeiten mit Namespaces

In Amazon Redshift Serverless definiert ein Namespace einen logischen Container für Datenbankobjekte. Es kann Tabellen, Arbeitsgruppen und andere Datenbankressourcen enthalten. Wenn Sie noch keine Arbeitsgruppe und keinen Namespace erstellt haben und nach Anleitungen zu den ersten Schritten mit Amazon Redshift Serverless suchen, informieren Sie sich unter Ersteinrichtung von Amazon Redshift Serverless.

Suchen nach einem Namespace

Im Menü von Amazon Redshift können Sie einen Namespace aus der Liste Namespaces auswählen, um die Eigenschaften für diesen Namespace anzuzeigen oder zu bearbeiten. Zu den Informationen in der Konsole gehören der Namespace-Name, der Administratorname und andere Eigenschaften.

Die Einstellungen und Eigenschaften eines Namespace befinden sich auf verschiedenen Registerkarten. Diese umfassen u. a. folgende:

- Workgroup (Arbeitsgruppe) – Zeigt Arbeitsgruppen an, die mit dem Namespace verknüpft sind.
- Data back up (Datensicherung) – Sie können Snapshots konfigurieren und erstellen und Wiederherstellungspunkte konfigurieren.
- Security and encryption (Sicherheit und Verschlüsselung) – Sie können IAM-Rollenberechtigungen verwalten und Ihre Sicherheits- und Verschlüsselungseinstellungen anzeigen oder bearbeiten. Dazu gehören Ihr Verschlüsselungsschlüsselstatus und Ihre Einstellungen für die Audit-Protokollierung.
- Datashares – Zeigt Datashares an.

Eigenschaften von Namespaces

In Amazon Redshift Serverless definiert ein Namespace einen Container für Datenbankobjekte. Sie können Namespace configuration (Namespace configuration) aus der Navigationsliste und einen Namespace aus der Liste auswählen und die Einstellungen bearbeiten.

Die allgemeinen Informationen für den Namespace umfassen Folgendes:

- Namespace – Der Name.
- Namespace ID (Namespace-ID) – Eindeutiger Bezeichner.
- ARN — Ein eindeutiger Bezeichner, der verwendet wird, um die Ressource übergreifend zu spezifizieren AWS. Sie enthält Eigenschaften wie die Region und den Service.
- Status – Der Status, z. B. Available (Verfügbar).
- Date created (Erstellungsdatum) – Das Datum, an dem der Namespace erstellt wurde.
- Storage used (Verwendeter Speicher) – Der vom Namespace und allen seinen Objekten belegte Speicherplatz.
- Admin user name (Administratorname) – Das Administratorkonto. Dies ist normalerweise das Konto, das zum Erstellen des Namespace verwendet wird.

- Database name (Datenbankname) – Der Name der Datenbank, die im Namespace enthalten ist.
- Total table count (Gesamte Tabellenanzahl) – Die Anzahl der Tabellen in allen Schemas.

Weitere Einstellungen und Eigenschaften für den Namespace befinden sich auf verschiedenen Registerkarten. Diese umfassen u. a. folgende:

- Workgroup (Arbeitsgruppe) – Zeigt die Arbeitsgruppe an, die mit dem Namespace verknüpft ist.
- Data back up (Datensicherung) – In diesem Bereich können Sie Snapshots konfigurieren und erstellen und Wiederherstellungspunkte konfigurieren.
- Security and encryption (Sicherheit und Verschlüsselung) – Sie können IAM-Rollenberechtigungen verwalten und Ihre Sicherheits- und Verschlüsselungseinstellungen anzeigen oder bearbeiten. Dazu gehören der Status Ihres Verschlüsselungsschlüssels und die Einstellung zum Aktivieren der Audit-Protokollierung. Weitere Informationen zur Audit-Protokollierung für Amazon Redshift Serverless finden Sie unter Audit-Protokollierung für Amazon Redshift Serverless.
- Datashares – Zeigt Datashares an. Mit der Datenfreigabe können Sie Zugriff auf Daten gewähren, ohne diese kopieren oder verschieben zu müssen. Weitere Informationen zur Datenfreigabe finden Sie unter Datenfreigabe in Amazon Redshift Serverless.

Bearbeiten der Sicherheit und Verschlüsselung

Amazon Redshift Serverless ist durch KMS-Verschlüsselung gesichert. Sie können die Verschlüsselungseinstellungen über die Konsole aktualisieren:

1. Klicken Sie im Hauptmenü der Konsole auf Namespace configuration (Namespace-Konfiguration). Wählen Sie den zu bearbeitenden Namespace und dann Edit (Bearbeiten) auf der Registerkarte Security and encryption (Sicherheit und Verschlüsselung) aus. Es wird ein Dialogfeld angezeigt.
2. Sie können „Verschlüsselungseinstellungen anpassen“ und dann „Vom AWS Kunden verwalteten Schlüssel auswählen“ auswählen, um den für die Verschlüsselung Ihrer Ressourcen verwendeten Schlüssel zu ändern.
3. Wählen Sie unter Audit logging (Prüfungsprotokollierung) die Protokolle aus, die exportiert werden sollen. Jeder Protokolltyp gibt verschiedene Metadaten an.
4. Wählen Sie Save changes (Änderungen speichern) aus, um das Konfigurationsupdate abzuschließen.

Den AWS KMS Schlüssel für einen Namespace ändern

In Amazon Redshift wird Data-at-Rest durch Verschlüsselung geschützt. Amazon Redshift Serverless verwendet automatisch die AWS KMS Schlüsselverschlüsselung, um sowohl Ihre Amazon Redshift Serverless-Ressourcen als auch Ihre Snapshots zu verschlüsseln. Als bewährte Methode überprüfen die meisten Organisationen die Art der Daten, die sie speichern, und verfügen über einen Plan zum Rotieren von Verschlüsselungsschlüsseln nach einem Zeitplan. Die Häufigkeit für das Rotieren von Schlüsseln kann abhängig von Ihren Richtlinien zur Datensicherheit variieren. Amazon Redshift Serverless unterstützt das Ändern des AWS KMS Schlüssels für den Namespace, sodass Sie die Sicherheitsrichtlinien Ihres Unternehmens einhalten können.

Wenn Sie den AWS KMS Schlüssel ändern, bleiben die Daten unverändert.

Ändern eines AWS KMS Schlüssels mithilfe der Konsole

In Amazon Redshift wird Data-at-Rest durch Verschlüsselung geschützt. Amazon Redshift Serverless verwendet automatisch AWS KMS Schlüsselverschlüsselung, um sowohl Amazon Redshift Serverless als auch Snapshots zu verschlüsseln. Als bewährte Methode überprüfen die meisten Organisationen die Art der Daten, die sie speichern, und verfügen über einen Plan zum Rotieren von Verschlüsselungsschlüsseln nach einem Zeitplan. Die Häufigkeit für das Rotieren von Schlüsseln kann abhängig von Ihren Richtlinien zur Datensicherheit variieren. Amazon Redshift Serverless unterstützt das Ändern des AWS KMS Schlüssels für den Namespace, sodass Sie die Sicherheitsrichtlinien Ihres Unternehmens einhalten können.

Wenn Sie den AWS KMS Schlüssel ändern, bleiben die Daten unverändert.

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Namespace configuration (Namespace-Konfiguration) aus. Wählen Sie Ihren Namespace aus der Liste aus.
3. Wählen Sie auf der Registerkarte Security and encryption (Sicherheit und Verschlüsselung) die Option Edit (Bearbeiten) aus.
4. Klicken Sie auf Customize encryption settings (Verschlüsselungseinstellungen anpassen) und wählen Sie einen Schlüssel für den Namespace aus. Optional können Sie einen neuen Schlüssel erstellen.

Ändern von AWS KMS Verschlüsselungsschlüsseln mit dem AWS CLI

Wird verwendet`update-namespace`, um den AWS KMS Schlüssel für den Namespace zu ändern. Nachfolgend finden Sie die allgemeine Syntax für den Befehl:

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

Sie müssen einen Namespace erstellt haben, sonst führt der CLI-Befehl zu einem Fehler.

Die benötigte Zeit zum Ändern des Schlüssels hängt von der Datenmenge in Amazon Redshift Serverless ab. Die Dauer beträgt normalerweise fünfzehn Minuten pro 8 TB gespeicherter Daten.

Einschränkungen

Sie können nicht von einem vom Kunden verwalteten KMS-Schlüssel zu einem AWS KMS Schlüssel wechseln. In diesem Fall müssen Sie einen neuen Namespace erstellen.

Sie können keine anderen Aktionen ausführen, während der Schlüssel geändert wird.

Löschen von Namespaces

Wenn Sie einen Namespace mit einer zugeordneten Arbeitsgruppe löschen möchten, müssen Sie zuerst die Arbeitsgruppe löschen.

Führen Sie in der Amazon-Redshift-Serverless-Konsole die folgenden Schritte aus:

1. Wählen Sie Namespace configuration (Namespace-Konfiguration) im linken Menü und dann den zu Namespace aus der Liste aus, den Sie löschen möchten.
2. Wählen Sie Actions (Aktionen) und anschließend Delete namespace (Namespace löschen) aus.
3. Es öffnet sich ein Dialogfeld. Sie können Ihre Daten beibehalten, indem Sie vor Abschluss des Löschvorgangs einen manuellen Snapshot erstellen.

   Geben Sie delete (löschen) ein und wählen Sie zur Bestätigung Delete (Löschen) aus.

Verwalten von Nutzungs- und Abfragelimits und andere administrative Aufgaben

Sie können Einstellungen in der Konsole konfigurieren, um die Nutzung zu kontrollieren und die Kosten zu begrenzen.

Verwalten von Nutzungslimits, einschließlich des Festlegens von RPU-Limits

Auf der Registerkarte Limits für eine Arbeitsgruppe können Sie ein oder mehrere Nutzungslimits hinzufügen, um die maximalen RPUs zu steuern, die Sie in einem bestimmten Zeitraum verwenden, oder um ein Nutzungslimit für die Datenfreigabe festzulegen.

1. Wählen Sie Manage usage limits (Nutzungslimits verwalten) aus. Der Abschnitt für die Limits wird unten im Bereich Rechenressourcennutzung nach Zeitraum angezeigt.
2. Legen Sie ein Nutzungslimit in RPU-Stunden fest.
3. Wählen Sie einen Wert für Häufigkeit aus. Dies kann Täglich, Wöchentlich oder Monatlich sein. Damit wird der Zeitraum für das Nutzungslimit festgelegt. Die Einstellung Daily (Täglich) verleiht Ihnen in diesem Fall mehr Kontrolle.
4. Legen Sie ein Nutzungslimit in Stunden fest.
5. Legen Sie die Option fest. Zur Verfügung stehen folgende Optionen:

   - Log to system table (In Systemtabelle protokollieren) – Fügt einer Systemtabelle einen Datensatz hinzu, den Sie abfragen können, um festzustellen, ob das Limit überschritten wird.
   - Alert (Warnung) – Verwendet Amazon SNS, um Benachrichtigungsabonnements einzurichten und Benachrichtigungen zu senden, wenn ein Limit überschritten wird. Sie können ein vorhandenes SNS-Thema auswählen oder ein neues Thema erstellen.
   - Turn off user queries (Benutzerabfragen deaktivieren) – Deaktiviert Abfragen, um die Verwendung von Amazon Redshift Serverless zu beenden. Außerdem wird eine Benachrichtigung gesendet.

   Die ersten beiden Aktionen sind informativ, während mit der letzten die Abfrageverarbeitung deaktiviert wird.
6. Optional können Sie einen Wert für Cross-Region data sharing usage limit (Nutzungslimit für regionsübergreifende Datenfreigabe) festlegen, der beschränkt, wie viele Daten, die von der Erzeugerregion an Verbraucherregion übertragen werden, von Verbrauchen abgefragt werden können. Wählen Sie dazu Add limit (Limit hinzufügen) aus und befolgen Sie die Schritte.

7. Wählen Sie unten auf der Seite Änderungen speichern aus, um das Limit zu speichern.
8. Sie können bis zu 3 weitere Limits wie notwendig einrichten.

Weitere konzeptuelle Informationen zu RPUs und zur Fakturierung finden Sie unter Fakturierung für Amazon Redshift Serverless.

Verwalten von Abfragelimits

Auf der Registerkarte Limits für eine Arbeitsgruppe können Sie einen Grenzwert zur Überwachung der Leistung und Limits hinzufügen. Weitere Informationen zu Limits für die Abfrageüberwachung finden Sie unter WLM-Abfrageüberwachungsregeln.

1. Wählen Sie Manage query limits (Abfragelimits verwalten) aus. Klicken Sie auf Add new limit (Neues Limit hinzufügen) im Dialogfeld Manage query limits (Abfragelimits verwalten).
2. Wählen Sie den Limittyp, den Sie festlegen möchten, und geben Sie einen Wert für das entsprechende Limit ein.
3. Wählen Sie zum Speichern des Limits Save Changes (Änderungen speichern) aus.

Wenn Sie Ihr Abfragelimit und Ihre Konfigurationsparameter ändern, wird Ihre Datenbank neu gestartet.

Filtern von Abfragen

Sie können die im Serverless-Dashboard verfügbaren Filter verwenden. Führen Sie zum Filtern von Abfragen die folgenden Schritte aus.

1. Wählen Sie die Dropdown-Liste auf der linken Seite des Bereichs Query summary (Abfrage-Übersicht) aus, um nach abgeschlossenen Abfragen, fehlgeschlagenen Abfragen oder beidem zu filtern.
2. Wählen Sie die Dropdown-Liste auf der rechten Seite des Bereichs Query summary (Abfrage-Übersicht) aus, um nach laufenden Abfragen, Abfragen in Warteschlangen oder beidem zu filtern.

Ändern des Administratorpassworts

1. Wählen Sie Namespace configuration (Namespace-Konfiguration) aus. Klicken Sie dann auf Change admin password (Administratorpasswort ändern). Es wird ein Dialogfeld angezeigt.

2. Sie können Angaben unter New admin username (Neuer Administratorbenutzername) und New admin user password (Neues Administratorbenutzerpasswort) vornehmen.
3. Wählen Sie Save (Speichern) aus.

Überprüfen der Gesamtdaten von Amazon Redshift Serverless über das Dashboard

Das Amazon Redshift Serverless Dashboard enthält eine Sammlung von Panels, in denen at-a-glance Metriken und Informationen zu Ihrer Arbeitsgruppe und Ihrem Namespace angezeigt werden. Diese Bereiche umfassen u. a.:

- Resources summary (Ressourcen-Übersicht) – Zeigt allgemeine Informationen über Amazon Redshift Serverless an, z. B. den verwendeten Speicher und andere Metriken.
- Query summary (Abfrage-Übersicht) – Zeigt Informationen zu Abfragen an, einschließlich abgeschlossener und laufender Abfragen. Klicken Sie auf View details (Details anzeigen), um zu einem Bildschirm mit zusätzlichen Filtern zu wechseln.
- RPU capacity used (Genutzte RPU-Kapazität) – Zeigt die Gesamtkapazität an, die in einem bestimmten Zeitraum, beispielsweise in den letzten zehn Stunden, genutzt wurde.
- Datashares – Zeigt die Anzahl der Datashares an, die für den Austausch von Daten, beispielsweise zwischen AWS -Konten, verwendet werden. Die Metriken zeigen unter anderem an, welche Datashares eine Autorisierung erfordern.
- Gesamte Rechenressourcennutzung – Zeigt die gesamten verbrauchten RPU-Stunden für die ausgewählte Arbeitsgruppe über einen ausgewählten Zeitbereich an (maximal die letzten 7 Tage).

Über das Dashboard können Sie diese verfügbaren Metriken schnell einsehen, um Details zu Amazon Redshift Serverless oder Abfragen zu überprüfen oder Arbeitselemente nachzuverfolgen.

Überwachen von Abfragen und Workloads mit Amazon Redshift Serverless

Überwachen von Abfragen und Workloads mit Amazon Redshift Serverless

Sie können Ihre Amazon-Redshift-Serverless-Abfragen und Ihre Workload mit den bereitgestellten Systemansichten überwachen.

Gewähren des Zugriffs auf Monitorabfragen

Ein Superuser kann Benutzern, die keine Superuser sind, Zugriff gewähren, damit sie eine Abfrageüberwachung für alle Benutzer durchführen können. Zuerst fügen Sie eine Richtlinie für einen Benutzer oder eine Rolle hinzu, um den Zugriff auf die Abfrageüberwachung zu gewähren. Anschließend erteilen Sie dem Benutzer oder der Rolle die Berechtigung zur Abfrageüberwachung.

So fügen Sie die Richtlinie zur Abfrageüberwachung hinzu

1. Wählen Sie https://console.aws.amazon.com/iam/ aus.
2. Wählen Sie unter Access management (Zugriffsverwaltung) Policies (Richtlinien) aus.
3. Wählen Sie Create Policy (Richtlinie erstellen) aus.
4. Wählen Sie JSON aus und fügen Sie die folgende Richtliniendefinition ein.

```
{
"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. Wählen Sie Review policy(Richtlinie prüfen).
6. Geben Sie unter Name einen Namen für die Richtlinie ein, z. B. `query-monitoring`.
7. Wählen Sie Richtlinie erstellen aus.

Nachdem Sie die Richtlinie erstellt haben, können Sie die entsprechenden Berechtigungen erteilen.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in: AWS IAM Identity Center

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

So erteilen Sie einem Benutzer die Berechtigung zur Abfrageüberwachung

Benutzer mit `sys:monitor`-Berechtigung können alle Abfragen anzeigen. Darüber hinaus können Benutzer mit `sys:operator`-Berechtigung Abfragen abbrechen, den Abfrageverlauf analysieren und Vakuumvorgänge ausführen.

1. Geben Sie den folgenden Befehl ein, um Systemüberwachungszugriff bereitzustellen, wobei user-name der Name des Benutzers ist, dem Sie Zugriff gewähren möchten.

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

2. (Optional) Geben Sie den folgenden Befehl ein, um Systemoperatorzugriff bereitzustellen, wobei user-name der Name des Benutzers ist, dem Sie Zugriff gewähren möchten.

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

So erteilen Sie Berechtigung zur Abfrageüberwachung für eine Rolle

Benutzer mit einer Rolle mit `sys:monitor`-Berechtigungen können alle Abfragen anzeigen. Darüber hinaus können Benutzer mit einer Rolle, die `sys:operator`-Berechtigung hat, Abfragen abbrechen, den Abfrageverlauf analysieren und Vakuumvorgänge ausführen.

1. Geben Sie den folgenden Befehl ein, um Systemüberwachungszugriff bereitzustellen, wobei role-name der Name der Rolle ist, für die Sie Zugriff gewähren möchten.

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

2. (Optional) Geben Sie den folgenden Befehl ein, um Systemoperatorzugriff bereitzustellen, wobei role-name der Name der Rolle ist, für die Sie Zugriff gewähren möchten.

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

Überwachungsansichten

Überwachungsansichten sind Systemansichten in Amazon Redshift Serverless, die zur Überwachung der Abfrage- und Workload-Nutzung verwendet werden. Diese Ansichten befinden sich im `pg_catalog`-Schema Die verfügbaren Systemansichten wurden entwickelt, um Ihnen die Informationen zu liefern, die zur Überwachung von Amazon Redshift Serverless erforderlich sind, was viel einfacher ist als für bereitgestellte Cluster. Die SYS-Systemansichten sind mit Amazon Redshift Serverless kompatibel. Um die von diesen Ansichten bereitgestellten Informationen anzuzeigen, führen Sie SQL SELECT-Anweisungen aus.

Systemansichten werden definiert, um die folgenden Überwachungsziele zu unterstützen.

Workload-Überwachung

Sie können Ihre Abfrageaktivitäten im Laufe der Zeit überwachen, um Folgendes zu erreichen:

- Nachvollziehen von Workload-Mustern, um den Normalzustand (Baseline) und den Umfang geschäftlicher Service Level Agreements (SLAs) zu ermitteln.
- Schnelles Erkennen von Anomalien, bei denen es sich um gewöhnliche Fluktuationen oder ernsthafte Probleme handeln kann, die behoben werden müssen.

Überwachen von Datenladungen und -entladungen

Die Datenübertragung in und aus Amazon Redshift Serverless ist eine kritische Funktion. Sie verwenden COPY und UNLOAD zum Laden oder Entladen von Daten und Sie müssen den

Fortschritt in Bezug auf übertragene Byte/Zeilen und abgeschlossene Dateien genau überwachen, um die Einhaltung von Geschäfts-SLAs nachzuverfolgen. Dies geschieht normalerweise durch häufige (d. h. minütliche) Abfragen von Systemtabellen, um den Fortschritt zu verfolgen und Warnungen für Untersuchung/Korrekturmaßnahmen auszulösen, wenn signifikante Abweichungen festgestellt werden.

Fehler- und Problemdiagnose

Es gibt Fälle, in denen Sie Maßnahmen für Abfrage- oder Laufzeitfehler ergreifen müssen. Entwickler nutzen Systemtabellen, um Probleme selbst zu diagnostizieren und richtige Abhilfemaßnahmen zu ermitteln.

Leistungsoptimierung

Möglicherweise müssen Sie Abfragen optimieren, die die SLA-Anforderungen von Anfang an nicht erfüllen oder sich im Laufe der Zeit verschlechtert haben. Zur Optimierung benötigen Sie Laufzeitdetails wie Ausführungsplan, Statistiken, Dauer und Ressourcenverbrauch. Sie benötigen Basisdaten für fehlerhafte Abfragen, um die Ursache für Abweichungen zu ermitteln und eine Orientierungshilfe für Verbesserung zu erhalten.

Ereignisüberwachung von Benutzerobjekten

Sie müssen Aktionen und Aktivitäten für Benutzerobjekte wie das Aktualisieren materialisierter Ansichten, Bereinigen und Analysieren überwachen. Dies schließt systemverwaltete Ereignisse wie die automatische Aktualisierung für materialisierte Ansichten ein. Sie müssen überwachen, wann ein Ereignis endet, ob es vom Benutzer initiiert wurde, oder wann der letzte erfolgreiche Lauf erfolgte, wenn das System initiiert wurde.

Nutzungsverfolgung für die Abrechnung

Sie können Ihre Nutzungstrends im Laufe der Zeit überwachen, um Folgendes zu erreichen:

- Informationen für die Budgetplanung und Schätzung von Geschäftskosten.
- Erkennen von potenziellen Kosteneinsparungen wie das Entfernen kalter Daten.

Sie können Amazon Redshift Serverless über die folgenden SYS-Systemansichten überwachen. Weitere Informationen zu den SYS-Überwachungsansichten finden Sie unter SYS-Überwachungsansichten.

Prüfungsprotokollierung für Amazon Redshift Serverless

Exportieren von Protokollen

Sie können Amazon Redshift Serverless so konfigurieren, dass Verbindungs-, Benutzer- und Benutzeraktivitätsprotokolldaten in eine Protokollgruppe in Amazon Logs exportiert werden. CloudWatch Mit Amazon CloudWatch Logs können Sie die Protokolldaten in Echtzeit analysieren und CloudWatch zur Erstellung von Alarmen und zum Anzeigen von Metriken verwenden. Sie können CloudWatch Logs verwenden, um Ihre Protokolldatensätze auf einem dauerhaften Speicher zu speichern.

Mit der Amazon Redshift Redshift-Konsole können Sie CloudWatch Alarme erstellen, um Ihre Metriken zu verfolgen. Weitere Informationen zum Erstellen von Alarmen finden Sie unter Verwalten von Alarmen.

Um generierte Protokolldaten nach Amazon CloudWatch Logs zu exportieren, müssen die entsprechenden Protokolle in Ihren Amazon Redshift Serverless-Konfigurationseinstellungen auf der Konsole für den Export ausgewählt werden. Sie können dies tun, indem Sie die Einstellungen zu Namespace-Konfiguration unter Sicherheit und Verschlüsselung auswählen.

Überwachung von Protokollereignissen in CloudWatch

Nachdem Sie ausgewählt haben, welche Redshift-Protokolle exportiert werden sollen, können Sie Ereignisse in Amazon CloudWatch Logs überwachen. Es wird automatisch eine neue Protokollgruppe für Amazon Redshift Serverless erstellt, in der `log_type` für den Protokolltyp steht.

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

Wenn Sie Ihre erste Arbeitsgruppe und Ihren ersten Namespace erstellen, ist default der Namespace-Name. Der Name der Protokollgruppe variiert je nachdem, wie Sie den Namespace benennen.

Wenn Sie beispielsweise das Verbindungsprotokoll exportieren, werden die Protokolldaten in der folgenden Protokollgruppe gespeichert.

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

Protokollereignisse werden mithilfe des Serverless-Protokollstreams in eine Protokollgruppe exportiert. Das Verhalten hängt davon ab, welche der folgenden Bedingungen zutrifft:

- Eine Protokollgruppe mit dem angegebenen Namen existiert. Redshift exportiert Protokolldaten unter Verwendung der vorhandenen Protokollgruppe. Um Protokollgruppen mit vordefinierten Aufbewahrungsfristen für Protokolle, Metrikfiltern und Kundenzugriff zu erstellen, können Sie eine automatisierte Konfiguration verwenden, wie sie beispielsweise von bereitgestellt wird. AWS CloudFormation
- Eine Protokollgruppe mit dem angegebenen Namen existiert nicht. Wenn im Protokoll für die Instance ein passender Protokolleintrag erkannt wird, erstellt Amazon Redshift Serverless automatisch eine neue Protokollgruppe in Amazon CloudWatch Logs. Die Protokollgruppe nutzt den standardmäßigen Aufbewahrungszeitraum für Protokolle Never Expire (Läuft nie ab). Um den Aufbewahrungszeitraum für Protokolle zu ändern, verwenden Sie die Amazon CloudWatch Logs-Konsole AWS CLI, die oder die Amazon CloudWatch Logs-API. Weitere Informationen zur Änderung der Aufbewahrungsfristen für CloudWatch Protokolle finden Sie unter Ändern der Aufbewahrung von Protokolldaten in Arbeiten mit Protokollgruppen und Protokollströmen.

Verwenden Sie die Amazon CloudWatch Logs-Konsole, die oder die Amazon Logs-API, um nach Informationen in CloudWatch Protokollereignissen zu suchen. AWS CLI Weitere Informationen finden Sie unter Suchen und Filtern von Protokolldaten.

Metriken für Amazon Redshift Serverless

Metriken sind bei Amazon Redshift Serverless in Rechenmetriken sowie Daten- und Speichermetriken unterteilt, die unter die Arbeitsgruppen- bzw. Namespace-Dimensionssätze fallen. Weitere Informationen zu Arbeitsgruppen und Namespaces finden Sie unter Übersicht über Amazon-Redshift-Serverless-Arbeitsgruppen und -Namespaces.

CloudWatch Die Berechnungsmetriken lauten wie folgt:

CloudWatch Metriken berechnen

Metrikname	Einheiten	Beschreibung	Dimensionssätze
`QueriesCompletedPerSecond`	Anzahl der Abfragen	Die Anzahl der pro Sekunde abgeschlossenen Abfragen.	{Datenbank LatencyRange, Arbeitsgruppe}, {LatencyRange, Arbeitsgruppe}
`QueryDuration`	Mikrosekunden	Die durchschnittliche Zeit, die	{Datenbank, LatencyRange,

Metrikname	Einheiten	Beschreibung	Dimensionssätze
		es dauert, bis eine Abfrage ausgeführt wurde.	Arbeitsgruppe}, {LatencyRange, Arbeitsgruppe}
QueriesRunning	Anzahl der Abfragen	Die Anzahl der zu einem bestimmte n Zeitpunkt ausgeführten Abfragen.	{Datenbank, QueryType, Arbeitsgruppe}, {QueryType, Arbeitsgruppe}
QueriesQueued	Anzahl der Abfragen	Die Anzahl der Abfragen in der Warteschl ange zu einem bestimmten Zeitpunkt.	{Datenbank, QueryType, Arbeitsgruppe}, {QueryType, Arbeitsgruppe}
DatabaseConnections	Anzahl der Verbindungen	Die Anzahl der Verbindun gen zu einer Datenbank zu einem bestimmten Zeitpunkt.	{Database, Workgroup}, {Workgroup}
QueryRuntimeBreakdown	Millisekunden	Die Gesamtzeit, in der Abfragen ausgeführt wurden, nach Abfragephase.	{Database, Stage, Workgroup}, {Stage, Workgroup}

Metrikname	Einheiten	Beschreibung	Dimensionssätze
ComputeCapacity	RPU	Durchschnittliche Anzahl der Computing einheiten, die in den letzten 30 Minuten zugewiesen wurden, auf die nächste ganze Zahl aufgerundet.	{Workgroup}
ComputeSeconds	RPU-Sekunden	In den letzten 30 Minuten verbrauchte kumulierte Computing einheiten in Sekunden.	{Workgroup}
QueriesSucceeded	Anzahl der Abfragen	Die Anzahl der Abfragen, die in den letzten 5 Minuten erfolgreich waren.	{Datenbank, QueryType, Arbeitsgruppe}, {QueryType, Arbeitsgruppe}
QueriesFailed	Anzahl der Abfragen	Die Anzahl der Abfragen, die in den letzten 5 Minuten fehlgeschlagen sind.	{Datenbank, QueryType, Arbeitsgruppe}, {QueryType, Arbeitsgruppe}

Metrikname	Einheiten	Beschreibung	Dimensionssätze
`UsageLimitAvailable`	RPU-Stunden oder TBs	Gibt je nach UsageType Folgendes UsageLimitAvailable zurück: • Wenn SERVERLESS_COMPUTE UsageType ist, wird die verbleibende Anzahl von RPU-Stunden UsageLimitAvailable zurückgegeben, die die Arbeitsgruppe innerhalb des angegebenen Grenzwerts abfragen kann. • Wenn CROSS_REGION_DATASHARING UsageType ist, wird die verbleibende Anzahl von TB UsageLimitAvailable	{,, Arbeitsgruppe} UsageLimitId UsageType

Metrikname	Einheiten	Beschreibung	Dimensionssätze
		zurückgegeben, die der Kunde innerhalb des angegebenen Limits scannen kann.	

Metrikname	Einheiten	Beschreibung	Dimensionssätze
`UsageLimitConsumed`	RPU-Stunden oder TBs	Gibt je nach UsageType , Folgendes UsageLimitConsumed zurück: • Wenn SERVERLESS_COMPUTE UsageType ist, wird die Anzahl der RPU-Stunden UsageLimitConsumed zurückgegeben, die die Arbeitsgruppe innerhalb des angegebenen Grenzwerts bereits abgefragt hat. • Wenn CROSS_REGION_DATASHARING UsageType ist, wird die Anzahl der TB UsageLimitConsumed zurückgegeben, die der	{,, Arbeitsgruppe} UsageLimitId UsageType

Metrikname	Einheiten	Beschreibung	Dimensionssätze
		Kunde im angegebenen Limit bereits zum Scannen verwendet hat.	

CloudWatch Die Daten- und Speichermetriken lauten wie folgt:

CloudWatch Daten- und Speichermetriken

Metrikname	Einheiten	Beschreibung	Dimensionssätze
`TotalTableCount`	Anzahl der Tabellen	Die Anzahl der zu einem bestimmten Zeitpunkt vorhandenen Benutzertabellen. Diese Summe enthält keine Amazon-Redshift-Spectrum-Tabellen.	{Database, Namespace}
`DataStorage`	Megabyte	Die Anzahl der für Redshift-Daten verwendeten Megabyte im Festplatten- oder Arbeitsspeicher.	{Namespace}

Die SnapshotStorage Metrik ist namespace- und arbeitsgruppenunabhängig. CloudWatchDie Metrik lautet wie folgt: SnapshotStorage

CloudWatch SnapshotStorage metrisch

Metrikname	Einheiten	Beschreibung	Dimensionssätze
SnapshotStorage	Megabyte	Die Anzahl der für Snapshots verwendeten Megabyte im Festplatten- oder Arbeitsspeicher.	{}

Dimensionssätze sind die Gruppierungsdimensionen, die auf Ihre Metriken angewendet werden. Sie können diese Dimensionsgruppen verwenden, um anzugeben, wie Ihre Statistiken abgerufen werden.

In der folgenden Tabelle werden Dimensionen und Dimensionswerte für bestimmte Metriken aufgeführt:

CloudWatch Dimensionen und Dimensionswerte

Dimension	Beschreibung und Werte
DatabaseName	Name der Datenbank. Ein benutzerdefinierter Wert.
Latency	Die möglichen Werte lauten wie folgt: • Kurz – unter 10 Sekunden • Mittel – zwischen 10 Sekunden und 10 Minuten • Lang – über 10 Minuten
QueryType	Mögliche Werte sind INSERT, DELETE, UPDATE, UNLOAD, LOAD, SELECT, CTAS und OTHER.

Dimension	Beschreibung und Werte
`stage`	Die Ausführungsstufen einer Abfrage. Die möglichen Werte lauten wie folgt: • QueryPlanning: Zeit, die für das Parsen und Optimieren von SQL-Anweisungen aufgewendet wurde. • QueryWaiting: Wartezeit in der WLM-Warte schlange. • QueryExecutingRead: Zeit, die für die Ausführung von Leseabfragen aufgewendet wurde. • QueryExecutingInsert: Zeit, die für die Ausführung von Insert-Abfragen aufgewendet wurde. • QueryExecutingDelete: Zeit, die für die Ausführung von Löschabfragen aufgewendet wurde. • QueryExecutingUpdate: Zeit, die mit der Ausführung von Aktualisierungsabfragen verbracht wurde. • QueryExecutingCtas: Zeit, die für die Ausführung von Abfragen zum Erstellen von Tabellen als Abfragen aufgewendet wurde. • QueryExecutingUnload: Zeit, die für die Ausführung von Entladeabfragen aufgewend et wurde. • QueryExecutingCopy: Zeit, die für die Ausführung von Kopieranfragen aufgewendet wurde. • QueryCommit: Zeit, die für das Festschreiben aufgewendet wurde.

Dimension	Beschreibung und Werte
`Namespace`	Der Name des Namespace. Ein benutzerd efinierter Wert.
`Workgroup`	Der Name der Arbeitsgruppe. Ein benutzerd efinierter Wert.
`UsageLimitId`	Der Bezeichner des Nutzungslimits.
`UsageType`	Die Funktion von Amazon Redshift Serverless ist eingeschränkt. Die möglichen Werte lauten wie folgt: • SERVERLESS_COMPUTE • CROSS_REGION_DATASHARING

Arbeiten mit Snapshots und Wiederherstellungspunkten

Ein Backup in Amazon Redshift Serverless ist eine point-in-time Darstellung der Objekte und Daten in Ihrem Namespace. Es gibt zwei Arten von Sicherungen: manuell erstellte Snapshots und Wiederherstellungspunkte, die Amazon Redshift Serverless automatisch für Sie erstellt. Wiederherstellungspunkte werden alle 30 Minuten erstellt und 24 Stunden aufbewahrt.

Wenn Sie die Daten in einem Snapshot oder Wiederherstellungspunkt abrufen möchten, können Sie einen Snapshot zu einem Serverless-Namespace oder bereitgestellten Cluster wiederherstellen. Es gibt drei Szenarien, in denen Sie Snapshots wiederherstellen können:

- Stellen Sie einen Serverless-Snapshot in einem Serverless-Namespace wieder her.
- Stellen Sie einen Serverless-Snapshot in einem bereitgestellten Cluster wieder her.
- Stellen Sie einen Snapshot bereitgestellter Cluster in einem Serverless-Namespace wieder her.

Wählen Sie einen Serverless-Snapshot zu einem bereitgestellten Cluster wiederherstellen, müssen Sie den zu verwendenden Knotentyp (z. B. RA3) und die Anzahl der Knoten auswählen, um die Einstellungen auf Cluster- oder Knotenebene steuern zu können.

wenn Sie einen Snapshot bereitgestellter Cluster in einem Serverless-Namespace wiederherstellen möchten, wählen Sie in der von Redshift bereitgestellten Konsole den Snapshot aus, der wiederhergestellt werden soll, und klicken Sie dann auf Restore from Snapshot (Aus Snapshot wiederherstellen) und auf Restore to serverless namespace (In Serverless-Namespace wiederherstellen). Amazon Redshift wandelt Tabellen mit verschachtelten Schlüsseln in zusammengesetzte Sortierschlüssel um, wenn Sie einen Snapshot bereitgestellter Cluster in einem Serverless-Namespace wiederherstellen. Weitere Informationen zu Sortierschlüsseln finden Sie unter Arbeiten mit Sortierschlüsseln.

Wenn Sie zusätzlichen Kontext hinzufügen möchten, können Sie Snapshots und Wiederherstellungspunkte mit Schlüssel-Wert-Paaren markieren, die Metadaten und Informationen zu diesen Snapshots und Wiederherstellungspunkten bereitstellen. Weitere Informationen zum Markieren von Ressourcen finden Sie unter Markieren von Ressourcen – Übersicht.

Schließlich können Sie Snapshots auch mit anderen AWS-Konten teilen, sodass diese auf Daten innerhalb des Snapshots zugreifen und Abfragen ausführen können.

Snapshots

Sie können einen Snapshot, den Sie über die Amazon-Redshift-Serverless-Konsole erstellt haben, in einem verfügbaren Namespace wiederherstellen, der mit einer Arbeitsgruppe verknüpft ist. Ein Namespace ist verfügbar, sobald er zum Abfragen und/oder Ändern bereit ist. Sie können einen Snapshot, der mit einem von AWS verwalteten KMS-Schlüssel verschlüsselt ist, in einem Serverless-Namespace wiederherstellen.

Wenn Sie eine Liste aller Snapshots anzeigen möchten, wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Datensicherung) aus.

So erstellen Sie einen Snapshot

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Daten-Backup) aus.
2. Wählen Sie Create snapshot (Snapshot erstellen) aus.
3. Wählen Sie einen Namespace aus, von dem Sie einen Snapshot erstellen möchten.
4. Geben Sie eine Snapshot-Kennung ein.
5. (Optional) Wählen Sie einen Aufbewahrungszeitraum aus. Wenn Sie Custom value (Benutzerdefinierter Wert) auswählen, wählen Sie die Anzahl der Tage aus. Der von Ihnen ausgewählte Wert muss zwischen 1 und 3 653 Tagen liegen. Die Standardeinstellung ist unbegrenzt.

6. Wählen Sie Create (Erstellen) aus.

So erstellen Sie einen Snapshot aus der Namespace-Konfiguration

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole die Option Namespace configuration (Namespace-Konfiguration) aus.
2. Wählen Sie den Namespace aus, von dem Sie einen Snapshot erstellen möchten. Sie können nur Snapshots von Namespaces erstellen, die einer Arbeitsgruppe zugeordnet sind und deren Status „Available“ (Verfügbar) lautet.
3. Wählen Sie die Registerkarte Data backup (Datensicherung) aus.
4. Wählen Sie Snapshot erstellen aus.
5. Geben Sie eine Snapshot-Kennung ein.
6. (Optional) Wählen Sie einen Aufbewahrungszeitraum aus. Wenn Sie Custom value (Benutzerdefinierter Wert) auswählen, wählen Sie die Anzahl der Tage aus. Der von Ihnen ausgewählte Wert muss zwischen 1 und 3 653 Tagen liegen.
7. Wählen Sie Erstellen.

So aktualisieren Sie den Aufbewahrungszeitraum eines Snapshots

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Daten-Backup) aus.
2. Wählen Sie einen Snapshot zum Aktualisieren aus.
3. Klicken Sie auf Actions (Aktionen) und Set manual snapshot settings (Manuelle Snapshot-Einstellungen festlegen).
4. Wählen Sie einen Aufbewahrungszeitraum aus. Wenn Sie Custom value (Benutzerdefinierter Wert) auswählen, wählen Sie die Anzahl der Tage aus.
5. Wählen Sie Änderungen speichern aus.

So löschen Sie einen Snapshot

> **Note**
>
> Sie können einen Snapshot, der für ein anderes Konto freigegeben wurde, nicht löschen. Sie müssen zuerst den Zugriff dieses Kontos auf den Snapshot entfernen, bevor Sie den Snapshot löschen.

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Daten-Backup) aus.
2. Wählen Sie einen Snapshot zum Löschen aus.
3. Wählen Sie Aktionen, Löschen aus.
4. Wählen Sie Delete (Löschen) aus.

So erstellen Sie einen finalen Snapshot aller Daten in einem Namespace, bevor der Namespace gelöscht wird

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole die Option Namespace configuration (Namespace-Konfiguration) aus.
2. Wählen Sie den Namespace aus, der gelöscht werden soll.
3. Wählen Sie Aktionen, Löschen aus.
4. Klicken Sie auf Create final Snapshot (Finalen Snapshot erstellen).
5. Geben Sie einen Namen für den Snapshot ein.
6. Geben Sie „delete“ (löschen) ein.
7. Wählen Sie Löschen aus.

So geben Sie einen Snapshot für ein anderes AWS-Konto frei oder entfernen den Zugriff eines Kontos auf einen Snapshot

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Daten-Backup) aus.
2. Wählen Sie einen Snapshot aus, den Sie freigeben möchten.
3. Wählen Sie Actions (Aktionen) und Manage access (Zugriff verwalten) aus.
4. Wenn Sie einen Snapshot für ein anderes Konto freigeben möchten, geben Sie eine AWS-Konto-ID ein. Wenn Sie den Zugriff eines Kontos entfernen möchten, wählen Sie Entfernen aus.
5. Wählen Sie Änderungen speichern aus.

Wiederherstellen eines Snapshots

Beim Wiederherstellen eines Snapshots zu einem Serverless-Namespace wird die aktuelle Datenbank durch die Datenbank im Snapshot ersetzt.

Das Wiederherstellen eines Snapshots in einem Serverless-Namespace erfolgt in zwei Phasen. Die erste Phase ist in wenigen Minuten abgeschlossen, stellt die Daten in Ihrem Namespace wieder

her und stellt sie für Abfragen zur Verfügung. In der zweiten Phase der Wiederherstellung wird Ihre Datenbank optimiert, was zu geringfügigen Leistungsproblemen führen kann. Die zweite Phase kann einige Stunden bis hin zu mehreren Tagen und in einigen Fällen ein paar Wochen dauern. Die Dauer hängt von der Datenmenge ab, die Leistung verbessert sich jedoch schrittweise mit zunehmender Optimierung der Datenbank. Am Ende dieser Phase ist Ihr Serverless-Namespace vollständig optimiert und Sie können Abfragen ohne Leistungsprobleme senden.

So stellen Sie einen Snapshot in einem Serverless-Namespace wieder her

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Daten-Backup) aus.
2. Wählen Sie den Snapshot aus, der wiederhergestellt werden soll. Sie können jeweils nur einen Snapshot wiederherstellen.
3. Klicken Sie auf Actions (Aktionen) und Restore to serverless namespace (In Serverless-Namespace wiederherstellen).
4. Wählen Sie einen verfügbaren Namespace für die Wiederherstellung aus. Sie können nur Namespaces wiederherstellen, deren Status „Available“ (Verfügbar) lautet.
5. Wählen Sie Restore (Wiederherstellen) aus.

So stellen Sie einen Snapshot in einem bereitgestellten Cluster wieder her

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Daten-Backup) aus.
2. Wählen Sie einen Snapshot zum Wiederherstellen aus.
3. Klicken Sie auf Action (Aktion) und Restore to provisioned cluster (Auf bereitgestelltem Cluster wiederherstellen).
4. Geben Sie eine Cluster-ID ein.
5. Wählen Sie einen Node type (Knotentyp) aus. Die Anzahl der Knoten hängt vom Knotentyp ab.
6. Folgen Sie den Anweisungen auf der Konsolenseite, um die Eigenschaften für die Cluster configuration (Clusterkonfiguration) einzugeben. Weitere Informationen finden Sie unter Erstellen eines Clusters.

Weitere Informationen zu Snapshorts für bereitgestellte Cluster finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.

Wiederherstellungspunkte

Wiederherstellungspunkte werden in Amazon Redshift Serverless ungefähr alle 30 Minuten erstellt und 24 Stunden lang gespeichert.

Wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Daten-Backup) aus, um die Wiederherstellungspunkte zu verwalten. Sie können die folgenden Operationen verwenden:

- Stellen Sie einen Wiederherstellungspunkt in einem Serverless-Namespace wieder her.
- Konvertieren eines Wiederherstellungspunkts zu einem Snapshot.

So stellen Sie einen Wiederherstellungspunkt in einem Serverless-Namespace wieder her

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Daten-Backup) aus.
2. Wählen Sie unter Recovery points (Wiederherstellungspunkte) die Creation time (Erstellungszeit) des Wiederherstellungspunkts aus, den Sie wiederherstellen möchten.
3. Wählen Sie Restore (Wiederherstellen) aus. Sie können nur Namespaces wiederherstellen, deren Status „Available“ (Verfügbar) lautet.
4. Geben Sie im Texteingabefeld restore (wiederherstellen) ein und wählen Sie Restore (Wiederherstellen) aus.

So konvertieren Sie einen Wiederherstellungspunkt in einen Snapshot

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Daten-Backup) aus.
2. Wählen Sie unter Recovery points (Wiederherstellungspunkte) die Creation time (Erstellungszeit) des Wiederherstellungspunkts aus, den Sie in einen Snapshot konvertieren möchten.
3. Wählen Sie Create snapshot from recovery point (Snapshot vom Wiederherstellungspunkt erstellen) aus.
4. Geben Sie einen Wert für Snapshot identifier (Snapshot-Kennung) ein.
5. Wählen Sie Erstellen.

Planen von Snapshots

Sie können einen Snapshot-Plan für bestimmte Namespaces erstellen, um den Zeitpunkt der Erstellung eines Snapshots präzise zu steuern. Beim Planen der Snapshot-Erstellung können Sie ein

einmaliges Ereignis erstellen oder Unix-Cron-Ausdrücke verwenden, um einen wiederkehrenden Plan zu erstellen. Cron-Ausdrücke unterstützen drei Felder und werden durch Leerzeichen getrennt.

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

Felder	Werte	Platzhalter
Minuten	0-59	, - * /
Stunden	0–23	, - * /
Day-of-month	1-31	, - * ? / L W
Monat	1-12 oder JAN-DEZ	, - * /
Day-of-week	1-7 oder SUN-SAT	, - * ? / L #
Jahr	1970-2199	, - * /

Platzhalter

- Das Platzhalterzeichen , (Komma) schließt zusätzliche Werte ein. Im Feld `Day-of-week` würde `MON,WED,FRI` Montag, Mittwoch und Freitag abdecken. Die Gesamtwerte sind auf 24 pro Feld begrenzt.
- Das Platzhalterzeichen - (Bindestrich) gibt einen Bereich an. Im Feld `Hour` steht 1–15 für die Stunden 1 bis 15 des angegebenen Tags.
- Das Platzhalterzeichen * (Sternchen) steht für alle Werte im Feld. Im Feld `Hours` steht * für alle Stunden.
- Das Platzhalterzeichen / (Schrägstrich) steht für schrittweise Steigerungen. Im Feld `Hours` können Sie **`1/10`** eingeben, um jede 10. Stunde anzugeben, beginnend mit der ersten Stunde des Tages (z. B. 01:00, 11:00 und 21:00).
- Das Platzhalterzeichen ? (Fragezeichen) steht für einen Wert. In das `Day-of-month` Feld könnten Sie 7 eingeben, und wenn es Ihnen egal war, welcher Wochentag der siebte war, könnten Sie ? in das ay-of-week Feld D eingeben.
- Das Platzhalterzeichen L in den Feldern für `Day-of-month` oder `Day-of-week` gibt den letzten Tag des Monats oder der Woche an.

- Das Platzhalterzeichen W im Feld `Day-of-month` gibt einen Wochentag an. Im Feld `Day-of-month` gibt den `3W` den Tag an, der dem dritten Tag des Monats am nächsten ist.
- Der Platzhalter # im ay-of-week Feld D gibt eine bestimmte Instance des angegebenen Wochentags innerhalb eines Monats an. Beispiel: 3#2 steht für den zweiten Dienstag des Monats: Die 3 bezieht sich auf Dienstag, da dies der dritte Tag jeder Woche ist, und die 2 bezieht sich auf den zweiten Tag dieses Typs innerhalb des Monats.

> **Note**
>
> Wenn Sie ein „#“-Zeichen verwenden, können Sie nur einen Ausdruck im day-of-week Feld definieren. Beispielsweise ist "3#1,6#3" ungültig, da dies als zwei Ausdrücke interpretiert wird.

Einschränkungen

- Es ist nicht möglich, die Felder `Day-of-month` und `Day-of-week` im gleichen Cron-Ausdruck anzugeben. Wenn Sie einen Wert in einem der Felder angeben, müssen Sie in dem anderen Feld ein ? (Fragezeichen) eingeben.
- Snapshot-Zeitpläne unterstützen folgende Häufigkeiten nicht:
  - Häufiger als einmal pro Stunde geplante Snapshots.
  - Seltener als einmal pro Tag (24 Stunden) geplante Snapshots.

  Wenn Zeitpläne sich so überschneiden, dass Snapshots innerhalb eines Fensters von 1 Stunde geplant werden, wird ein Validierungsfehler erzeugt.

Die folgende Tabelle enthält einige Beispiele für Cron-Zeichenfolgen.

Minuten	Stunden	Wochentag	Bedeutung			
0	14-20/1	TUE	Jede Stunde zwischen 14:00 und 20:00 Uhr am Dienstag.			

Minuten	Stunden	Wochentag	Bedeutung
0	21	MO-FR	Von Montag bis Freitag jeden Abend um 21.00 Uhr.
30	0/6	SAT-SUN	Inkrementell alle 6 Stunden am Samstag und Sonntag, beginnend 30 Minuten nach Mitternacht (00:30) an diesem Tag. Das Ergebnis ist ein Snapshot um [00:30, 06:30, 12:30 und 18:30] Uhr am jeweiligen Tag.
30	12/4	*	Inkrementell alle 4 Stunden jeden Tag, beginnend um 12:30 Uhr. Das ergibt [12:30, 16:30, 20:30] Uhr.

Das folgende Beispiel zeigt die Erstellung eines Plans, der jeden Tag in 2-Stunden-Schritten ab 15:15 Uhr ausgeführt wird.

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

Derzeit können Sie nur die Amazon-Redshift-Serverless-API oder die AWS CLI verwenden, um einen Snapshot-Plan zu erstellen. Weitere Informationen zu diesen Operationen finden Sie unter Verwenden der AWS CLI und der Amazon Redshift-Serverless-API.

Kopieren von Sicherungen zu einer anderen AWS-Region

Sie können Amazon Redshift Serverless für das automatische Kopieren von Snapshots und Wiederherstellungspunkten zu einer anderen AWS-Region konfigurieren. Wenn Sie einen Snapshot in der ursprünglichen AWS-Region erstellen, wird er zu einer Zielregion kopiert. Sie können Ihren Namespace so konfigurieren, dass er Snapshots und Wiederherstellungspunkte jeweils nur zu einer Ziel-AWS-Region kopiert. Eine Liste der AWS-Regionen, in denen Amazon Redshift Serverless verfügbar ist, finden Sie in der Übersicht über die Endpunkte für die Redshift-Serverless-API in der Allgemeine Amazon Web Services-Referenz.

Bei der Konfiguration des Kopierens von Sicherungen können Sie auch einen Aufbewahrungszeitraum angeben, über den Amazon Redshift Serverless den kopierten Snapshot aufbewahren soll. Sie können die Aufbewahrungszeiträume von Wiederherstellungspunkten nicht ändern, die 1 Tag betragen muss. Die Aufbewahrungszeiträume für Snapshots in der Zielregion sind unabhängig von den Aufbewahrungszeiträumen für Snapshots in der Quellregion. Standardmäßig werden Snapshots für einen unbegrenzten Zeitraum aufbewahrt. Wenn Sie Benutzerdefinierter Wert auswählen, müssen Sie die Anzahl der Tage auswählen. Der von Ihnen ausgewählte Wert muss zwischen 1 und 3653 Tagen liegen.

Um die Zielregion zu ändern, zu der Snapshots kopiert werden sollen, müssen Sie zunächst das Kopieren von Sicherungen deaktivieren und die neue Zielregion angeben, wenn Sie das Kopieren erneut aktivieren.

Wenn ein Snapshot oder Wiederherstellungspunkt zu einer Zielregion kopiert wurde, können Sie diesen für die Wiederherstellung von Daten zur Region verwenden.

Standardmäßig werden Ihre Daten mit einem Schlüssel verschlüsselt, den AWS für Sie verwaltet. Wenn Sie einen anderen Schlüssel verwenden möchten, wählen Sie beim Konfigurieren des Kopierens der Sicherung in der ursprünglichen AWS-Region den gewünschten Schlüssel aus. Anschließend erstellt Amazon Redshift Serverless automatisch eine Gewährung, die die Snapshot-Verschlüsselung in der Ziel-AWS-Region aktiviert.

Um Sicherungen zu einer anderen Region zu kopieren, müssen Sie die folgenden IAM-Berechtigungen besitzen:

```
redshift-serverless:CreateSnapshotCopyConfiguration
redshift-serverless:UpdateSnapshotCopyConfiguration
redshift-serverless:ListSnapshotCopyConfigurations
redshift-serverless:DeleteSnapshotCopyConfiguration
```

Wenn Sie Ihre Sicherungen mit einem eigenen KMS-Schlüssel verschlüsseln, benötigen Sie außerdem die folgenden Berechtigungen:

```
kms:CreateGrant
kms:DescribeKey
```

Konfigurieren des Kopierens Ihrer Snapshots oder Wiederherstellungspunkte zu einer anderen AWS-Region

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole den Namespace aus, für den Sie das Kopieren von Snapshots oder Wiederherstellungspunkten konfigurieren möchten.
2. Wählen Sie Aktionen und dann Regionsübergreifende Sicherung konfigurieren aus.
3. Wählen Sie die gewünschte AWS-Region aus, zu der der Snapshot kopiert werden soll.
4. (Optional) Wählen Sie den Aufbewahrungszeitraum für den Snapshot aus. Wenn Sie Benutzerdefinierter Wert auswählen, müssen Sie die Anzahl der Tage angeben. Der von Ihnen ausgewählte Wert muss zwischen 1 und 3653 Tagen (einschließlich) liegen. Standardmäßig werden Snapshots unbegrenzt aufbewahrt.
5. (Optional) Wählen Sie einen anderen AWS KMS-Schlüssel aus, der zum Verschlüsseln in der Zielregion verwendet werden soll.
6. Wählen Sie Save configuration (Konfiguration speichern) aus.

Wiederherstellen einer Tabelle

Sie können auch eine bestimmte Tabelle aus einem Snapshot oder Wiederherstellungspunkt wiederherstellen. Hierzu geben Sie den Quell-Snapshot oder -Wiederherstellungspunkt, die Datenbank, das Schema, die Tabelle, die Zieldatenbank, das Schema und den Namen der neuen Tabelle an. Der Name dieser neuen Tabelle darf nicht mit dem Namen einer vorhandenen Tabelle identisch sein. Wenn Sie eine vorhandene Tabelle ersetzen möchten, indem Sie eine Tabelle wiederherstellen, müssen Sie die vorhandene Tabelle umbenennen oder entfernen, bevor Sie die Tabelle wiederherstellen.

Die Zieltabelle wird mithilfe der Spaltendefinitionen, Tabellenattribute und Spaltenattribute der Quelltabelle erstellt. Eine Ausnahme gilt für Fremdschlüssel. Um Konflikte aufgrund von Abhängigkeiten zu vermeiden, übernimmt die Zieltabelle keine Fremdschlüssel von der Quelltabelle. Alle Abhängigkeiten, wie z. B. Ansichten oder Berechtigungen, die für die Quelltabelle gewährt wurden, gelten nicht für die Zieltabelle.

Wenn der Eigentümer der Quelltabelle existiert, dann ist der Benutzer der Eigentümer der wiederhergestellten Tabelle, vorausgesetzt, dieser Benutzer verfügt über ausreichend Berechtigungen, um der Eigentümer einer Beziehung in der angegebenen Datenbank und dem Schema zu sein. Anderenfalls ist die wiederhergestellte Tabelle Besitz des Adminbenutzers, der beim Starten des Clusters angelegt wurde.

Die wiederhergestellte Tabelle wird wieder in den Status zurückgesetzt, in dem sie sich zum Zeitpunkt der Sicherung befunden hat. Dazu gehören Sichtbarkeitsregeln für die Transaktion, die durch die Einhaltung der serialisierbaren Isolation durch Amazon Redshift definiert sind. Das heißt, dass Daten für derzeit übertragene Transaktionen, die nach dem Backup gestartet wurden, sofort sichtbar sind.

Sie können die Amazon-Redshift-Serverless-Konsole verwenden, um Tabellen aus einen Snapshot wiederherzustellen.

Für die Wiederherstellung einer Tabelle aus einer Datensicherung gelten die folgenden Einschränkungen:

- Sie können jeweils nur eine Tabelle wiederherstellen.
- Alle Abhängigkeiten, wie z. B. Ansichten oder Berechtigungen, die für die Quelltabelle gewährt wurden, gelten nicht für die Zieltabelle.
- Wenn die Sicherheit auf Zeilenebene für die Wiederherstellung einer Tabelle aktiviert ist, stellt Amazon Redshift Serverless die Tabelle wieder her, wobei die Sicherheit auf Zeilenebene aktiviert ist.

Wiederherstellen einer Tabelle über die Amazon-Redshift-Serverless-Konsole

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole Data backup (Daten-Backup) aus.
2. Wählen Sie den Snapshot oder Wiederherstellungspunkt aus, der die wiederherzustellende Tabelle enthält.
3. Wählen Sie Aktionen, Tabelle aus Snapshot wiederherstellen oder Tabelle aus Wiederherstellungspunkt wiederherstellen aus.
4. Geben Sie Informationen zum Quell-Snapshot und -Wiederherstellungspunkt ein. Wählen Sie dann Tabelle wiederherstellen aus.

Verwenden der AWS Command Line Interface und Amazon-Redshift-Serverless-API

Abgesehen von der Verwendung der AWS-Konsole können Sie auch die AWS CLI oder die Amazon Redshift Serverless API zur Interaktion mit Snapshots und Wiederherstellungspunkten nutzen. In der folgenden Tabelle werden die API- und CLI-Operationen aufgeführt, die Sie für die Verwaltung von Snapshots und Wiederherstellungspunkten verwenden können.

API-Operation	CLI-Befehl	Beschreibung
CreateSnapshot	create-snapshot	Erstellt einen Snapshot. Snapshots müssen mit einem Namespace verknüpft sein, daher müssen Sie den Namen eines Namespace in Ihre Anfrage aufnehmen . Standardmäßig speichert Amazon Redshift Serverles s Snapshots für unbegrenz te Zeit. Sie können jedoch einen Aufbewahrungszeitraum angeben.
RestoreFromSnapshot	restore-from-snapshot	Stellt die Datenbanken in einem Snapshot in Ihrem Namespace wieder her. Wenn Sie einen Snapshot von Amazon Redshift Serverless in einem bereitgestellten Cluster wiederherstellen, müssen Sie den `snapshotArn` des Snapshots angeben, den Sie wiederherstellen. Andernfalls können Sie bei der Wiederher stellung von Serverless auf Serverless `snapshotA`

API-Operation	CLI-Befehl	Beschreibung
		`rn` oder `snapshotName` angeben, aber nicht beides.
RestoreTableFromSnapshot	restore-table-from-snapshot	Stellt eine Tabelle aus einem Snapshot zu Ihrem Amazon-Redshift-Serverless-Namespace wieder her. Sie können diese Operation nicht zur Wiederherstellung von Tabellen mit verschachtelten Sortierschlüsseln verwenden.
GetSnapshot	get-snapshot	Ruft Informationen zu einem Snapshot ab.
ListSnapshots	list-snapshots	Ruft Informationen zu mehreren Snapshots ab.
DeleteSnapshot	delete-snapshot	Löscht einen Snapshot.
RestoreFromRecoveryPoint	restore-from-recovery-point	Stellt die Daten innerhalb eines Wiederherstellungs punkts zu Ihrem Namespace wieder her.
RestoreTableFromRecoveryPoint	restore-table-from-recovery-Punkt	Stellt eine Tabelle aus einem Wiederherstellungspunkt zu Ihrem Amazon-Redshift-Serverless-Namespace wieder her. Sie können diese Operation nicht zur Wiederherstellung von Tabellen mit verschachtelten Sortiersc hlüsseln verwenden.

API-Operation	CLI-Befehl	Beschreibung
ConvertRecoveryPointToSnapshot	convert-recovery-point-to-Snapshot	Konvertiert einen Wiederherstellungspunkt in einen Snapshot.
GetRecoveryPoint	get-recovery-point	Ruft Informationen zu einem Wiederherstellungspunkt ab.
ListRecoveryPoints	list-recovery-points	Ruft Informationen zu mehreren Wiederherstellungspunkten ab.

Verwenden Sie die folgenden API-Operationen, um die Snapshot-Erstellung zu planen.

API-Operation	CLI-Befehl	Beschreibung
CreateScheduledAction	create-scheduled-action	Erstellt eine geplante Aktion, die einen Zeitplan und eine Amazon-Redshift-Serverless-Aktion enthält. Beispielsweise können Sie einen Zeitplan erstellen, wann der `CreateSnapshot` -API-Vorgang ausgeführt werden soll.
DeleteScheduledAction	delete-scheduled-action	Löscht eine geplante Aktion.
GetScheduledAction	get-scheduled-action	Ruft Informationen zu einer geplanten Aktion ab.
ListScheduledActions	list-scheduled-actions	Ruft Informationen zu einer Liste geplanter Aktionen ab.
UpdateScheduledAction	update-scheduled-action	Aktualisiert eine geplante Aktion.

Datenfreigabe in Amazon Redshift Serverless

Verwenden Sie Data Sharing, um die meisten up-to-date und konsistentesten Informationen auszutauschen, sobald sie in Amazon Redshift Serverless aktualisiert werden.

Datenfreigabe in Amazon Redshift Serverless

Durch die gemeinsame Nutzung von Daten haben Sie Live-Zugriff auf Daten, sodass Ihre Benutzer die meisten up-to-date und konsistentesten Informationen sehen können, wenn sie in Amazon Redshift Serverless aktualisiert werden.

Erste Schritte mit der Datenfreigabe in Amazon Redshift Serverless

Sie können Daten für Lesezwecke auf verschiedenen Amazon-Redshift-Serverless-Instances eines oder mehrerer AWS-Konten freigeben.

Sie können mit der Datenfreigabe beginnen, indem Sie entweder die SQL-Schnittstelle oder die Amazon-Redshift-Konsole verwenden. Weitere Informationen finden Sie unter Erste Schritte mit der Datenfreigabe über die SQL-Schnittstelle oder Erste Schritte bei der Datenfreigabe mit der Konsole im Amazon Redshift Datenbankentwicklerhandbuch im Amazon Redshift Datenbankentwicklerhandbuch.

Durch die gemeinsame Nutzung von Daten können serverlose Amazon Redshift Namespaces und bereitgestellte Cluster Live-Daten miteinander teilen, unabhängig davon, ob sie sich innerhalb eines Across oder eines Across befinden. AWS-Konto AWS-Konten AWS-Regionen Weitere Informationen finden Sie unter Regionen, in denen Datenfreigabe verfügbar ist.

Um mit dem Teilen von Daten innerhalb eines zu beginnen AWS-Konto, öffnen Sie die AWS Management Console und wählen Sie dann die Amazon Redshift Redshift-Konsole aus. Klicken Sie auf Namespace configuration (Namespace-Konfiguration) und dann auf Datashares. Befolgen Sie die unter Erste Schritte bei der Datenfreigabe mit der Konsole beschriebenen Verfahren im Datenbankentwicklerhandbuch zu Amazon Redshift.

Um mit der gemeinsamen Nutzung von Daten zu beginnen AWS-Konten, öffnen Sie die AWS Management Console Amazon Redshift-Konsole und wählen Sie dann die Amazon Redshift Redshift-Konsole aus. Klicken Sie auf Datashares. Befolgen Sie die unter Erste Schritte bei der Datenfreigabe mit der Konsole beschriebenen Verfahren im Datenbankentwicklerhandbuch zu Amazon Redshift.

Erstellen Sie eine Datenbank in einem Namespace, dem eine Arbeitsgruppe zugeordnet ist, um mit der Abfrage von Daten in einem Datashare zu beginnen. Wählen Sie einen Namespace aus

einem angegebenen Datashare aus, dem eine Arbeitsgruppe zugeordnet ist, und erstellen Sie eine Datenbank, um Daten abzufragen. Folgen Sie den Schritten unter Erstellen von Datenbanken aus Datashares.

Gewähren des Zugriffs zum Anzeigen von Datashares mithilfe der Konsole

Ein Superuser kann Benutzern, die keine Superuser sind, Zugriff gewähren, damit sie die von allen Benutzern erstellten Datashares anzeigen können.

Wenn Sie einem Benutzer Zugriff auf ein Datashare ermöglichen möchten, verwenden Sie den folgenden Befehl. Dabei ist datashare_name der Name des Datashare und user-name der Name des Benutzers, dem Sie den Zugriff ermöglichen möchten.

```
grant share on datashare datashare_name to "IAM:test_user";
```

Wenn Sie einer Benutzergruppe Zugriff auf ein Datashare ermöglichen möchten, erstellen Sie zunächst eine Benutzergruppe mit Benutzern. Informationen zum Erstellen von Benutzergruppen finden Sie unter CREATE GROUP. Verwenden Sie dann den folgenden Befehl, um einem Benutzer Zugriff auf das Datashare zu ermöglichen. Dabei ist datashare_name der Name des Datashare und user-group der Name der Benutzergruppe, der Sie den Zugriff ermöglichen möchten.

```
grant share on datashare datashare_name to group user_group;
```

Informationen zur Verwendung der GRANT-Anweisung finden Sie unter GRANT.

Überlegungen zur Datenfreigabe in Amazon Redshift Serverless

Im Folgenden finden Sie Überlegungen für das Arbeiten mit der Amazon-Redshift-Serverless-Datenfreigabe:

- Amazon Redshift unterstützt nur bereitgestellte Cluster der Instance-Typen ra3.16xlarge, ra3.4xlarge und ra3.xlplus sowie Serverless-Endpunkte als Produzent und Verbraucher des Datasharing.
- Amazon Redshift Serverless ist standardmäßig verschlüsselt.

Eine Liste der Datasharing-Einschränkungen, einschließlich unterstützter Datenbankobjekte, Verschlüsselungsanforderungen und Sortierschlüsselanforderungen, finden Sie unter Überlegungen zur Verwendung der Datenfreigabe in Amazon Redshift im Datenbankentwicklerhandbuch zu Amazon Redshift.

Markieren von Ressourcen – Übersicht

In AWS sind Tags benutzerdefinierte Markierungen, die aus Schlüssel-Wert-Paaren bestehen. Amazon Redshift Serverless unterstützt das Markieren, um Metadaten für Ressourcen auf einen Blick bereitzustellen.

Tags sind für Ressourcen nicht erforderlich, aber sie helfen dabei, Kontextinformationen bereitzustellen. Sie können Ressourcen mit Metadaten und Informationen zur Ressource markieren. Beispiel: Nehmen Sie an, Sie möchten nachverfolgen, welche Ressourcen zu einer Testumgebung und welche zu einer Produktionsumgebung gehören. Dazu könnten Sie einen Schlüssel namens Umgebung erstellen und dann einen Wert „Test“ oder „Produktion“ angeben, um die Ressourcen anzugeben, die in der jeweiligen Umgebung verwendet werden. Wenn Sie auch in anderen AWS-Services Markierungen oder Standardkategorien für Ihr Geschäft verwenden, sollten Sie aus Konsistenzgründen dieselben Schlüssel-Wert-Paare erstellen.

Wenn Sie eine Ressource löschen, werden alle Tags der Ressource ebenfalls gelöscht. Sie können AWS CLI und die Amazon-Redshift-Serverless-Konsole verwenden, um Serverless-Ressourcen zu kennzeichnen. Verfügbare API-Operationen sind: `TagResource`, `UntagResource` und `ListTagsForResource`.

Jede Ressource verfügt über genau einen Tag-Satz, d. h. eine Zusammenstellung von einem oder mehreren Tags, die der Ressource zugewiesen sind. Jede Ressource kann pro Tag-Satz bis zu 50 Tags enthalten. Sie können Tags beim Erstellen der Ressource hinzufügen, aber auch noch, nachdem die Ressource erstellt wurde. Sie können den folgenden Serverless-Ressourcentypen Tags hinzufügen:

- Arbeitsgruppen
- Namespaces
- Snapshots
- Wiederherstellungspunkte

Für Tags gelten zwei Anforderungen:

- Schlüssel dürfen nicht mit dem Präfix `aws:` beginnen.
- Schlüssel müssen in einem Tag-Satz eindeutig sein.
- Schlüssel müssen zwischen 1 und 128 Zeichen lang sein.
- Ein Wert muss zwischen 0 und 256 Zeichen haben.

- Werte brauchen pro Tag-Satz nicht eindeutig zu sein.
- Zulässige Zeichen für Schlüssel und Werte sind Unicode-Buchstaben, Ziffern, Leerzeichen sowie die folgenden Sonderzeichen: _ . : / = + - @.
- Bei Schlüsseln und Werten wird die Groß-/Kleinschreibung berücksichtigt.

So verwalten Sie Tags Ihrer Amazon-Redshift-Serverless-Ressourcen

1. Wählen Sie in der Amazon-Redshift-Serverless-Konsole Manage tags (Tags verwalten) aus.
2. Geben Sie den zu suchenden Ressourcentyp ein und wählen Sie Search resources (Ressourcen durchsuchen). Wählen Sie die Ressource aus, für die Sie Tags verwalten möchten, und wählen Sie dann Manage tags (Tags verwalten) aus.
3. Geben Sie die Schlüssel und optionalen Werte an, die Sie der Ressource hinzufügen möchten. Wenn Sie ein Tag ändern, können Sie den Wert des Tags ändern, aber nicht den Schlüssel.
4. Wenn Sie mit dem Hinzufügen, Entfernen oder Ändern von Tags fertig sind, wählen Sie Save changes (Änderungen speichern) und dann Apply (Anwenden) aus, um Ihre Änderungen zu speichern.

Von Amazon Redshift bereitgestellte Cluster

In den folgenden Abschnitten erlernen Sie die Grundlagen der Erstellung eines Data Warehouses durch den Start von Datenverarbeitungsknoten, den so genannten Amazon-Redshift-Clustern.

Themen

- Überblick über Amazon Redshift
- Verwenden von EC2-VPC beim Erstellen Ihres Clusters
- Standard-Festplattenspeicherplatzalarm
- Cluster-Status
- Überlegungen zur Verwendung von von Amazon Redshift bereitgestellten Clustern
- Cluster-Operationen
- Konfigurieren einer Multi-AZ-Bereitstellung
- Verwalten von Clustern mithilfe der Konsole
- Verwaltung von Clustern mithilfe der AWS CLI und der Amazon Redshift Redshift-API
- Verwaltung von Clustern in einer VPC
- Cluster-Versionsverlauf

Überblick über Amazon Redshift

Ein Amazon-Redshift-Data-Warehouse ist eine Sammlung von Datenverarbeitungsressourcen, den so genannten Knoten, die zu Gruppen, den so genannten Clustern, zusammengefasst werden. In jedem Cluster wird eine Amazon-Redshift-Engine ausgeführt, und er enthält mindestens eine Datenbank.

> **Note**
>
> Derzeit ist die Amazon-Redshift-Engine der Version 1.0 verfügbar. Wenn die Engine aktualisiert wird, können jedoch künftig mehrere Amazon-Redshift-Engine-Versionen zur Auswahl verfügbar sein.

Cluster und Knoten in Amazon Redshift

Ein Amazon-Redshift-Cluster besteht aus mehreren Knoten. Jeder Cluster hat einen Leader- und einen oder mehrere Datenverarbeitungsknoten. Der Leader-Knoten erhält Abfragen von Client-Anwendungen, parst diese und entwickelt Abfrageausführungspläne. Der Leader-Knoten koordiniert dann die parallele Ausführung dieser Pläne mit den Datenverarbeitungsknoten und aggregiert die Zwischenergebnisse von diesen Knoten. Anschließend werden die Ergebnisse an die Client-Anwendungen zurückgegeben.

Computing-Knoten führen die Abfrageausführungspläne aus und übermitteln Daten untereinander, um diese Abfragen zu bedienen. Die Zwischenergebnisse werden zur Aggregierung an den Leader-Knoten gesendet, bevor sie an die Client-Anwendungen zurückgesendet werden. Weitere Informationen zu Leader- und Datenverarbeitungsknoten finden Sie unter Data-Warehouse-Systemarchitektur im Entwicklerhandbuch für Amazon Redshift Database.

> **Note**
>
> Wenn Sie einen Cluster auf der Amazon Redshift Redshift-Konsole (https://console.aws.amazon.com/redshiftv2/) erstellen, können Sie eine Empfehlung für Ihre Cluster-Konfiguration erhalten, die auf der Größe Ihrer Daten und Abfrageeigenschaften basiert. Um diesen Größenrechner zu verwenden, suchen Sie auf der Konsole unter AWS Regionen, die RA3-Knotentypen unterstützen, nach Hilfe bei der Auswahl. Weitere Informationen finden Sie unter Erstellen eines Clusters.

Wenn Sie einen Cluster starten, ist eine der anzugebenden Optionen der Knotentyp. Der Knotentyp bestimmt, CPU, RAM, Speicherkapazität und Speichertreibertyp für jeden Knoten.

Amazon Redshift bietet verschiedene Knotentypen für Ihre Workloads. Wir empfehlen Ihnen die Auswahl von RA3 oder DC2, je nach benötigter Leistung, Datenvolumen und dessen Wachstum.

RA3-Knoten mit verwaltetem Speicher ermöglichen die Optimierung Ihres Data Warehouse durch unabhängige Skalierung und Zahlung für Datenverarbeitungs- und Speicherkapazitäten. Mit RA3 wählen Sie die Anzahl der benötigten Knoten auf Grundlage der Leistungsanforderungen aus und zahlen nur für den tatsächlich genutzten verwalteten Speicher. Sie sollten die Größe Ihres RA3-Clusters nach dem Datenvolumen richten, das sie täglich verarbeiten. Cluster, die den Knotentyp RA3 verwenden, werden in einer Virtual Private Cloud (VPC) gestartet. RA3-Cluster können nicht in EC2-Classic gestartet werden. Weitere Informationen finden Sie unter Erstellen eines Clusters in einer VPC.

Für von Amazon Redshift verwalteten Speicher werden in jedem RA3-Knoten große Hochleistungs-SSDs als schnelle lokale Speicher sowie Amazon S3 für die langfristige Speicherung eingesetzt. Sobald die Daten in einem Knoten die Kapazität der großen lokalen SSDs übersteigen, lagert der von Amazon Redshift verwaltete Speicher die Daten automatisch zu Amazon S3 aus. Unabhängig vom verwendeten Speicher – Hochleistungs-SSDs oder Amazon S3 – zahlen Sie für Amazon-Redshift-verwalteten Speicher den gleichen niedrigen Tarif. Für Workloads, die ständig wachsenden Speicherplatz benötigen, können Sie mit Managed Storage Ihre Data Warehouse-Speicherkapazität unabhängig von den Rechenknoten automatisch skalieren.

DC2-Knoten empfehlen sich für datenverarbeitungsintensive Data Warehouses mit lokalem SSD-Speicher. Hier können Sie die Anzahl der benötigten Knoten auf der Grundlage Ihres Datenvolumens und Ihrer Leistungsanforderungen auswählen. DC2-Knoten speichern Ihre Daten für eine möglichst hohe Leistung lokal. Bei steigendem Datenvolumen können Sie weitere Datenverarbeitungsknoten hinzufügen, um die Speicherkapazität des Clusters zu erhöhen. Bei Datensätzen unter 1 TB (komprimiert) empfehlen sich DC2-Knoten für eine optimale Leistung zum günstigsten Preis. Sollten Sie von einem Anstieg des Datenvolumens ausgehen, empfehlen wir die Verwendung von RA3-Knoten, damit Sie die Datenverarbeitungsleistung und Speicherkapazität unabhängig voneinander skalieren können, um den besten Preis und die beste Leistung zu erzielen. Cluster, die den Knotentyp DC2 verwenden, werden in einer Virtual Private Cloud (VPC) gestartet. DC2-Cluster können nicht im EC2-Classic-Modus gestartet werden. Weitere Informationen finden Sie unter Erstellen eines Clusters in einer VPC.

DS2-Knoten eignen sich für große Data Warehouses mit HDDs. Wir empfehlen jedoch die Verwendung von RA3-Knoten. Wenn Sie DS2-Knoten verwenden, finden Sie unter Migration zu RA3-Knotentypen Upgrade-Richtlinien. Kunden, die acht oder mehr ds2.xlarge-Knoten oder eine beliebige Anzahl von ds2.8xlarge-Knoten nutzen, können jetzt ein Upgrade auf RA3 vornehmen und sich doppelte Speicherkapazität sowie eine bessere Leistung für die gleichen On-Demand-Kosten sichern.

Knotentypen sind in unterschiedlichen Größen verfügbar. Die Knotengröße und die Anzahl der Knoten bestimmen den gesamten Speicherplatz für einen Cluster. Weitere Informationen finden Sie unter Details zu Knotentypen.

Einige Knotentypen erlauben einen Knoten (Single Node) oder mehrere Knoten (Multiple Node). Die minimale Anzahl von Knoten für Cluster einiger Knotentypen beträgt zwei Knoten. Auf einem Single Node-Cluster dient der einzelne Knoten für Leader- und Datenverarbeitungsfunktionen. Cluster mit einem Knoten werden nicht für die Ausführung von Produktions-Workloads empfohlen. Auf einem Multi Node-Cluster ist der Leader-Knoten von den Datenverarbeitungsknoten getrennt.

Der Führungsknoten hat denselben Knotentyp wie die Datenverarbeitungsknoten. Sie zahlen nur für Datenverarbeitungsknoten.

Amazon Redshift wendet Kontingente auf Ressourcen für jedes AWS Konto in jeder AWS Region an. Ein Kontingent schränkt die Anzahl der Ressourcen ein, die Ihr Konto für einen bestimmten Ressourcentyp, z. B. Knoten oder Snapshots, innerhalb einer Region erstellen kann. AWS Weitere Informationen zu den Standardkontingenten für Amazon-Redshift-Ressourcen finden Sie unter Amazon-Redshift-Limits in der Allgemeine Amazon Web Services-Referenz. Um eine Erhöhung anzufragen, übermitteln Sie ein Formular für die Erhöhung des Amazon-Redshift-Limits.

Die Kosten Ihres Clusters hängen von der AWS Region, dem Knotentyp, der Anzahl der Knoten und davon ab, ob die Knoten im Voraus reserviert wurden. Weitere Informationen zu den Kosten von Knoten finden Sie auf der Seite Amazon Redshift – Preise.

Details zu Knotentypen

Die folgenden Tabellen führen die Knotenspezifikationen für alle Knotentypen und -größen auf. Die Überschriften in den Tabellen haben folgende Bedeutungen:

- vCPU ist die Anzahl der virtuellen CPUs für jeden Knoten.
- RAM ist der Speicherplatz in Gibibyte (GiB) für jeden Knoten.
- Standard-Slices pro Knoten ist die Anzahl von Slices, in die ein Datenverarbeitungsknoten partitioniert wird, wenn ein Cluster mit klassischer Größenanpassung erstellt oder geändert wird.

  Die Anzahl der Slices pro Knoten ändert sich unter Umständen, wenn die Clustergröße mithilfe der elastischen Größenanpassung geändert wird. Die Gesamtzahl der Slices auf allen Datenverarbeitungsknoten im Cluster bleibt jedoch nach der elastischen Größenanpassung gleich.

  Wenn Sie einen Cluster mit der Wiederherstellungsoperation aus einem Snapshot erstellen, ändert sich die Anzahl der Slices des resultierenden Clusters möglicherweise gegenüber dem ursprünglichen Cluster, wenn Sie den Knotentyp ändern.
- Speicher steht für die Kapazität und den Typ des Speichers für jeden Knoten.
- Knotenbereich steht für die minimale und maximale Anzahl von Knoten, die Amazon Redshift für den Knotentyp und die Knotengröße unterstützt.

> **Note**
>
> Je nach dem Kontingent, das für Ihr AWS Konto in der ausgewählten AWS Region gilt, sind Sie möglicherweise auf weniger Knoten beschränkt. Um eine Erhöhung anzufragen, übermitteln Sie ein Formular für die Erhöhung des Amazon-Redshift-Limits.

- Gesamtkapazität ist die gesamte Speicherkapazität für den Cluster, wenn Sie die maximale in dem Knotenbereich angegebene Zahl von Knoten verwenden.

RA3-Knotentypen

Knotentyp	vCPU	RAM (GiB)	Standar Slices pro Knoten	Limit für verwaltet en Speicher pro Knoten [1]	Knotenber eich mit Cluster-E rstellung	Gesamte verwaltete Speicherk apazität [2]
ra3.xlplus (Einzelkn oten)	4	32	2	4 TB	1	4 TB[3]
ra3.xlplus (mehrere Knoten)	4	32	2	32 TB	2–16[4]	1 024 TB[4]
ra3.4xlarge	12	96	4	128 TB	2–32[5]	8192 TB[5]
ra3.16xla rge	48	384	16	128 TB	2–128	16 384 TB

[1] Das Speicherkontingent für verwalteten Amazon-Redshift-Speicher. Dies ist ein hartes Limit.

[2] Das insgesamt verwaltete Speicherkontingent ist die maximale Anzahl von Knoten multipliziert mit dem verwalteten Speicherkontingent pro Knoten.

[3] Zum Ändern der Größe eines Clusters mit nur einem Knoten auf mehrere Knoten wird nur die klassische Größenanpassung unterstützt.

[4] Sie können einen Cluster mit dem Knotentyp ra3.xlplus (mehrere Knoten) erstellen, der bis zu 16 Knoten hat. Bei Clustern mit mehreren Knoten können Sie die Größe mit elastischer Größenanpassung auf maximal 32 Knoten ändern.

[5] Sie können einen Cluster mit dem Knotentyp ra3.4xlarge mit bis zu 32 Knoten erstellen. Sie können die Größe mit der elastischen Größenanpassung auf maximal 64 Knoten ändern.

Dense Storage-Knotentypen

Knotentyp	vCPU	RAM (GiB)	Standar Slices pro Knoten	Speicher pro Knoten	Knotenber eich	Gesamtkap azität
ds2.xlarge	4	31	2	2 TB HDD	1–32	64 TB
ds2.8xlarge	36	244	16	16 TB HDD	2–128	2 PB

Dense Compute-Knotentypen

Knotentyp	vCPU	RAM (GiB)	Standar Slices pro Knoten	Speicher pro Knoten	Knotenber eich	Gesamtkap azität
dc2.large	2	15	2	160 GB NVMe-SSD	1–32	5.12 TB
dc2.8xlarge	32	244	16	2,56 TB NVMe-SSD	2–128	326 TB
dc1.large[1]	2	15	2	160 GB SSD	1–32	5.12 TB
dc1.8xlarge[1]	32	244	32	2.56 TB SSD	2–128	326 TB

[1] Wir empfehlen DC2-Knotentypen anstelle von DC1-Knotentypen. Weitere Informationen zum Upgrade finden Sie unter Migrieren von DC1-Knotentypen zu DC2-Knotentypen.

Frühere Namen für Knotentypen

In früheren Versionen von Amazon Redshift hatten bestimmte Knotentypen andere Namen. Sie können die vorherigen Namen in der Amazon Redshift Redshift-API und AWS CLI verwenden. Wir empfehlen jedoch, alle Scripts, die die alten Namen verwenden, so zu aktualisieren, dass sie die neuen Namen enthalten. Die aktuellen und die früheren Namen sind die folgenden.

Aktueller Name	Frühere Namen
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

Bestimmung der Anzahl der Knoten

Da Amazon Redshift Abfragen über alle Computing-Knoten eines Clusters verteilt und parallel verarbeitet, können Sie die Abfrageleistung verbessern, indem Sie Ihrem Cluster Knoten hinzufügen. Wenn Sie einen Cluster mit mindestens zwei Computing-Knoten betreiben, werden die Daten auf jedem Knoten auf Festplatten eines anderen Knotens gespiegelt, um das Risiko eines Datenverlustes zu verringern.

Sie können die Abfrageleistung in der Amazon Redshift Redshift-Konsole und mit CloudWatch Amazon-Metriken überwachen. Sie können auch Knoten nach Bedarf hinzufügen oder entfernen, um das Gleichgewicht zwischen Preis und Leistung für Ihren Cluster zu wahren. Wenn Sie einen zusätzlichen Knoten anfragen, übernimmt Amazon Redshift alle Details der Bereitstellung, des Load Balancings und der Datenpflege. Weitere Informationen zur Clusterleistung finden Sie unter Überwachen der Amazon-Redshift-Cluster-Leistung.

Reservierte Knoten eignen sich für kontinuierliche Produktions-Workloads und bieten erhebliche Einsparungen gegenüber On-Demand-Preisen. Sie können reservierte Knoten erwerben, nachdem Sie Experimente durchgeführt und proof-of-concepts Ihre Produktionskonfiguration validiert haben. Weitere Informationen finden Sie unter Kaufen reservierter Amazon-Redshift-Knoten.

Wenn Sie einen Cluster anhalten, unterbrechen Sie die On-Demand-Abrechnung während der Zeit, in der der Cluster angehalten ist. Während dieser angehaltenen Zeit zahlen Sie nur für den Sicherungsspeicher. So müssen Sie Data Warehouse-Kapazitäten nicht planen und kaufen, bevor Sie sie tatsächlich benötigen. Dies ist kostengünstiger und einfacher, und Sie können preisgünstig Umgebungen zu Entwicklungs- oder Testzwecken verwalten.

Weitere Informationen zur Preisgestaltung von On-Demand-Knoten und reservierten Knoten finden Sie unter Amazon Redshift – Preise.

Verwenden von EC2-VPC beim Erstellen Ihres Clusters

Amazon-Redshift-Cluster werden in Amazon-EC2-Instances ausgeführt, die für den von Ihnen ausgewählten Amazon-Redshift-Knotentyp und die -Größe konfiguriert sind. Erstellen Sie Ihren Cluster mit EC2-VPC. Wenn Sie weiterhin EC2-Classic verwenden, empfehlen wir Ihnen, EC2-VPC zu verwenden, um die Leistung und Sicherheit zu verbessern. Weitere Informationen zu den unterstützten Netzwerkplattformen finden Sie unter Supported Platforms (Unterstützte Plattformen) im Amazon-EC2-Benutzerhandbuch für Linux-Instances. Ihre AWS Kontoeinstellungen bestimmen, ob EC2-VPC oder EC2-Classic für Sie verfügbar sind.

> **Note**
>
> Um Verbindungsprobleme zwischen SQL-Client-Tools und der Amazon-Redshift-Datenbank zu vermeiden, empfehlen wir, einen der folgenden Schritte auszuführen. Sie können eine eingehende Regel konfigurieren, die dem Host die Aushandlung der Paketgröße ermöglicht. Alternativ können Sie TCP/IP-Jumbo-Frames deaktivieren, indem Sie die MTU (Maximum Transmission Unit) auf dem Netzwerkinterface (NIC) Ihrer Amazon-EC2-Instances auf 1500 setzen. Weitere Informationen zu diesen Verfahren finden Sie unter Abfragen scheinen zu hängen und erreichen manchmal den Cluster nicht.

EC2-VPC

Wenn Sie EC2-VPC verwenden, wird Ihr Cluster in einer Virtual Private Cloud (VPC) ausgeführt, die logisch von Ihrem Konto isoliert ist. AWS Wenn Sie Ihren Cluster in der EC2-VPC bereitstellen, steuern Sie den Zugriff auf Ihren privaten Cluster dadurch, dass Sie dem Cluster eine oder mehrere VPC-Sicherheitsgruppen zuweisen. Weitere Informationen finden Sie unter Sicherheitsgruppen für Ihre VPC im Amazon VPC Benutzerhandbuch.

Zur Erstellung eines Clusters in einer VPC müssen Sie zuerst eine Amazon-Redshift-Cluster-Subnetzgruppe erstellen, indem Sie die Subnetzinformationen Ihrer VPC angeben und dann die Subnetzgruppe bereitstellen, wenn Sie den Cluster starten. Weitere Informationen finden Sie unter Amazon-Redshift-Cluster-Subnetzgruppen.

Weitere Informationen zu Amazon Virtual Private Cloud (Amazon VPC) finden Sie auf der Produktdetailseite zu Amazon VPC.

EC2-Classic

Die EC2-Classic-Plattform wird am 15. August 2022 außer Betrieb genommen. Wir empfehlen , Ihre Cluster von der EC2-Classic-Plattform auf eine EC2-VPC-Plattform zu migrieren. Weitere Informationen finden Sie unter Aktualisieren eines DS2-Clusters auf EC2-Classic auf EC2-VPC und unter EC2-Classic-Networking geht in den Ruhestand – So bereiten Sie sich vor.

In EC2-Classic läuft Ihr Cluster in einem einzigen, flachen Netzwerk, das Sie mit anderen Kunden teilen. AWS Wenn Sie Ihren Cluster in EC2-Classic bereitstellen, steuern Sie den Zugriff auf Ihren privaten Cluster dadurch, dass Sie dem Cluster eine oder mehrere Amazon-Redshift-Cluster-Sicherheitsgruppen zuweisen. Weitere Informationen finden Sie unter Amazon-Redshift-Cluster-Sicherheitsgruppen.

Starten Sie einen Cluster.

Ihr AWS Konto kann entweder Instances von EC2-VPC und EC2-Classic oder nur EC2-VPC auf einer Basis starten. region-by-region Um festzustellen, welche Netzwerkplattform Ihr Konto unterstützt, und dann einen Cluster zu starten, gehen Sie wie folgt vor:

1. Entscheiden Sie, in welcher Region Sie einen Cluster AWS bereitstellen möchten. Eine Liste der AWS Regionen, in denen Amazon Redshift verfügbar ist, finden Sie unter Amazon Redshift Redshift-Endpoints in der. Allgemeine Amazon Web Services-Referenz
2. Bringen Sie in Erfahrung, welche Amazon-EC2-Plattformen Ihr Konto in der ausgewählten AWS -Region unterstützt. Sie finden diese Informationen in der Amazon-EC2-Konsole. step-by-stepAnweisungen finden Sie unter Unterstützte Plattformen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.
3. Wenn Ihr Konto beide Plattformen unterstützt, empfehlen wir EC2-VPC. Wenn Ihr Konto nur EC2-VPC unterstützt, müssen Sie Ihren Cluster in einer VPC bereitstellen.

4. Starten Sie Ihren Amazon-Redshift-Cluster. Sie können einen Cluster mithilfe der Amazon Redshift Redshift-Konsole oder mithilfe der Amazon Redshift Redshift-API oder AWS CLI SDK-Bibliotheken erstellen. Weitere Informationen zu diesen Optionen und Links zu der jeweiligen Dokumentation finden Sie unter Was ist Amazon Redshift?.

Standard-Festplattenspeicherplatzalarm

Wenn Sie einen Amazon Redshift Redshift-Cluster erstellen, können Sie optional einen CloudWatch Amazon-Alarm konfigurieren, um den durchschnittlichen Prozentsatz des Festplattenspeichers zu überwachen, der von allen Knoten in Ihrem Cluster genutzt wird. Wir bezeichnen diesen Alarm als Standard-Festplattenspeicherplatzalarm.

Der Standard-Festplattenspeicherplatzalarm dient dazu, Ihnen bei der Überwachung der Speicherkapazität Ihres Clusters zu helfen. Sie können diesen Alarm auf der Grundlage der Anforderungen Ihres Data Warehouses konfigurieren. Sie können die Warnung z. B. als Anzeichen dafür verwenden, dass Sie die Größe Ihres Clusters anpassen müssen. Sie können die Größe entweder auf einen anderen Knotentyp oder durch die Hinzufügung weiterer Knoten anpassen oder reservierte Knoten kaufen, um die zukünftige Erweiterung des Clusters zu unterstützen.

Der Standard-Festplattenspeicherplatzalarm wird ausgelöst, wenn die Festplattennutzung einen bestimmten Prozentsatz mit einer bestimmten Häufigkeit und für eine bestimmte Dauer erreicht oder überschreitet. Standardmäßig wird dieser Alarm ausgelöst, wenn der von Ihnen angegebene Prozentsatz erreicht wird und für fünf Minuten oder länger bestehen bleibt oder überschritten wird. Sie können die Standardwerte nach dem Start des Clusters bearbeiten.

Wenn der CloudWatch Alarm ausgelöst wird, sendet Amazon Simple Notification Service (Amazon SNS) eine Benachrichtigung an bestimmte Empfänger, um sie zu warnen, dass der prozentuale Schwellenwert erreicht ist. Amazon SNS verwendet ein Thema für die Angabe der Empfänger und der Nachricht, die in einer Benachrichtigung gesendet wird. Sie können dazu ein vorhandenes Amazon-SNS-Thema verwenden; andernfalls wird ein Thema auf der Grundlage der von Ihnen beim Start des Clusters angegebenen Einstellungen erstellt. Sie können das Thema für diesen Alarm nach dem Start des Clusters bearbeiten. Weitere Informationen zum Erstellen von Amazon-SNS-Themen erhalten Sie unter Erste Schritte mit Amazon Simple Notification Service.

Nachdem Sie den Cluster gestartet haben, können Sie den Alarm im Statusfenster des Clusters unter CloudWatch Alarme anzeigen und bearbeiten. *Der Name lautet* ***percentage-disk-space-used-default-<*** *string* ***>.*** Sie können den Alarm öffnen, um das damit verbundene Amazon-SNS-Thema anzuzeigen und die Alarmeinstellungen zu bearbeiten. Wenn Sie kein vorhandenes

Amazon SNS SNS-Thema zur Verwendung ausgewählt haben, trägt das für Sie erstellte Thema den Namen < ***clustername*** >-default-alarms (< ***recipient*** >), zum Beispiel (notify@example.com). examplecluster-default-alarms

Für weitere Informationen zur Konfiguration und Bearbeitung des Standard-Festplattenspeicherplatzalarm vgl. Erstellen eines Clusters und Erstellen oder Bearbeiten eines Speicherplatzalarms.

> **Note**
>
> Wenn Sie Ihren Cluster löschen, wird der damit verbundene Alarm nicht gelöscht, jedoch nicht mehr ausgelöst. Sie können den Alarm von der Konsole löschen, wenn Sie ihn nicht mehr benötigen CloudWatch .

Cluster-Status

Der Cluster-Status zeigt den aktuellen zustand des Clusters an. Die folgende Tabelle enthält Beschreibungen für alle Cluster-Status.

Status	Description
`available`	Der Cluster läuft und ist verfügbar.
`available, prep-for-resize`	Der Cluster wird gerade für die elastische Größenanpassung vorbereit et. Der Cluster wird ausgeführt und ist für Lese- und Schreibabfragen verfügbar, aber Clusteroperationen wie das Erstellen eines Snapshots stehen nicht zur Verfügung.
`available, resize-cleanup`	Eine Operation zur elastischen Größenanpassung überträgt gerade Daten an die neuen Clusterknoten. Der Cluster wird ausgeführt und ist für Lese- und Schreibabfragen verfügbar, aber Clusteroperationen wie das Erstellen eines Snapshots stehen nicht zur Verfügung.
`cancelling-resize`	Die Größenänderung wird abgebrochen.
`creating`	Amazon Redshift erstellt den Cluster. Weitere Informationen finden Sie unter Erstellen eines Clusters.

Status	Description
`deleting`	Amazon Redshift löscht den Cluster. Weitere Informationen finden Sie unter Löschen eines Clusters.
`final-snapshot`	Amazon Redshift erstellt einen abschließenden Snapshot des Clusters, bevor dieser gelöscht wird. Weitere Informationen finden Sie unter Löschen eines Clusters.
`hardware-failure`	Der Cluster ist von einem Hardwareausfall betroffen. Wenn Sie einen Single Node-Cluster haben, kann der Knoten nicht ersetzt werden. Um Ihren Cluster zurückzuerhalten, müssen Sie einen Snapshot wiederherstellen. Weitere Informationen finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.
`incompatible-hsm`	Amazon Redshift kann keine Verbindung zum Hardware Security Module (HSM) herstellen. Überprüfen Sie die HSM-Konfiguration zwischen dem Cluster und dem HSM. Weitere Informationen finden Sie unter Verschlüsselung für Amazon Redshift mit Hardwaresicherheitsmodulen.
`incompatible-network`	Es liegt ein Problem mit der zugrunde liegenden Netzwerkkonfiguration vor. Stellen Sie sicher, dass die VPC, in der Sie den Cluster gestartet haben, vorhanden ist, und dass ihre Einstellungen korrekt sind. Weitere Informationen finden Sie unter Verwaltung von Clustern in einer VPC.
`incompatible-parameters`	Es liegt ein Problem mit einem oder mehreren Parameterwerten in der zugehörigen Parametergruppe vor, und der/die Parameterwert(e) kann/können nicht angewendet werden. Modifizieren Sie die Parameter gruppe, und aktualisieren Sie alle ungültigen Werte. Weitere Informationen finden Sie unter Amazon-Redshift-Parametergruppen.
`incompatible-restore`	Bei der Wiederherstellung des Clusters aus dem Snapshot ist ein Problem aufgetreten. Versuchen Sie, den Cluster erneut aus einem anderen Snapshot wiederherzustellen. Weitere Informationen finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.
`modifying`	Amazon Redshift wendet Änderungen auf den Cluster an. Weitere Informationen finden Sie unter Modifizieren eines Clusters.

Status	Description
`paused`	Der Cluster wird angehalten. Weitere Informationen finden Sie unter Anhalten und Fortsetzen von Clustern.
`rebooting`	Amazon Redshift startet den Cluster neu. Weitere Informationen finden Sie unter Neustart eines Clusters.
`renaming`	Amazon Redshift wendet einen neuen Namen auf den Cluster an. Weitere Informationen finden Sie unter Umbenennen von Clustern.
`resizing`	Amazon Redshift gibt eine neue Größe für den Cluster an. Weitere Informationen finden Sie unter Größenanpassung eines Clusters.
`rotating-keys`	Amazon Redshift rotiert Verschlüsselungsschlüssel für den Cluster. Weitere Informationen finden Sie unter Rotation von Verschlüsselungsschlüsseln in Amazon Redshift.
`storage-full`	Der Cluster hat seine Speicherkapazität erreicht. Passen Sie die Größe des Clusters an, oder wählen Sie eine andere Knotengröße. Weitere Informationen finden Sie unter Größenanpassung eines Clusters.
`updating-hsm`	Amazon Redshift aktualisiert die HSM-Konfiguration.

Überlegungen zur Verwendung von von Amazon Redshift bereitgestellten Clustern

Nach der Erstellung Ihres Clusters finden Sie in diesem Abschnitt Informationen zu Regionen, in denen Funktionen verfügbar sind, zu Wartungsaufgaben, Knotentypen und Nutzungsbeschränkungen.

Themen

- Überlegungen zu Regionen und Availability Zones
- Clusterwartung
- Verwalten von Nutzungslimits in Amazon Redshift
- Netzwerkfunktionen, die von RA3-Knoten unterstützt werden

- Knotentypen

Überlegungen zu Regionen und Availability Zones

Amazon Redshift ist in mehreren AWS Regionen verfügbar. Standardmäßig stellt Amazon Redshift Ihren Cluster in einer zufällig ausgewählten Availability Zone (AZ) innerhalb der von Ihnen ausgewählten AWS Region bereit. Alle Knoten des Clusters werden in derselben Availability Zone bereitgestellt.

Sie können optional eine bestimmte Availability Zone anfordern, wenn in dieser Zone Amazon Redshift verfügbar ist. Zum Beispiel: Wenn Sie bereits eine Amazon-EC2-Instance in einer Availability Zone ausführen, sollten Sie Ihren Amazon-Redshift-Cluster auch in dieser Zone erstellen, um die Latenz zu reduzieren. Andererseits können Sie eine andere Availability Zone für höhere Verfügbarkeit wählen. Amazon Redshift ist möglicherweise nicht in allen Availability Zones innerhalb einer AWS Region verfügbar.

Eine Liste der unterstützten AWS Regionen, in denen Sie einen Amazon Redshift Redshift-Cluster bereitstellen können, finden Sie unter Amazon Redshift Redshift-Endpoints in der. Allgemeine Amazon Web Services-Referenz

Clusterwartung

Amazon Redshift führt periodisch Wartungsaktivitäten durch, um Upgrades auf Ihren Cluster anzuwenden. Während dieser Aktualisierungen ist Ihr Amazon-Redshift-Cluster nicht für den Normalbetrieb verfügbar. Sie haben verschiedene Möglichkeiten zu steuern, wie wir Ihr Cluster warten. Sie können beispielsweise den Zeitpunkt der Bereitstellung von Updates für Ihre Cluster kontrollieren. Sie können auch auswählen, ob in Ihrem Cluster die neueste oder die zweitneueste Version ausgeführt wird. Schließlich können Sie noch einstellen, dass optionale Wartungsupdates eine Weile zurückgestellt werden.

Themen

- Wartungsfenster
- Aufschieben der Wartung
- Auswählen des Cluster-Wartungspfads
- Verwalten von Cluster-Versionen
- Rollback der Cluster-Version
- Ermitteln der Cluster-Wartungsversion

Wartungsfenster

Amazon Redshift weist nach dem Zufallsprinzip ein 30-minütiges Wartungsfenster aus einem 8-Stunden-Zeitblock pro AWS Region zu, das an einem zufälligen Wochentag (Montag bis einschließlich Sonntag) stattfindet.

Standardwartungsfenster

Die folgende Liste zeigt die Zeitblöcke für jede AWS Region, aus der die Standard-Wartungsfenster zugewiesen werden:

- Region USA Ost (Nord-Virginia): 03.00 bis 11.00 Uhr (UTC)
- Region USA Ost (Ohio): 03.00 bis 11.00 Uhr (UTC)
- Region USA West (Nordkalifornien): 06.00 bis 14.00 Uhr (UTC)
- Region USA West (Oregon): 06.00 bis 14.00 Uhr (UTC)
- Region Afrika (Kapstadt): 20.00 bis 04.00 Uhr (UTC)
- Region Asien-Pazifik (Hongkong): 13.00 bis 21.00 Uhr (UTC)
- Region Asien-Pazifik (Hyderabad): 16.30 bis 00.30 Uhr (UTC)
- Region Asien-Pazifik (Jakarta): 15.00 bis 23.00 Uhr (UTC)
- Region Asien-Pazifik (Melbourne): 12.00 bis 20.00 Uhr (UTC)
- Region Asien-Pazifik (Mumbai): 16.30 bis 00.30 Uhr (UTC)
- Region Asien-Pazifik (Osaka): 13.00 bis 21.00 Uhr (UTC)
- Region Asien-Pazifik (Seoul): 13.00 bis 21.00 Uhr (UTC)
- Region Asien-Pazifik (Singapur): 14.00 bis 22.00 Uhr (UTC)
- Region Asien-Pazifik (Sydney): 12.00 bis 20.00 Uhr (UTC)
- Region Asien-Pazifik (Tokio): 13.00 bis 21.00 Uhr (UTC)
- Region Kanada (Zentral): 03.00 bis 11.00 Uhr (UTC)
- Region Kanada West (Calgary): 04:00–12:00 Uhr UTC
- Region China (Peking): 13.00 bis 21.00 Uhr (UTC)
- Region China (Ningxia): 13.00 bis 21.00 Uhr (UTC)
- Region Europa (Frankfurt): 06.00 bis 14.00 Uhr (UTC)
- Region Europa (Irland): 22.00 bis 06.00 Uhr (UTC)
- Region Europa (London): 22.00 bis 06.00 Uhr (UTC)

- Region Europa (Mailand): 21.00 bis 05.00 Uhr (UTC)
- Region Europa (Paris): 23.00 bis 07.00 Uhr (UTC)
- Region Europa (Stockholm): 23.00 bis 07.00 Uhr (UTC)
- Region Europa (Zürich): 20.00 bis 04.00 Uhr (UTC)
- Region Israel (Tel Aviv): 20:00–04:00 Uhr UTC
- Region Europa (Spanien): 21.00 bis 05.00 Uhr (UTC)
- Region Naher Osten (Bahrain): 13.00 bis 21.00 Uhr (UTC)
- Region Naher Osten (VAE): 18:00 bis 02:00 Uhr (UTC)
- Region Südamerika (São Paulo): 19.00 bis 03.00 Uhr (UTC)

Wenn ein Wartungsereignis für eine bestimmte Woche geplant ist, wird es in dem zugewiesenen 30-minütigen Wartungsfenster gestartet. Während Amazon Redshift die Wartung durchführt, beendet es alle Abfragen und anderen ausgeführten Operationen. Die meisten Wartungsaktivitäten werden innerhalb des 30-minütigen Wartungsfensters abgeschlossen. Einige können jedoch auch nach dem Schließen des Fensters fortgesetzt werden. Wenn während des geplanten Wartungsfensters keine Wartungsaktivitäten auszuführen sind, wird Ihr Cluster bis zum nächsten geplanten Wartungsfenster normal weiterbetrieben.

Sie können das geplante Wartungsfenster ändern, indem Sie den Cluster modifizieren, entweder auf programmatischem Wege oder mit der Amazon-Redshift-Konsole. Auf der Registerkarte Wartung finden Sie das Wartungsfenster und können den Tag und die Uhrzeit der Ausführung für den Cluster festlegen.

Es ist möglich, dass ein Cluster außerhalb eines Wartungsfensters neu gestartet wird. Es gibt mehrere Gründe, warum dies geschehen kann. Ein häufiger Grund ist, dass ein Problem mit dem Cluster festgestellt wurde und Wartungsarbeiten durchgeführt werden, um den Cluster wieder in einen fehlerfreien Zustand zu versetzen. Weitere Informationen finden Sie hier: Warum wurde mein Amazon-Redshift-Cluster außerhalb des Wartungsfensters neu gestartet? Dort werden die Gründe dafür detailliert beschrieben.

Aufschieben der Wartung

Um den Zeitplan für das Wartungsfenster Ihres Clusters zu ändern, können Sie die Wartung um bis zu 45 Tage aufschieben. Beispiel: Wenn Ihr Wartungsfenster auf Mittwoch, 08:30–09:00 Uhr UTC festgelegt ist, Sie aber zu dieser Zeit auf den Cluster zugreifen müssen, können Sie die Wartung aufschieben.

Wenn Sie die Wartung verschieben, wendet Amazon Redshift weiterhin Hardware-Updates oder andere obligatorische Sicherheitsupdates auf Ihren Cluster an. Während dieser Aktualisierungen ist Ihr Cluster nicht verfügbar.

Wenn während des bevorstehenden Wartungsfensters ein Hardware-Update oder ein anderes obligatorisches Sicherheitsupdate geplant ist, sendet Ihnen Amazon Redshift Vorabbenachrichtigungen in der Kategorie Ausstehend. Weitere Informationen zu Benachrichtigungen über ausstehende Ereignisse finden Sie unter Ereignisbenachrichtigungen zu Amazon Redshift.

Zum Senden und Empfangen von SMS-Benachrichtigungen können Sie den Amazon Simple Notification Service (Amazon SNS) verwenden. Weitere Informationen zum Abonnieren von Amazon-RDS-Ereignisbenachrichtigungen finden Sie unter Abonnieren von Cluster-Ereignisbenachrichtigungen von Amazon Redshift.

Wenn Sie die Wartung Ihres Clusters aufschieben, ist das auf den Aufschub folgende Wartungsfenster obligatorisch und kann nicht seinerseits verschoben werden.

> **Note**
>
> Es ist nicht möglich, eine bereits begonnene Wartung aufzuschieben.

Weitere Informationen zur Cluster-Wartung finden Sie in der folgenden Dokumentation:

- Wartungsfenster
- Verwalten von Clustern mithilfe der Konsole
- Modifizieren eines Clusters

Auswählen des Cluster-Wartungspfads

Wenn Amazon Redshift eine neue Clusterversion veröffentlicht, wird Ihr Cluster in seinem Wartungsfenster aktualisiert. Sie können angeben, ob der Cluster auf die zuletzt freigegebene oder die vorherige Version aktualisiert wird.

Welche Clusterversion in einem Wartungszeitraum installiert wird, wird über den Wartungspfad gesteuert. Wenn Amazon Redshift eine neue Clusterversion veröffentlicht, wird diese Version dem aktuellen Pfad zugewiesen, und die Vorversion dem nachgestellten Pfad. Geben Sie einen der folgenden Werte an, um den Wartungspfad für den Cluster festzulegen:

- Current (Aktuell) – Es wird die aktuellste genehmigte Clusterversion verwendet.
- Trailing (Nachgestellt) – Es wird die letzte Clusterversion vor der aktuellen Version verwendet.
- Preview (Vorversion) – Verwenden Sie die Cluster-Version mit neuen Vorversionsfunktionen.

Angenommen, Ihr Cluster verwendet derzeit die Version 1.0.2762 und die aktuelle Amazon-Redshift-Version ist 1.0.3072. Wenn Sie Current (Aktuelle) als Wartungspfad festlegen, wird der Cluster im nächsten Wartungsfenster auf Version 1.0.3072 (die nächste freigegebene Version) aktualisiert. Wenn Sie den Wartungspfad des Clusters auf Trailing (Vorhergehende) setzen, wird der Cluster erst aktualisiert, sobald eine neue Version nach 1.0.3072 veröffentlicht wurde.

Preview tracks (Preview-Tracks

Ein Preview-Track steht möglicherweise nicht immer zur Auswahl. Wenn Sie einen Preview-Track auswählen, muss auch ein Trackname ausgewählt werden. Vorversionspfade und die damit verbundenen Ressourcen sind temporär, haben funktionale Einschränkungen und enthalten möglicherweise nicht alle aktuellen Amazon-Redshift-Funktionen, die in anderen Pfaden verfügbar sind. Bei der Arbeit mit Preview-Tracks:

- Verwenden Sie die neue Amazon-Redshift-Konsole, wenn Sie mit Vorversionspfaden arbeiten. Beispielsweise wenn Sie einen Cluster erstellen, der mit Vorversionsfunktionen verwendet werden soll.
- Sie können einen Cluster nicht von einem Preview-Track zum anderen wechseln.
- Sie können einen Cluster nicht von einem aktuellen oder nachfolgenden Track zu einem Preview-Track wechseln.
- Sie können einen Cluster nicht von einem Preview-Track zu einem aktuellen oder nachfolgenden Track wechseln.
- Sie können nicht von einem Snapshot wiederherstellen, der aus einem anderen Preview-Track erstellt wurde.
- Sie können den Preview-Track nur beim Erstellen eines neuen Clusters oder beim Wiederherstellen aus einem Snapshot verwenden.
- Sie können nicht von einem Snapshot wiederherstellen, der aus einem anderen Preview-Track oder mit einer Cluster-Wartungsversion erstellt wurde, die neuer ist als die Preview-Track-Cluster-Version. Wenn Sie beispielsweise einen Cluster in einem Preview-Track wiederherstellen, können Sie nur einen Snapshot verwenden, der aus einer älteren Cluster-Wartungsversion als dem Preview-Track erstellt wurde.

Umschalten zwischen Wartungspfaden

Das Ändern des Pfads für einen Cluster ist normalerweise eine einmalige Entscheidung. Sie sollten beim Ändern des Wartungspfads vorsichtig vorgehen. Wenn Sie den Wartungspfad von Trailing (Vorhergehende) in Current (Aktuelle) ändern, wird der Cluster im nächsten Wartungsfenster auf die Releaseversion des Pfades Current (Aktuelle) gesetzt. Wenn Sie nun den Wartungspfad des Clusters in Trailing (Vorhergehende) ändern, wird der Cluster erst dann aktualisiert, wenn nach der Releaseversion des Pfades Current (Aktuelle) eine neue Version veröffentlicht wird.

Wartungspfade und Wiederherstellung

Snapshot erben den Wartungspfad des Quellclusters. Wenn Sie den Wartungspfad des Quellclusters ändern, nachdem Sie einen Snapshot erstellt haben, ist der Wartungspfad des Snapshots ein anderer als der des Quellclusters. Wenn Sie mit dem Snapshot eine Wiederherstellung vornehmen, befindet sich der neue Cluster auf dem Wartungspfad, der vom Quellcluster übernommen wurde. Sie können den Wartungspfad ändern, nachdem die Wiederherstellung abgeschlossen ist. Eine Größenänderung des Clusters wirkt sich nicht auf seinen Wartungspfad aus.

Verwalten von Cluster-Versionen

Ein Wartungspfad ist als eine Reihe von Releases definiert. Sie können für einen Cluster als Wartungspfad die aktuellen Versionen oder deren Vorversionen festlegen. Wenn Sie für Ihren Cluster Current (Aktuelle) als Wartungspfad festlegen, wird der Cluster in seinem nächsten Wartungsfenster auf die neueste freigegebene Version aktualisiert. Wenn Sie für Ihren Cluster Trailing (Vorherige) als Wartungspfad festlegen, wird der Cluster stets in der letzten Vorversion vor der neuesten Version ausgeführt.

Die Spalte Release status (Release-Status) in der Amazon-Redshift-Konsolenliste der Cluster zeigt an, ob einer Ihrer Cluster für ein Upgrade verfügbar ist.

Rollback der Cluster-Version

Wenn Ihr Cluster die aktuelle Cluster-Version ist, können Sie ein Rollback auf die vorherige Version auswählen.

Ausführliche Informationen über Funktionen und Verbesserungen der jeweiligen Cluster-Version finden Sie unter Cluster-Versionsverlauf.

So führen Sie ein Rollback zu einer früheren Cluster-Version durch

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus.
3. Wählen Sie den Cluster aus, der zurückgesetzt werden soll.
4. Wählen Sie für Actions (Aktionen) Roll back cluster version (Rollback der Cluster-Version) aus. Die Seite Roll back cluster version (Cluster-Version-Rollback) wird angezeigt.
5. Wenn es eine Version für den Rollback gibt, folgen Sie den Anweisungen auf der Seite.
6. Wählen Sie Roll back now (Jetzt Rollback durchführen) aus.

Ermitteln der Cluster-Wartungsversion

Sie können die Amazon-Redshift-Engine und Datenbankversion mithilfe der Amazon-Redshift-Konsole ermitteln.

So finden Sie die Version eines Clusters:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster-Namen aus der Liste aus, um die Details zu dem Cluster aufzurufen. Die Details des Clusters werden möglicherweise einschließlich der Registerkarten Cluster performance (Cluster-Leistung), Query monitoring (Abfrageüberwachung), Databases (Datenbanken), Datashares (Datenaustausche), Schedules (Zeitpläne), Maintenance (Wartung) und Properties (Eigenschaften) angezeigt.
3. Wählen Sie die Registerkarte Maintenance (Wartung) für weitere Details aus.
4. Suchen Sie im Abschnitt Maintenance (Wartung) nach Current cluster version (Aktuelle Clusterversion).

> **Note**
>
> Obwohl die Konsole diese Informationen in einem Feld anzeigt, sind dies zwei Parameter in der Amazon-Redshift-API, `ClusterVersion` und `ClusterRevisionNumber`. Weitere Informationen finden Sie unter Cluster in der API-Referenz von Amazon Redshift.

Verwalten von Nutzungslimits in Amazon Redshift

Sie können Limits definieren, um Ihre Nutzung und die damit verbundenen Kosten einiger Amazon-Redshift-Funktionen zu überwachen und zu kontrollieren. Sie können tägliche, wöchentliche und monatliche Nutzungslimits erstellen und Aktionen definieren, die Amazon Redshift automatisch ausführt, wenn diese Limits erreicht werden. Zu den Aktionen gehören beispielsweise das Protokollieren eines Ereignisses in einer Systemtabelle, um jegliche Nutzung zu erfassen, die Ihre definierten Limits überschreitet. Weitere mögliche Aktionen sind das Auslösen von Warnungen mit Amazon SNS und Amazon CloudWatch, um einen Administrator zu benachrichtigen, und das Deaktivieren der weiteren Nutzung zur Kostenkontrolle.

Sie können Nutzungslimits für jeden Cluster definieren. Nachdem Ihr Cluster erstellt wurde, können Sie Nutzungslimits für die folgenden Features definieren:

- Amazon Redshift Spectrum
- Amazon-Redshift-Nebenläufigkeitsskalierung
- Regionsübergreifende Amazon-Redshift-Datenfreigabe

Nutzungslimits sind ab Version 1.0.14677 in den AWS-Regionen verfügbar, in denen Amazon Redshift Spectrum und die Amazon-Redshift-Nebenläufigkeitsskalierung verfügbar sind.

Ein Redshift-Spectrum-Limit gibt den Schwellenwert für die Gesamtmenge der gescannten Daten in 1-TB-Schritten an. Ein Limit für die Nebenläufigkeitsskalierung gibt in 1-Minuten-Schritten den Schwellenwert für die von der Nebenläufigkeitsskalierung benötigte Gesamtdauer an. Ein Limit für die regionsübergreifende Datenfreigabe gibt den Schwellenwert für die Gesamtmenge der gescannten Daten in 1-TB-Schritten an.

Ein Limit kann für einen täglichen, wöchentlichen oder monatlichen Zeitraum festgelegt werden (zum Bestimmen von Anfang und Ende des Zeitraums wird UTC verwendet). Wenn Sie während eines Zeitraums ein Limit erstellen, wird das Limit von diesem Zeitpunkt bis zum Ende des Zeitraums gemessen. Wenn Sie beispielsweise am 15. März ein monatliches Limit erstellen, wird der erste Monatszeitraum vom 15. März bis zum 31. März gemessen.

Sie können für jedes Feature mehrere Nutzungslimits definieren. Jedes Limit kann eine andere Aktion haben. Folgende Aktionen sind möglich:

- Log to system table (In Systemtabelle protokollieren): Dies ist die Standardaktion. Die Informationen werden in der Tabelle STL_USAGE_CONTROL protokolliert. Die Protokollierung

ist hilfreich, wenn die bisherige Nutzung ausgewertet wird und zukünftige Nutzungslimits festgelegt werden. Weitere Informationen zu den protokollierten Informationen finden Sie unter STL_USAGE_CONTROL im Datenbankentwicklerhandbuch zu Amazon Redshift.

- Alert (Warnung): Amazon Redshift gibt CloudWatch-Metriken für die verfügbare und die verbrauchte Nutzung aus. Sie können für jede Funktion bis zu drei Nutzungslimits definieren. Wenn Sie die Warnungsaktion über die Amazon-Redshift-Konsole aktivieren, wird automatisch ein CloudWatch-Alarm für diese Metriken erstellt. Sie können optional ein Amazon-SNS-Abonnement an diesen Alarm anhängen. Wenn Sie einen AWS CLI- oder API-Vorgang verwenden, erstellen Sie den CloudWatch-Alarm unbedingt manuell. Wenn der Schwellenwert erreicht ist, werden Ereignisse auch in einer Systemtabelle protokolliert.
- Disable feature (Deaktivierungsfunktion): Wenn der Schwellenwert erreicht ist, deaktiviert Amazon Redshift die Funktion, bis das Kontingent für den nächsten Zeitraum (täglich, wöchentlich oder monatlich) aktualisiert wird. Die Deaktivierungsaktion kann nur ein Limit für jede Funktion haben. Ereignisse werden auch in einer Systemtabelle protokolliert. Warnungen können ausgegeben werden.

Nutzungslimits bleiben bestehen, bis die Definition der Nutzungslimits selbst oder der Cluster gelöscht wird.

Sie können Nutzungslimits mit der neuen Amazon-Redshift-Konsole, der AWS CLI oder mithilfe von Amazon-Redshift-API-Vorgängen definieren und verwalten. Um ein Limit in der Amazon-Redshift-Konsole zu definieren, navigieren Sie zu Ihrem Cluster und wählen für Actions (Aktionen) Configure usage limit (Nutzungslimit konfigurieren) aus. Um zuvor definierte Nutzungslimits für Ihren Cluster anzuzeigen, navigieren Sie zu Ihrem Cluster und wählen die Registerkarte Maintenance (Wartung) im Bereich Usage limits (Nutzungslimits) aus. Navigieren Sie zu Ihrem Cluster, um die verfügbare und verbrauchte Nutzung für Ihren Cluster anzuzeigen. Wählen Sie die Registerkarte Cluster performance (Clusterleistung) aus und zeigen Sie dann die Diagramme zur Nutzung eines Features an.

Sie können zur Verwaltung von Nutzungslimits die folgenden Amazon-Redshift-CLI-Vorgänge verwenden. Weitere Informationen finden Sie in der AWS CLI-Befehlsreferenz.

- create-usage-limit
- describe-usage-limits
- modify-usage-limit
- delete-usage-limit

Sie können zur Verwaltung von Nutzungslimits die folgenden Amazon-Redshift-API-Vorgänge verwenden. Weitere Informationen finden Sie in der Amazon-Redshift-API-Referenz.

- CreateUsageLimit
- DescribeUsageLimits
- ModifyUsageLimit
- DeleteUsageLimit

Sehen Sie sich das folgende Video an, um zu erfahren, wie Sie Nutzungslimits mithilfe der Amazon-Redshift-Konsole erstellen und überwachen: Cost Controls for Amazon Redshift Spectrum and Concurrency Scaling.

Netzwerkfunktionen, die von RA3-Knoten unterstützt werden

RA3-Knoten unterstützen eine Reihe von Netzwerkfunktionen, die für DS2- oder DC2-Knoten nicht verfügbar sind. Dieser Abschnitt enthält kurze Beschreibungen der einzelnen Funktionen und Links zu zusätzlicher Dokumentation:

- VPC-Endpunkt für bereitgestellte Cluster — Wenn Sie einen RA3-Cluster erstellen oder wiederherstellen, verwendet Amazon Redshift einen Port im Bereich von 5431-5455 oder 8191-8215. Wenn der Cluster auf einen Port in einem dieser Bereiche eingestellt ist, erstellt Amazon Redshift automatisch einen VPC-Endpunkt in Ihrem AWS Konto für den Cluster und fügt ihm eine private IP-Adresse hinzu. Wenn Sie den Cluster auf öffentlich zugänglich einstellen, erstellt Redshift eine elastische IP-Adresse in Ihrem AWS Konto und fügt sie dem VPC-Endpunkt hinzu. Weitere Informationen finden Sie unter Konfiguration der Kommunikationseinstellungen für Sicherheitsgruppen für einen Amazon Redshift-Cluster oder eine Amazon Redshift Serverless-Arbeitsgruppe.
- RA3-Cluster mit einem einzigen Subnetz – Sie können einen RA3-Cluster mit einem einzigen Subnetz erstellen, dieser kann jedoch keine Notfallwiederherstellungs-Funktionen verwenden. Eine Ausnahme tritt auf, wenn Sie die Cluster-Verlagerung aktivieren und das Subnetz nicht über mehrere Availability Zones (AZs) verfügt.
- RA3-Cluster und Subnetzgruppen mit mehreren Subnetzen — Sie können einen RA3-Cluster mit mehreren Subnetzen erstellen, indem Sie bei der Bereitstellung des Clusters in Ihrer Virtual Private Cloud (VPC) eine Subnetzgruppe erstellen. Eine Cluster-Subnetzgruppe ermöglicht es Ihnen, eine Reihe von Subnetzen in Ihrer VPC anzugeben, und Amazon Redshift erstellt den Cluster in einem davon. Nachdem Sie eine Subnetzgruppe erstellt haben, können Sie Subnetze, die Sie zuvor

hinzugefügt haben, entfernen oder weitere hinzufügen. Weitere Informationen finden Sie unter Amazon Redshift Redshift-Cluster-Subnetzgruppen.

- Konto- oder VPC-übergreifender Endpunktzugriff — Sie können auf einen bereitgestellten Cluster oder eine Amazon Redshift Serverless-Arbeitsgruppe zugreifen, indem Sie einen von Redshift verwalteten VPC-Endpunkt einrichten. Sie können es als private Verbindung zwischen einer VPC, die einen Cluster oder eine Arbeitsgruppe enthält, und einer VPC einrichten, auf der Sie beispielsweise ein Client-Tool ausführen. Auf diese Weise können Sie auf das Data Warehouse zugreifen, ohne eine öffentliche IP-Adresse zu verwenden und ohne den Datenverkehr über das Internet weiterzuleiten. Weitere Informationen finden Sie unter Arbeiten mit von Redshift verwalteten VPC-Endpunkten.
- Cluster-Verlagerung — Sie können einen Cluster in eine andere Availability Zone (AZ) verschieben, ohne dass Daten verloren gehen, wenn es zu einer Betriebsunterbrechung kommt. Diesen Vorgang führen Sie in der Konsole durch. Weitere Informationen finden Sie unter Ihren Cluster verlagern.
- Benutzerdefinierter Domain-Name – Sie können für Ihren Amazon-Redshift-Cluster einen benutzerdefinierten Domain-Namen, auch als benutzerdefinierte URL bezeichnet, erstellen. Es ist ein easy-to-read DNS-Eintrag, der SQL-Client-Verbindungen an Ihren Cluster-Endpunkt weiterleitet. Weitere Informationen finden Sie unter Verwenden eines benutzerdefinierten Domain-Namens für Client-Verbindungen.

Knotentypen

In diesen Abschnitten werden die Aufgaben beschrieben, die für verschiedene Knotentypen verfügbar sind.

Themen

- RA3-Knoten
- DC2- und DS2-Knoten

RA3-Knoten

In diesen Abschnitten werden die Aufgaben beschrieben, die für RA3-Knoten verfügbar sind.

Themen

- Übersicht

- Migration zu RA3-Knotentypen

Übersicht

Es wird empfohlen, vorhandene Workloads, die auf DS2-Knotentypclustern ausgeführt werden, auf RA3-Knotentypen zu aktualisieren, um die Leistung zu verbessern und mehr Speicherkapazität zu erhalten. RA3-Knoten bieten folgende Vorteile:

- Sie sind flexibel, um Ihre Datenverarbeitungskapazität zu erweitern, ohne Ihre Speicherkosten zu erhöhen. Dazu skalieren sie Ihren Speicher ohne übermäßige Bereitstellung von Datenverarbeitungskapazität.
- Sie verwenden Hochleistungs-SSDs für Ihre heißen Daten und Amazon S3 für kalte Daten. So bieten sie Benutzerfreundlichkeit, kostengünstige Speicherung und hohe Abfrageleistung.
- Sie verwenden Netzwerke mit hoher Bandbreite, die auf dem AWS Nitro-System basieren, um die Zeit, die für das Auslagern und Abrufen von Daten in Amazon S3 benötigt wird, weiter zu reduzieren.

In folgenden Fällen sollten Sie erwägen, RA3-Knotentypen zu wählen:

- Sie benötigen Flexibilität, um Datenverarbeitungsleistung getrennt vom Speicher zu skalieren.
- Sie fragen einen Bruchteil Ihrer Gesamtdaten ab.
- Ihr Datenvolumen wächst schnell, oder es wird erwartet, dass es schnell wächst.
- Sie brauchen die Flexibilität, den Cluster nur auf Ihre Leistungsanforderungen zu skalieren.

Um RA3-Knotentypen verwenden zu können, muss Ihre AWS Region RA3 unterstützen. Weitere Informationen finden Sie unter Verfügbarkeit des RA3-Knotentyps in Regionen AWS.

> **Important**
>
> ra3.xlplus-Knotentypen können nur mit Cluster-Version 1.0.21262 oder höher verwendet werden. Sie können sich die Version eines vorhandenen Clusters mithilfe der Amazon-Redshift-Konsole anzeigen lassen. Weitere Informationen finden Sie unter Ermitteln der Cluster-Wartungsversion.
> Stellen Sie sicher, dass Sie beim Arbeiten mit RA3-Knotentypen die neue Amazon-Redshift-Konsole verwenden.

Um RA3-Knotentypen mit Amazon-Redshift-Operationen verwenden zu können, die den Wartungspfad verwenden, muss der Wert des Wartungspfads auf eine Clusterversion gesetzt werden, die RA3 unterstützt. Weitere Informationen zu Wartungspfaden finden Sie unter Auswählen des Cluster-Wartungspfads.

Berücksichtigen Sie Folgendes, wenn Sie RA3-Knotentypen mit nur einem Knoten verwenden.

- Datenfreigabe-Produzenten und -Konsumenten werden unterstützt.
- Zum Ändern der Knotentypen wird nur klassische Größenanpassung unterstützt. Das Ändern des Knotentyps mit elastischer Größenanpassung oder Snapshot-Wiederherstellung wird nicht unterstützt. Die folgenden Szenarien werden unterstützt:
  - Klassische Größenanpassung eines ds2.xlarge mit 1 Knoten zu einem ra3.xlplus mit 1 Knoten und umgekehrt.
  - Klassische Größenanpassung eines ds2.xlarge mit 1 Knoten zu einem ra3.xlplus mit mehreren Knoten und umgekehrt.
  - Klassische Größenanpassung eines ds2.xlarge mit mehreren Knoten zu einem ra3.xlplus mit 1 Knoten und umgekehrt.
  - Klassische Größenanpassung eines dc2.xlarge mit 1 Knoten zu einem ra3.xlplus mit 1 Knoten und umgekehrt.
  - Klassische Größenanpassung eines dc2.xlarge mit 1 Knoten zu einem ra3.xlplus mit mehreren Knoten und umgekehrt.
  - Klassische Größenanpassung eines dc2.xlarge mit mehreren Knoten zu einem ra3.xlplus mit 1 Knoten und umgekehrt.

Arbeiten mit von Amazon Redshift verwaltetem Speicher

Mit von Amazon Redshift verwaltetem Speicher können Sie alle Ihre Daten in Amazon Redshift speichern und verarbeiten und gleichzeitig mehr Flexibilität bei der getrennten Skalierung von Datenverarbeitungs- und Speicherkapazität erhalten. Sie speisen weiterhin Daten mit dem Befehl COPY (KOPIEREN) bzw. INSERT (EINFÜGEN) ein. Um die Leistung zu optimieren und die automatische Datenplatzierung über verschiedene Speicherebenen hinweg zu verwalten, nutzt Amazon Redshift Optimierungen wie die Datenblocktemperatur, das Datenblockalter und die Workload-Muster. Bei Bedarf skaliert Amazon Redshift die Lagerung automatisch auf Amazon S3, ohne dass manuelle Maßnahmen erforderlich sind.

Weitere Information zu Speicherkosten finden Sie unter Amazon Redshift – Preise.

Verwalten von RA3-Knotentypen

Um die Vorteile der Trennung von Datenverarbeitungsleistung und Speicher zu nutzen, können Sie Ihren Cluster mit dem RA3-Knotentyp erstellen oder aktualisieren. Um die RA3-Knotentypen zu verwenden, erstellen Sie Ihre Cluster in einer Virtual Private Cloud (EC2-VPC).

Führen Sie einen der folgenden Schritte aus, um die Anzahl der Knoten des Amazon-Redshift-Clusters mit einem RA3-Knotentyp zu ändern:

- Hinzufügen oder Entfernen von Knoten mit der elastischen Größenanpassung. In einigen Situationen ist das Entfernen von Knoten aus einem RA3-Cluster mit der elastischen Größenanpassung nicht zulässig. Dies ist beispielsweise der Fall, wenn bei einem Upgrade der 2:1 -Knotenanzahl die Anzahl der Slices pro Knoten auf 32 gesetzt wird. Weitere Informationen finden Sie unter Größenanpassung von Clustern. Wenn die elastische Größenanpassung nicht verfügbar ist, verwenden Sie die klassische Größenanpassung.
- Hinzufügen oder Entfernen von Knoten mit der klassischen Größenanpassung. Wählen Sie diese Option aus, wenn Sie die Konfiguration auf eine Größe ändern, die über die elastische Größenanpassung nicht verfügbar ist. Die elastische Größenanpassung ist schneller als die klassische Größenanpassung. Weitere Informationen finden Sie unter Größenanpassung von Clustern.

Verfügbarkeit des RA3-Knotentyps in Regionen AWS

Die RA3-Knotentypen sind nur in den folgenden AWS Regionen verfügbar:

- Region USA Ost (Nord-Virginia) (us-east-1)
- Region USA Ost (Ohio) (us-east-2)
- Region USA West (Nordkalifornien) (us-west-1)
- Region USA West (Oregon) (us-west-2)
- Region Afrika (Kapstadt) (af-south-1)
- Region Asien-Pazifik (Hongkong) (ap-east-1)
- Region Asien-Pazifik (Hyderabad) (ap-south-2)
- Region Asien-Pazifik (Jakarta) (ap-southeast-3)
- Region Asien-Pazifik (Melbourne) (ap-southeast-4)

- Region Asien-Pazifik (Mumbai) (ap-south-1)
- Region Asien-Pazifik (Osaka) (ap-northeast-3)
- Region Asien-Pazifik (Seoul) (ap-northeast-2)
- Region Asien-Pazifik (Singapur) (ap-southeast-1)
- Region Asien-Pazifik (Sydney) (ap-southeast-2)
- Region Asien-Pazifik (Tokio) (ap-northeast-1)
- Region Kanada (Zentral) (ca-central-1)
- Region Kanada West (Calgary) (ca-west-1)
- Region China (Peking) (cn-north-1)
- Region China (Ningxia) (cn-northwest-1)
- Region Europa (Frankfurt) (eu-central-1)
- Region Europa (Zürich) (eu-central-2)
- Region Europa (Irland) (eu-west-1)
- Region Europa (London) (eu-west-2)
- Region Europa (Mailand) (eu-south-1)
- Region Europa (Spanien) (eu-south-2)
- Region Europa (Paris) (eu-west-3)
- Region Europa (Stockholm) (eu-north-1)
- Region Israel (Tel Aviv) (il-central-1)
- Region Naher Osten (Bahrain) (me-south-1)
- Region Naher Osten (VAE) (me-central-1)
- Region Südamerika (São Paulo) (sa-east-1)
- AWS GovCloud (US-Ost) (us-gov-east-1)
- AWS GovCloud (US-West) (us-gov-west-1)

Migration zu RA3-Knotentypen

Um Ihren vorhandenen Knotentyp zu RA3 zu aktualisieren, haben Sie die folgenden Optionen, um den Knotentyp zu ändern:

- Die Wiederherstellung aus einem Snapshot – Amazon Redshift verwendet den neuesten Snapshot Ihres DS2- oder DC2-Clusters und stellt ihn wieder her, um einen neuen RA3-Cluster zu erstellen.

Sobald die Clustererstellung abgeschlossen ist (in der Regel innerhalb von Minuten), sind RA3-Knoten bereit, den vollständigen Produktions-Workload auszuführen. Da die Datenverarbeitung vom Speicher getrennt ist, werden Hot Data dank einer großen Netzwerkbandbreite mit hohen Geschwindigkeiten in den lokalen Cache verschoben. Wenn Sie aus dem neuesten DS2- oder DC2-Snapshot wiederherstellen, behält RA3 Hot-Block-Informationen des DS2- oder DC2-Workloads bei und füllt den lokalen Cache mit den neuesten Blöcken auf. Weitere Informationen finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot.

Um den gleichen Endpunkt für Ihre Anwendungen und Benutzer beizubehalten, können Sie den neuen RA3-Cluster mit demselben Namen wie der ursprüngliche DS2- oder DC2-Cluster umbenennen. Um den Cluster umzubenennen, ändern Sie den Cluster in der Amazon-Redshift-Konsole oder die API-Operation `ModifyCluster`. Weitere Informationen finden Sie unter Umbenennen von Clustern oder API-Operation `ModifyCluster` in der API-Referenz von Amazon Redshift.

- Elastische Größenanpassung – ändern Sie die Größe des Clusters mit der elastischen Größenanpassung. Wenn Sie die elastische Größenanpassung verwenden, um den Knotentyp zu ändern, erstellt Amazon Redshift automatisch einen Snapshot, einen neuen Cluster, löscht den alten Cluster und benennt den neuen Cluster um. Die elastische Größenanpassung kann On-Demand ausgeführt oder für einen Zeitpunkt in der Zukunft geplant werden. Sie können mit der elastischen Größenanpassung Ihre vorhandenen DS2- oder DC2-Knotentypcluster schnell auf RA3 aktualisieren. Weitere Informationen finden Sie unter Elastic resize (Elastische Größenanpassung).

Die folgende Tabelle zeigt Empfehlungen für das Upgrade auf RA3-Knotentypen. (Diese Empfehlungen gelten auch für reservierte Knoten.)

Die Empfehlungen in dieser Tabelle beziehen sich auf die Typen und Größen von Clusterknoten, hängen jedoch von den Rechenanforderungen Ihres Workloads ab. Um Ihre Anforderungen besser einschätzen zu können, sollten Sie einen Machbarkeitsnachweis (Proof of Concept, POC) durchführen, bei dem Test Drive zur Ausführung potenzieller Konfigurationen verwendet wird. Stellen Sie anstelle von Redshift Serverless einen Cluster für Ihr POC Data Warehouse bereit. Weitere Informationen zur Durchführung eines Machbarkeitsnachweises finden Sie unter Durchführen eines Machbarkeitsnachweises (POC) für Amazon Redshift im Amazon Redshift Database Developer Guide.

Vorhandener Knotentyp	Vorhandene Anzahl von Knoten	Empfohlener neuer Knotentyp	Upgrade-Aktion
ds2.xlarge	1	ra3.xlplus	Erstellen Sie einen ra3.xlplus-Cluster mit 1 Knoten[1].
ds2.xlarge	2	ra3.xlplus	Erstellen Sie einen ra3.xlplus-Cluster mit 2 Knoten[1].
ds2.xlarge	3	ra3.xlplus	Erstellen Sie einen ra3.xlplus-Cluster mit 2 Knoten[1].
ds2.xlarge	4	ra3.xlplus	Erstellen Sie einen ra3.xlplus-Cluster mit 3 Knoten[1].
ds2.xlarge	5	ra3.xlplus	Erstellen Sie einen ra3.xlplus-Cluster mit 4 Knoten[1].
ds2.xlarge	6	ra3.xlplus	Erstellen Sie einen ra3.xlplus-Cluster mit 4 Knoten[1].
ds2.xlarge	7	ra3.xlplus	Erstellen Sie einen ra3.xlplus-Cluster mit 5 Knoten[1].

Vorhandener Knotentyp	Vorhandene Anzahl von Knoten	Empfohlener neuer Knotentyp	Upgrade-Aktion
ds2.xlarge	8	ra3.4xlarge	Erstellen Sie einen ra3.4xlarge-Cluster mit 2 Knoten[1].
ds2.xlarge	9	ra3.4xlarge	Erstellen Sie einen ra3.4xlarge-Cluster mit 3 Knoten[1].
ds2.xlarge	10	ra3.4xlarge	Erstellen Sie einen ra3.4xlarge-Cluster mit 3 Knoten[1].
ds2.xlarge	11-128	ra3.4xlarge	Erstellen Sie 1 Knoten des Typs ra3.4xlarge für jeweils 4 Knoten des Typs ds2.xlarge[1].
ds2.8xlarge	2–15	ra3.4xlarge	Erstellen Sie 2 Knoten des Typs ra3.4xlarge für jeweils 1 Knoten des Typs ds2.8xlarge[1].

Vorhandener Knotentyp	Vorhandene Anzahl von Knoten	Empfohlener neuer Knotentyp	Upgrade-Aktion
ds2.8xlarge	16–128	ra3.16xlarge	Erstellen Sie 1 Knoten des Typs ra3.16xlarge für jeweils 2 Knoten des Typs ds2.8xlarge[1].
dc2.8xlarge	2–15	ra3.4xlarge	Erstellen Sie 2 Knoten des Typs ra3.4xlarge für jeweils 1 Knoten des Typs dc2.8xlarge[1].
dc2.8xlarge	16–128	ra3.16xlarge	Erstellen Sie 1 Knoten des Typs ra3.16xlarge für jeweils 2 Knoten des Typs dc2.8xlarge[1].
dc2.large	1–4	Keine	Behalten Sie den vorhandenen dc2.large-Cluster.
dc2.large	5–15	ra3.xlplus	Erstellen Sie drei Knoten des Typs ra3.xlplus für jeweils acht Knoten des Typs dc2.large[1].

Vorhandener Knotentyp	Vorhandene Anzahl von Knoten	Empfohlener neuer Knotentyp	Upgrade-Aktion	
dc2.large	16–32	ra3.4xlarge	Erstellen Sie 1 Knoten des Typs ra3.4xlarge für jeweils 8 Knoten des Typs dc2.large[1] [2].	

[1]Je nach Workload-Anforderungen können zusätzliche Knoten benötigt werden. Fügen Sie Knoten basierend auf den Datenverarbeitungsanforderungen Ihrer erforderlichen Abfrageleistung hinzu, oder entfernen Sie sie.

[2] Cluster mit dem Knotentyp dc2.large sind auf 32 Knoten begrenzt.

Die Mindestanzahl von Knoten für einige RA3-Knotentypen beträgt zwei Knoten. Berücksichtigen Sie dies beim Erstellen eines RA3-Clusters.

Aktualisieren reservierter DS2-Knoten auf reservierte RA3-Knoten durch elastische Größenanpassung oder Snapshot-Wiederherstellung

Wenn Sie über reservierte DS2-Knoten verfügen, können Sie sie mit der Aktualisierungsfunktion für reservierte RA3-Knoten aktualisieren, indem Sie die Amazon-Redshift-Konsole oder die AWS CLI verwenden. In der Konsole gibt es dafür mehrere Möglichkeiten.

Eine Möglichkeit besteht darin, reservierte DS2-Knoten auf RA3 während einer elastischen Größenanpassung zu aktualisieren. Wenn Sie reservierte Knoten haben und RA3-Knoten auswählen, führt die Konsole Sie durch den Aktualisierungsprozess für reservierte Knoten. Aus technischer Sicht funktioniert die elastische Größenanpassung für reservierte Knoten und nicht reservierte Knoten gleich.

Wenn Sie die Clustergröße gegenüber der empfohlenen Größe ändern, ist bei der Konfiguration der elastischen Größenanpassung das Upgrade für den reservierten RA3-Knoten nicht verfügbar und wird nicht auf der Konsole angezeigt. (Sie können weiterhin reservierte DS2-Knoten auf RA3 aktualisieren, aber die Größenanpassung umfasst kein Upgrade von reservierten RA3-Knoten als Teil des Prozesses.) Beachten Sie auch, dass die gewünschte Clustergröße aufgrund von

Beschränkungen der Clustergröße für die elastische Größenanpassung möglicherweise nicht verfügbar ist. Wenn Sie beispielsweise einen DS2-Cluster mit 4 Knoten mit reserviertem Knoten haben, können Sie möglicherweise keinen RA3-Cluster mit 3 Knoten auswählen. In diesem Fall können Sie eine klassische Größenanpassung durchführen, um die gewünschte Clustergröße zu erhalten.

Nach der Größenanpassung des Clusters werden einige Schritte ausgeführt. Zunächst werden Daten in den RA3-Cluster migriert. Dann wird der Lease mit reserviertem DS2-Knoten in einen Lease mit reserviertem RA3-Knoten umgewandelt. Beachten Sie, dass die Zeit für die Datenmigration je nach Größe des Clusters und ob die Größenanpassung elastisch oder klassisch ist, variieren kann. Im Falle einer klassischen Größenanpassung dauert die Datenmigration häufig mehrere Stunden.

Nachdem Sie mit der Größenanpassung begonnen haben, verfolgen Sie den Fortschritt, indem Sie Nachrichten in Events (Ereignisse), anzeigen die auf dem Amazon-Redshift-Dashboard verfügbar sind. Es gibt eine Ereignisbenachrichtigung für die Größenanpassung und eine weitere für die Aktualisierung reservierter Knoten. Weitere Informationen zum Arbeiten mit Ereignissen finden Sie unter Amazon-Redshift-Ereignisse. Nach der Größenanpassung erscheint der aktive Cluster in der AWS Management Console. Sie können auch den konvertierten RA3-Lease mit reserviertem Knoten anzeigen. Die reservierten Quell-Knoten für DS2-Knoten werden möglicherweise noch etwa einen Tag lang in der Konsole angezeigt. Ihnen entstehen dafür keine Kosten. Löschen Sie den reservierten Quellknoten DS2 erst, wenn Sie sicherstellen, dass der RA3-Cluster aktiv ist und die konvertierte Lease für reservierte Knoten generiert wird.

Die andere Möglichkeit, die Aktualisierungsfunktion für reservierte RA3-Knoten zu verwenden, ist bei der Wiederherstellung von einem Snapshot. Wenn Sie den RA3-Knotentyp auswählen und über reservierte DS2-Knoten verfügen, können Sie zu diesem Zeitpunkt die Aktualisierungsfunktion für reservierte RA3-Knoten auswählen. Wenn Sie von einem Snapshot wiederherstellen, erfolgt die Wiederherstellung in einen Cluster mit reserviertem RA3-Knoten. Wie bereits erwähnt, ist die Option zur Aktualisierung für reservierte RA3-Knoten in der Konsole nicht verfügbar, wenn Sie eine andere als die empfohlene Cluster-Größe wählen.

Weitere Informationen zur Größenanpassung von Clustern und zur Aktualisierung von Knoten finden Sie unter Größenanpassung von Clustern. Dort finden Sie eine detaillierte Beschreibung des Prozesses sowie Informationen dazu, was beim Anpassen der Größe mit dem Cluster und den Daten passiert. Weitere Informationen zu den einzelnen Schritten des Prozesses zur elastischen Größenanpassung finden Sie unter Elastic resize (Elastische Größenanpassung). Weitere Informationen zum Wiederherstellen aus einem Snapshot finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot.

Wenn Sie weitere Fragen zum Upgrade reservierter Knoten auf RA3 haben, z. B. zum Upgrade reservierter DC2-Knoten auf RA3, wenden Sie sich an den Support. AWS Weitere Informationen zur Preisgestaltung von On-Demand-Knoten und reservierten Knoten finden Sie unter Amazon Redshift – Preise.

Wenn Sie bereits reservierte DS2-Knoten erworben haben, wenden Sie sich an AWS , um Hilfe bei der Konvertierung von reservierten DS2-Knoten in reservierte RA3-Knoten zu erhalten. AWS Weitere Informationen erhalten Sie unter Amazon Redshift RA3-Instances mit verwaltetem Speicher.

DC2- und DS2-Knoten

In diesen Abschnitten werden die Aufgaben beschrieben, die für DC2- und DS2-Knoten verfügbar sind.

Themen

- Migrieren von DC1-Knotentypen zu DC2-Knotentypen
- Aktualisieren eines DS2-Clusters auf EC2-Classic auf EC2-VPC

Migrieren von DC1-Knotentypen zu DC2-Knotentypen

Um von Leistungsverbesserungen zu profitieren, können Sie ihre DC1-Cluster zu DC2-Knotentypen migrieren.

Cluster, die den Knotentyp DC2 verwenden, müssen in einer Virtual Private Cloud (EC2-VPC) gestartet werden.

Wenn sich Ihr DC1-Cluster nicht in einer VPC befindet:

1. Erstellen Sie einen Snapshot Ihres DC1-Clusters. Weitere Informationen finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.
2. Erstellen Sie eine VPC oder wählen Sie eine vorhandene VPC in Ihrem Konto aus. Weitere Informationen finden Sie unter Verwaltung von Clustern in einer VPC.
3. Stellen Sie den Snapshot auf einem neuen DC2-Cluster in der VPC wieder her. Weitere Informationen finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot.

Wenn sich Ihr DC1-Cluster bereits in einer VPC befindet, wählen Sie eine der folgenden Methoden aus:

- Passen Sie die Größe des DC1-Clusters an und ändern Sie als Teil des Vorgangs den Knotentyp in DC2. Ihr Cluster ist während der Größenänderung für einen bestimmten Zeitraum nicht verfügbar. Weitere Informationen finden Sie unter Größenanpassung von Clustern.
- Erstellen Sie einen Snapshot des DC1-Clusters, und stellen Sie dann den Snapshot in einem DC2-Cluster in der VPC wieder her. Weitere Informationen finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot.

Beachten Sie Folgendes, wenn Sie von DC1-Knoten zu DC2-Knotentypen migrieren.

- DC1-Cluster, die zu 100 % voll sind, werden möglicherweise nicht auf eine entsprechende Anzahl von DC2-Knoten aktualisiert. Sollte mehr Speicherplatz erforderlich sein, können Sie Folgendes tun:
  - Eine Neudimensionierung auf eine Konfiguration mit mehr verfügbarem Speicherplatz vornehmen
  - Bereinigen Sie nicht benötigte Daten, indem Sie Tabellen kürzen oder Zeilen löschen.
- DC2-Cluster unterstützen die EC2-Classic-Vernetzung nicht. Wenn Ihr DC1-Cluster nicht in einer VPC ausgeführt wird, sollten Sie für Ihre DC2-Migration eine VPC erstellen. Weitere Informationen finden Sie unter Verwaltung von Clustern in einer VPC.
- Bei einer Neudimensionierung des Clusters wird er während der Operation womöglich in den schreibgeschützten Modus geschaltet. Weitere Informationen finden Sie unter Größenanpassung von Clustern.
- Wenn Sie reservierte DC1-Knoten erworben haben, können Sie Ihre reservierten DC1-Knoten für den Rest Ihrer Laufzeit auf DC2-Knoten aktualisieren. Weitere Informationen darüber, wie Sie Ihre Reservierung mit dem ändern können AWS CLI, finden Sie unter. Aktualisierung reservierter Knoten mit dem AWS CLI
- Wenn Sie die Wiederherstellung verwenden, um ein Upgrade von dc1.dc2 auf dc2.8xlarge durchzuführen, und die Anzahl der Knoten ändern, muss der Snapshot in der Clusterversion 1.0.10013 oder höher erstellt worden sein.
- Wenn Sie die Wiederherstellung verwenden, um ein Upgrade von dc1.8xlarge auf dc2.8xlarge durchzuführen, muss der Snapshot in der Clusterversion 1.0.10013 oder höher erstellt worden sein.
- Wenn Sie elastische Größenanpassung verwenden, um ein Upgrade von DC1 auf DC2 durchzuführen, und die Anzahl der Knoten ändern, muss der Cluster die Clusterversion 1.0.10013 oder höher aufweisen.

- Stammt ein Snapshot eines dc1.8xlarge-Clusters für die Aktualisierung aus einem Cluster vor Version 1.0.10013, stellen Sie zuerst den Snapshot aus dem dc1.8xlarge-Cluster in einem neuen dc1.8xlarge-Cluster mit der gleichen Anzahl an Knoten wieder her. Verwenden Sie dann eine der folgenden Methoden, um den neuen dc1.8xlarge-Cluster zu aktualisieren.
  - Verwenden Sie einen Snapshot aus dem neu wiederhergestellten Cluster, um ein Upgrade auf dc2.8xlarge durchzuführen.
  - Verwenden Sie die elastische Größenanpassung, um den neu wiederhergestellten Cluster auf dc2.8xlarge zu aktualisieren.

Aktualisieren eines DS2-Clusters auf EC2-Classic auf EC2-VPC

Amazon-Redshift-Cluster werden in Amazon-EC2-Instances ausgeführt, die für den von Ihnen ausgewählten Amazon-Redshift-Knotentyp und die -Größe konfiguriert sind. Für verbesserte Leistung und Sicherheit empfehlen wir Ihnen, Ihren Cluster auf EC2-Classic zu aktualisieren, um in einer VPC mit EC2-VPC zu starten.

So upgraden Sie Ihr DS2-Cluster auf EC2-Classic auf EC2-VPC

1. Erstellen Sie einen Snapshot Ihres DS2-Clusters. Weitere Informationen finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.
2. Erstellen Sie eine VPC oder wählen Sie eine vorhandene VPC in Ihrem Konto aus. Weitere Informationen finden Sie unter Verwaltung von Clustern in einer VPC.
3. Stellen Sie den Snapshot auf dem neuen DS2-Cluster in der VPC wieder her. Weitere Informationen finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot.

Cluster-Operationen

Nachdem Ihr Cluster erstellt wurde, können Sie mehrere Vorgänge ausführen. Zu den Operationen gehören die Größenanpassung, das Anhalten, das Fortsetzen, das Umbenennen und das Löschen.

Themen

- Größenanpassung von Clustern
- Anhalten und Fortsetzen von Clustern
- Umbenennen von Clustern
- Schließen und Löschen von Clustern

- Ihren Cluster verlagern
- Amazon-Redshift-Snapshots und -Sicherungen

Größenanpassung von Clustern

Wenn sich Ihre Data-Warehousing-Kapazität und Leistungsanforderungen ändern, können Sie die Größe Ihres Clusters anpassen, um die Rechen- und Speicheroptionen von Amazon Redshift optimal zu nutzen.

Es gibt zwei Arten von Größenanpassungsvorgängen:

- Elastische Größenanpassung – Sie können Knoten zu Ihrem Cluster hinzufügen oder daraus entfernen. Sie können auch den Knotentyp ändern, z. B. von DS2-Knoten zu RA3-Knoten. Eine elastische Größenanpassung erfolgt in der Regel schnell und dauert durchschnittlich zehn Minuten. Aus diesem Grund empfehlen wir es als erste Option. Wenn Sie eine elastische Größenanpassung durchführen, werden Daten-Slices neu verteilt, d. h. Partitionen, denen Speicher- und Festplattenspeicher in jedem Knoten zugewiesen wird. Elastische Größenanpassung ist geeignet, wenn Sie:
  - Hinzufügen oder Reduzieren von Knoten in einem bestehenden Cluster, ohne jedoch den Knotentyp zu ändern – dies wird allgemein als Größenanpassung vor Ort bezeichnet. Wenn Sie diese Art der Größenanpassung durchführen, werden einige laufende Abfragen erfolgreich abgeschlossen, andere können jedoch als Teil des Vorgangs entfernt werden.
  - Ändern des Knotentyps für einen Cluster – Wenn Sie den Knotentyp ändern, wird ein Snapshot erstellt und Daten werden vom Quell-Cluster an einen Cluster neu verteilt, der aus dem neuen Knotentyp besteht. Nach Abschluss werden laufende Abfragen entfernt. Wie die Größenanpassung vor Ort ist auch diese schnell abgeschlossen.
- Klassische Größenanpassung – Sie können den Knotentyp, die Anzahl der Knoten oder beides ähnlich wie bei der elastischen Größenänderung ändern. Die klassische Größenanpassung dauert länger, kann aber in Fällen nützlich sein, in denen die Änderung der Knotenanzahl oder des Knotentyps, zu dem migriert werden soll, nicht innerhalb der Grenzen für die elastische Größenänderung liegt. Dies kann zum Beispiel zutreffen, wenn die Änderung der Knotenanzahl sehr groß ist.

Themen

- Elastic resize (Elastische Größenanpassung)
- Classic resize (Klassische Größenanpassung)

Elastic resize (Elastische Größenanpassung)

Eine Operation zur elastischen Größenanpassung beim Hinzufügen oder Entfernen von Knoten desselben Typs hat die folgenden Phasen:

1. Bei der elastischen Größenanpassung wird ein Cluster-Snapshot erstellt. Dieser Snapshot beinhaltet immer Tabellen ohne Backup für Knoten, bei denen es anwendbar ist. (Einige Knotentypen, wie RA3, haben keine Tabellen ohne Backup.) Wenn Ihr Cluster keinen aktuellen Snapshot hat, weil Sie automatische Snapshots deaktiviert haben, kann der Sicherungsvorgang länger dauern. (Um die Zeit bis zum Beginn des Größenanpassungsvorgangs zu minimieren, empfehlen wir, dass Sie automatische Snapshots aktivieren oder einen manuellen Snapshot erstellen, bevor Sie mit der Größenanpassung beginnen.) Wenn Sie eine elastische Größenanpassung starten und ein Snapshot-Vorgang ausgeführt wird, kann die Größenänderung fehlschlagen, wenn der Snapshot-Vorgang nicht innerhalb weniger Minuten abgeschlossen wird. Weitere Informationen finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.
2. Der Vorgang migriert Cluster-Metadaten. Der Cluster ist für einige Minuten nicht verfügbar. Die meisten Abfragen werden vorübergehend angehalten und Verbindungen offen gehalten. Es ist jedoch möglich, dass einige Abfragen entfernt werden. Diese Phase ist kurz.
3. Die Sitzungsverbindungen werden wiederhergestellt und die Abfragen fortgesetzt.
4. Bei der elastischen Größenanpassung werden Daten im Hintergrund auf Knoten-Slices umverteilt. Der Cluster ist für Lese- und Schreibvorgänge verfügbar, die Ausführung einiger Abfragen kann jedoch länger dauern.
5. Nachdem der Vorgang abgeschlossen ist, sendet Amazon Redshift eine Ereignisbenachrichtigung.

Wenn Sie die elastische Größenanpassung verwenden, um den Knotentyp zu ändern, funktioniert dies ähnlich wie beim Hinzufügen oder Entfernen von Knoten desselben Typs. Zunächst wird ein Snapshot erstellt. Ein neuer Ziel-Cluster wird mit den aktuellen Daten aus dem Snapshot bereitgestellt und die Daten werden im Hintergrund auf den neuen Cluster übertragen. Während dieser Zeit sind die Daten schreibgeschützt. Wenn die Größenanpassung kurz vor dem Abschluss steht, aktualisiert Amazon Redshift den Endpunkt so, dass er auf den neuen Cluster verweist, und alle Verbindungen zum Quell-Cluster werden getrennt.

Es ist unwahrscheinlich, dass eine elastische Größenänderung fehlschlägt. Im Falle eines Fehlers erfolgt das Rollback jedoch in den meisten Fällen automatisch, ohne dass ein manuelles Eingreifen erforderlich ist.

Wenn Sie reservierte Knoten haben, z. B. reservierte DS2-Knoten, können Sie bei einer Größenanpassung ein Upgrade auf reservierte RA3-Knoten durchführen. Sie können dies tun, wenn Sie eine elastische Größenanpassung durchführen oder die Konsole verwenden, um aus einem Snapshot wiederherzustellen. Die Konsole führt Sie durch diesen Prozess. Weitere Informationen zum Aktualisieren auf RA3-Knoten finden Sie unter Migration zu RA3-Knotentypen.

Bei der elastischen Größenanpassungen werden keine Tabellensortierungen durchgeführt und es wird kein Speicherplatz freigegeben. Daher ist sie kein Ersatz für eine Bereinigungsoperation. Weitere Informationen finden Sie unter Bereinigen von Tabellen.

Für die elastische Größenanpassung gelten die folgenden Einschränkungen:

- Cluster zur elastischen Größenänderung und Datenfreigabe – Wenn Sie Knoten in einem Cluster addieren oder subtrahieren, der ein Produzent für die Datenfreigabe ist, können Sie keine Verbindung von Verbrauchern mit diesem Cluster herstellen, während Amazon Redshift Cluster-Metadaten migriert. Wenn Sie eine elastische Größenänderung durchführen und einen neuen Knotentyp auswählen, ist die Datenfreigabe ebenfalls nicht verfügbar, während Verbindungen getrennt und auf den neuen Ziel-Cluster übertragen werden. Bei beiden Arten der elastischen Größenänderung ist der Produzent einige Minuten nicht verfügbar.
- Datenübertragung von einem freigegebenen Snapshot – Um eine elastische Größenanpassung auf einem Cluster auszuführen, der Daten von einem freigegebenen Snapshot überträgt, muss mindestens eine Sicherung für den Cluster verfügbar sein. Sie können Ihre Backups in der Konsolen-Snapshot-Liste von Amazon Redshift, im `describe-cluster-snapshots`-CLI-Befehl oder in der API-Operation `DescribeClusterSnapshots` anzeigen.
- Plattformeinschränkung – Elastische Größenanpassung ist nur für Cluster verfügbar, die die EC2-VPC-Plattform verwenden. Weitere Informationen finden Sie unter Verwenden von EC2-VPC beim Erstellen Ihres Clusters.
- Überlegungen zur Speicherung – Stellen Sie sicher, dass Ihre neue Knotenkonfiguration über genügend Speicherplatz für vorhandene Daten verfügt. Möglicherweise müssen Sie zusätzliche Knoten hinzufügen oder die Konfiguration ändern.
- Quell- versus Ziel-Cluster-Größe – Die Knotenanzahl und der Knotentyp, die für die Größenänderung mit der elastischen Größenanpassung infrage kommen, werden durch die Anzahl der Knoten im Quell-Cluster und den Knotentyp bestimmt, der für den in der Größe geänderten Clusters ausgewählt wurde. Zum Ermitteln der verfügbaren Konfigurationen können Sie die Konsole verwenden. Oder Sie können den `describe-node-configuration-options` AWS CLI Befehl mit der `action-type resize-cluster` Option verwenden. Weitere Informationen

zur Größenanpassung mithilfe der Amazon-Redshift-Konsole finden Sie unter Größenanpassung eines Clusters.

Der folgende CLI-Beispielbefehl beschreibt die möglichen Konfigurationsoptionen. In diesem Beispiel handelt es sich bei dem Cluster `mycluster` um einen `dc2.large`-Cluster mit acht Knoten.

```
aws redshift describe-node-configuration-options --cluster-identifier mycluster --
region eu-west-1 --action-type resize-cluster
```

Dieser Befehl gibt eine Optionenliste mit empfohlenen Knotentypen, der Knotenanzahl und der Festplattennutzung für jede Option aus. Die zurückgegebenen Konfigurationen können basierend auf dem spezifischen Eingabe-Cluster variieren. Sie können eine dieser Konfigurationen auswählen, wenn Sie die Optionen des CLI-Befehls `resize-cluster` angeben.

- Limit für zusätzliche Knoten – Die elastische Größenanpassung hat Limits für die Knoten, die Sie einem Cluster hinzufügen können. Beispielsweise unterstützt ein dc2-Cluster die elastische Größenanpassung bis zur doppelten Anzahl der Knoten. Zur Veranschaulichung können Sie einem dc2.8xlarge-Cluster mit 4 Knoten einen Knoten hinzufügen, um daraus einen Cluster mit fünf Knoten zu machen, oder weitere Knoten hinzufügen, bis Sie acht erreichen.

  > **Note**
  >
  > Die Wachstums- und Reduktionsgrenzen basieren auf dem ursprünglichen Knotentyp und der Anzahl der Knoten im ursprünglichen Cluster oder seiner letzten klassischen Größenanpassung. Wenn eine elastische Größenanpassung die Wachstums- oder Reduktionsgrenze überschreitet, verwenden Sie eine klassische Größenanpassung.

  Bei einigen ra3-Knotentypen können Sie die Anzahl der Knoten um das Vierfache der vorhandenen Anzahl erhöhen. Gehen wir davon aus, Ihr Cluster besteht aus ra3.4xlarge oder ra3.16xlarge Knoten. Anschließend können Sie die elastische Größenanpassung verwenden, um die Anzahl der Knoten in einem Cluster mit 8 Knoten auf 32 zu erhöhen. Oder Sie können einen Wert unter dem Limit auswählen. (Beachten Sie, dass die Möglichkeit, den Cluster um das Vierfache zu vergrößern, von der Größe des Quell-Clusters abhängt.) Wenn Ihr Cluster ra3.xlplus-Knoten hat, ist das Limit doppelt so hoch.

Alle ra3-Knotentypen unterstützen eine Verringerung der Anzahl der Knoten auf ein Viertel der vorhandenen Anzahl. Beispielsweise können Sie die Größe eines Clusters mit ra3.4xlarge-Knoten von 12 Knoten auf 3 oder auf eine Zahl über dem Minimum verringern.

In der folgenden Tabelle sind die Wachstums- und Reduktionsgrenzen für jeden Knotentyp aufgeführt, der die elastische Größenanpassung unterstützt.

Original-Knotentyp	Grenzwert	Begrenzung der Reduzierung
ra3.16xlarge	4x (von 4 bis 16 Knoten, zum Beispiel)	Auf ein Viertel der Zahl (z. B. von 16 auf 4 Knoten)
ra3.4xlarge	4x	Auf ein Viertel der Zahl
ra3.xlplus	2x (von 4 bis 8 Knoten, zum Beispiel)	Auf ein Viertel der Zahl
dc2.8xlarge	2x	Auf die Hälfte der Zahl (z. B. von 16 auf 8 Knoten)
dc2.large	2x	Auf die Hälfte der Zahl
ds2.8xlarge	2x	Auf die Hälfte der Zahl
ds2.xlarge	2x	Auf die Hälfte der Zahl

Note

Auswahl älterer Knotentypen beim Ändern der Größe eines RA3-Clusters – Wenn Sie versuchen, die Größe von einem Cluster mit RA3-Knoten auf einen anderen Knotentyp wie DC2 oder DS2 zu ändern, wird in der Konsole eine Überprüfungswarnung angezeigt und der Größenänderungsvorgang wird nicht abgeschlossen. Dies liegt daran, dass die Größenänderung älterer Knotentypen nicht unterstützt wird. Dies soll verhindern, dass ein Kunde die Größe auf einen Knotentyp ändert, der veraltet ist oder bald veraltet sein wird. Dies gilt sowohl für die elastische als auch die klassische Größenanpassung.

Classic resize (Klassische Größenanpassung)

Die klassische Größenanpassung behandelt Anwendungsfälle, in denen die Änderung der Cluster-Größe oder des Knotentyps nicht von der elastischen Größenanpassung unterstützt wird. Wenn Sie eine klassische Größenanpassung durchführen, erstellt Amazon Redshift einen Ziel-Cluster und migriert Ihre Daten und Metadaten aus dem Quell-Cluster dorthin.

Die klassische Größenanpassung an RA3 kann für eine bessere Verfügbarkeit sorgen

Die klassische Größenanpassung wurde verbessert, wenn der Zielknotentyp RA3 ist. Dies geschieht durch die Verwendung einer Backup- und Wiederherstellungsoperation zwischen dem Quell- und dem Ziel-Cluster. Wenn die Größenanpassung beginnt, wird der Quell-Cluster neu gestartet und ist für einige Minuten nicht verfügbar. Danach ist der Cluster für Lese- und Schreibvorgänge verfügbar, während die Größenanpassung im Hintergrund fortgesetzt wird.

Überprüfen Ihres Clusters

Füllen Sie diese Checkliste aus, um sicherzustellen, dass Sie bei einer klassischen Größenanpassung eines RA3-Clusters die beste Leistung und optimale Ergebnisse erzielen. Wenn Sie die Checkliste nicht befolgen, können Sie möglicherweise einige der Vorteile der klassischen Größenänderung mit RA3-Knoten nicht nutzen, z. B. die Fähigkeit, Lese- und Schreiboperationen durchzuführen.

1. Die Größe der Daten muss unter 2 Petabyte liegen. (Ein Petabyte entspricht 1 000 Terabyte.) Erstellen Sie einen Snapshot und überprüfen Sie dessen Größe, um die Größe Ihrer Daten zu validieren. Sie können auch die folgende Abfrage ausführen, um die Größe zu überprüfen:

   ```
   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;
   ```

   Die Tabelle `svv_table_info` ist nur für Superuser sichtbar.
2. Bevor Sie eine klassische Größenanpassung einleiten, stellen Sie sicher, dass Sie über einen manuellen Snapshot verfügen, der nicht älter als 10 Stunden ist. Erstellen Sie andernfalls einen Snapshot.
3. Der Snapshot, der für die klassische Größenanpassung verwendet wird, kann nicht für eine Tabellenwiederherstellung oder für andere Zwecke verwendet werden.

4. Der Cluster muss sich in einer VPC befinden.

Sortier- und Verteilungsoperationen, die sich aus der klassischen Größenanpassung an RA3 ergeben

Während der klassischen Größenanpassung an RA3 werden Tabellen mit KEY-Verteilung, die als EVEN-Verteilung migriert werden, in ihren ursprünglichen Verteilungsstil umgewandelt. Die Dauer dieses Vorgangs hängt von der Größe der Daten und der Auslastung Ihres Clusters ab. Abfrage-Workloads erhalten eine höhere Priorität als die Datenmigration. Weitere Informationen finden Sie unter Verteilungsstile. Während dieses Migrationsprozesses funktionieren sowohl Lese- als auch Schreibvorgänge in der Datenbank, die Durchführung von Abfragen kann jedoch länger dauern. Eine Nebenläufigkeitsskalierung kann die Leistung in dieser Zeit jedoch steigern, indem Ressourcen für Abfrage-Workloads hinzugefügt werden. Sie können den Fortschritt der Datenmigration anhand der Ergebnisse in den Ansichten SYS_RESTORE_STATE und SYS_RESTORE_LOG verfolgen. Weitere Informationen zur Überwachung folgen.

Nachdem die Größe des Clusters vollständig angepasst wurde, tritt das folgende Sortierverhalten auf:

- Wenn die Größenanpassung dazu führt, dass der Cluster mehr Segmente hat, werden die KEY-Verteilungstabellen teilweise unsortiert, EVEN-Tabellen bleiben jedoch sortiert. Darüber hinaus sind die Informationen darüber, wie viele Daten sortiert sind, möglicherweise direkt nach der Größenanpassung nicht aktuell. Nach der Schlüsselwiederherstellung wird die Tabelle durch die automatische Bereinigung im Laufe der Zeit sortiert.
- Wenn die Größenanpassung dazu führt, dass der Cluster weniger Segmente hat, werden sowohl die KEY- als auch die EVEN-Verteilungstabellen teilweise unsortiert. Die Tabelle wird durch die automatische Bereinigung im Laufe der Zeit sortiert.

Weitere Informationen zur automatischen Tabellenbereinigung finden Sie unter Bereinigen von Tabellen. Weitere Informationen zu Segmenten von Datenverarbeitungsknoten finden Sie unter Data Warehouse-Systemarchitektur.

Schritte zur klassischen Größenanpassung, wenn der Ziel-Cluster RA3 ist

Die klassische Größenanpassung besteht aus den folgenden Schritten, wenn der Ziel-Cluster-Typ RA3 ist und Sie die im vorherigen Abschnitt beschriebenen Voraussetzungen erfüllt haben.

1. Die Migration wird vom Quell-Cluster zum Ziel-Cluster eingeleitet. Wenn der neue Ziel-Cluster bereitgestellt wird, sendet Amazon Redshift eine Ereignisbenachrichtigung, dass die Größenanpassung begonnen hat. Ihr vorhandener Cluster wird neu gestartet, wodurch alle

Verbindungen geschlossen werden. Wenn es sich bei Ihrem vorhandenen Cluster um einen Producer-Cluster für den Datenaustausch handelt, werden Verbindungen zu Consumer-Clustern ebenfalls geschlossen. Der Neustart dauert einige Minuten.

Beachten Sie, dass jede Datenbankbeziehung, z. B. eine Tabelle oder eine materialisierte Ansicht, die mit `BACKUP NO` erstellt wurde, bei der klassischen Größenanpassung nicht beibehalten wird. Weitere Informationen finden Sie unter CREATE MATERIALIZED VIEW.

2. Nach dem Neustart steht die Datenbank für Lese- und Schreibvorgänge zur Verfügung. Darüber hinaus wird der Datenaustausch wieder aufgenommen, was wiederum einige Minuten dauert.
3. Zunächst werden Daten zum Ziel-Cluster migriert. Wenn der Zielknotentyp RA3 ist, sind Lese- und Schreibvorgänge während der Datenmigration verfügbar.
4. Wenn der Prozess der Größenanpassung fast abgeschlossen ist, aktualisiert Amazon Redshift den Endpunkt auf den Ziel-Cluster und alle Verbindungen zum Quell-Cluster werden getrennt. Der Ziel-Cluster wird zum Produzenten für die Datenfreigabe.
5. Die Größenanpassung wird abgeschlossen. Amazon Redshift sendet eine Ereignisbenachrichtigung.

Sie können den Fortschritt der Größenanpassung auf der Amazon-Redshift-Konsole anzeigen. Die Zeit, die zum Ändern der Größe eines Clusters benötigt wird, hängt von der Datenmenge ab.

> **Note**
>
> Auswahl älterer Knotentypen beim Ändern der Größe eines RA3-Clusters – Wenn Sie versuchen, die Größe von einem Cluster mit RA3-Knoten auf einen anderen Knotentyp wie DC2 oder DS2 zu ändern, wird in der Konsole eine Überprüfungswarnung angezeigt und der Größenänderungsvorgang wird nicht abgeschlossen. Dies liegt daran, dass die Größenänderung älterer Knotentypen nicht unterstützt wird. Dies soll verhindern, dass ein Kunde die Größe auf einen Knotentyp ändert, der veraltet ist oder bald veraltet sein wird. Dies gilt sowohl für die elastische als auch die klassische Größenanpassung.

Überwachung einer klassischen Größenanpassung, wenn der Ziel-Cluster RA3 ist

Verwenden Sie SYS_RESTORE_STATE, um den Fortschritt einer klassischen Größenanpassung eines bereitgestellten Clusters, einschließlich der KEY-Verteilung, zu überwachen. Es wird der Prozentsatz angezeigt, zu dem die Konvertierung der Tabelle abgeschlossen wurde. Sie müssen ein Superuser sein, um auf die Daten zugreifen zu können.

Löschen Sie Tabellen, die Sie nicht benötigen, wenn Sie eine klassische Größenanpassung durchführen. Dadurch können vorhandene Tabellen schneller verteilt werden.

Schritte zur klassischen Größenanpassung, wenn der Ziel-Cluster nicht RA3 ist

Die klassische Größenänderung besteht aus den folgenden Schritten, wenn der Zielknotentyp ein anderer als RA3 ist, beispielsweise DS2.

1. Die Migration wird vom Quell-Cluster zum Ziel-Cluster eingeleitet. Wenn der neue Ziel-Cluster bereitgestellt wird, sendet Amazon Redshift eine Ereignisbenachrichtigung, dass die Größenanpassung begonnen hat. Ihr vorhandener Cluster wird neu gestartet, wodurch alle Verbindungen geschlossen werden. Wenn es sich bei Ihrem vorhandenen Cluster um einen Producer-Cluster für den Datenaustausch handelt, werden Verbindungen zu Consumer-Clustern ebenfalls geschlossen. Der Neustart dauert einige Minuten.

   Beachten Sie, dass jede Datenbankbeziehung, z. B. eine Tabelle oder eine materialisierte Ansicht, die mit `BACKUP NO` erstellt wurde, bei der klassischen Größenanpassung nicht beibehalten wird. Weitere Informationen finden Sie unter CREATE MATERIALIZED VIEW.
2. Nach dem Neustart ist die Datenbank schreibgeschützt verfügbar. Der Datenaustausch wird wieder aufgenommen, was wiederum einige Minuten dauert.
3. Zunächst werden Daten zum Ziel-Cluster migriert. Die Datenbank bleibt schreibgeschützt.
4. Wenn der Prozess der Größenanpassung fast abgeschlossen ist, aktualisiert Amazon Redshift den Endpunkt auf den Ziel-Cluster und alle Verbindungen zum Quell-Cluster werden getrennt. Der Ziel-Cluster wird zum Produzenten für die Datenfreigabe.
5. Die Größenanpassung wird abgeschlossen. Amazon Redshift sendet eine Ereignisbenachrichtigung.

Sie können den Fortschritt der Größenanpassung auf der Amazon-Redshift-Konsole anzeigen. Die Zeit, die zum Ändern der Größe eines Clusters benötigt wird, hängt von der Datenmenge ab.

> **Note**
>
> Es kann Tage oder möglicherweise Wochen dauern, die Größe eines Clusters mit einer großen Datenmenge anzupassen, wenn der Ziel-Cluster nicht RA3 ist oder der Cluster die im vorherigen Abschnitt beschriebenen Voraussetzungen für einen RA3-Ziel-Cluster nicht erfüllt. Beachten Sie auch, dass sich die genutzte Speicherkapazität für den Cluster nach einer klassischen Größenanpassung erhöhen kann. Dies entspricht dem normalen

Systemverhalten, wenn der Cluster infolge der klassischen Größenanpassung über zusätzliche Daten-Slices verfügt. Diese Nutzung zusätzlicher Kapazität kann auch dann erfolgen, wenn die Anzahl der Knoten im Cluster gleich bleibt.

Elastische Größenanpassung im Vergleich zur klassischen Größenanpassung

In der folgenden Tabelle wird das Verhalten zwischen den beiden Größenanpassungstypen verglichen.

Elastische Größenanpassung im Vergleich zur klassischen Größenanpassung

Behavior	Elastic resize (Elastische Größenanpassung)	Classic resize (Klassische Größenanpassung)	Komme
Aufbewahrung von Systemdaten	Die elastische Größenanpassung behält die Systemprotokolldaten bei.	Die klassische Größenanpassung behält keine Systemtabellen und -daten bei.	Wenn Sie die Audit-Protokollierung in Ihrem Quell-Cluster aktiviert haben, können Sie nach einer Größenänderung weiterhin auf

Behavior	Elastic resize (Elastische Größenanpassung)	Classic resize (Klassische Größenanpassung)	Komme			
			die Protokolle in Amazon S3 oder in CloudWatch zugreifen. Sie können diese Protokolle je nach Vorgabe Ihrer Datenrichtlinien behalten oder löschen			

Behavior	Elastic resize (Elastische Größenanpassung)	Classic resize (Klassische Größenanpassung)	Komme e			
Ändern von Knotentypen	Elastische Größenanpassung, wenn sich der Knotentyp nicht ändert: Größenänderung vor Ort, und die meisten Abfragen werden gehalten. Elastische Größenanpassung mit einem neuen ausgewählten Knotentyp: Ein neuer Cluster wird erstellt. Abfragen werden entfernt, wenn der Größenanpassungsprozess abgeschlossen ist.	Klassische Größenanpassung: Ein neuer Cluster wird erstellt. Abfragen werden während des Größenanpassungsprozess entfernt.				

Behavior	Elastic resize (Elastische Größenanpassung)	Classic resize (Klassische Größenanpassung)	Kommentare
Aufbewahrung von Sitzungen und Abfragen	Die elastische Größenanpassung behält Sitzungen und Abfragen bei, wenn der Knotentyp im Quellcluster und im Ziel identisch ist. Wenn Sie einen neuen Knotentyp auswählen, werden Abfragen entfernt.	Die klassische Größenanpassung behält keine Sitzungen und Abfragen bei. Abfragen werden entfernt.	Wenn Abfragen entfernt werden, müssen Sie mit einer gewissen Leistungsminderung rechnen. Am besten führen Sie eine Größenanpassung während einer Zeit mit geringer Nutzung durch.

Behavior	Elastic resize (Elastische Größenanpassung)	Classic resize (Klassische Größenanpassung)	Kommentare
Abbrechen einer Größenanpassung	Sie können eine elastische Größenanpassung nicht abbrechen.	Sie können eine klassische Größenanpassung abbrechen, bevor sie abgeschlossen ist. Wählen Sie dafür Cancel resize (Größenanpassung abbrechen) in den Clusterdetails in der Amazon-Redshift-Konsole.	Die zum Abbrechen einer Größenanpassung erforderliche Zeit hängt davon ab, in welcher Stufe sich die Größenanpassung gerade befindet, wenn sie abgebrochen wird. Wenn Sie dies tun, ist der Cluster

Behavior	Elastic resize (Elastische Größenanpassung)	Classic resize (Klassische Größenanpassung)	Komme e
			nicht verfügbar, bis der Abbruchvorgang abgeschlossen ist. Wenn sich der Größenanpassungsvorgang in der Endphase befindet, können Sie ihn nicht abbrechen. Eine klassische Größenanpassung eines RA3-

Behavior	Elastic resize (Elastische Größenanpassung)	Classic resize (Klassische Größenanpassung)	Kommentare
			Clusters können Sie nicht abbrechen.

Planen einer Größenanpassung

Sie können Größenanpassungsvorgänge für Ihren Cluster so planen, dass er hochskaliert wird, um eine hohe Auslastung zu antizipieren, oder herunterskaliert wird, um Kosten zu sparen. Die Planung funktioniert sowohl für die elastische als auch für die klassische Größenanpassung. Sie können einen Zeitplan in der Amazon-Redshift-Konsole einrichten. Weitere Informationen finden Sie unter Größenanpassung eines Clusters, unter Managing clusters using the console (Verwalten von Clustern mithilfe der Konsole). Sie können auch unsere Amazon Redshift Redshift-API-Operationen verwenden AWS CLI , um eine Größenänderung zu planen. Weitere Informationen finden Sie create-scheduled-actionin der AWS CLI Befehlsreferenz oder CreateScheduledActionin der Amazon Redshift API-Referenz.

Snapshot, Wiederherstellung und Größenanpassung

Die elastische Größenanpassung stellt die schnellste Möglichkeit für die Anpassung der Größe eines Amazon-Redshift-Clusters dar. Wenn die elastische Größenanpassung keine Option für Sie darstellt und Sie einen annähernd konstanten Schreibzugriff auf Ihren Cluster benötigen, verwenden Sie die im folgenden Abschnitt beschriebene Snapshot- und Wiederherstellungsoperationen mit klassischer Größenanpassung. Dafür ist es erforderlich, dass alle Daten, die nach der Erstellung des Snapshots zum Quellcluster geschrieben werden, nach dem Wechsel manuell zum Zielcluster kopiert werden. Je nachdem, wie lange der Kopiervorgang dauert, müssen Sie dies möglicherweise mehrmals wiederholen, bis sich in beiden Clustern die gleichen Daten befinden. Anschließend können Sie den Wechsel zum Zielcluster durchführen. Dieser Prozess kann negative Auswirkungen auf bestehende

Abfragen haben, bis alle Daten im Zielcluster verfügbar sind. Er minimiert jedoch den Zeitraum, in dem keine Schreibvorgänge in der Datenbank möglich sind.

Der Snapshot-, Wiederherstellungs- und klassische Größenanpassungsansatz verwendet den folgenden Prozess:

1. Erstellen Sie einen Snapshot des bestehenden Clusters. Der bestehende Cluster ist der Quellcluster.
2. Notieren Sie sich die Erstellungszeit des Snapshots. Auf diese Weise können Sie später den Punkt identifizieren, an dem Sie Extraktions-, Transaktions- und Lade-Prozesse (ETL) erneut ausführen müssen, um nach dem Snapshot entstandene Daten in die Zieldatenbank zu laden.
3. Stellen Sie den Snapshot in einem neuen Cluster wieder her. Dieser neue Cluster ist der Zielcluster. Prüfen Sie, ob sich die Beispieldaten im Zielcluster befinden.
4. Passen Sie die Größe des Zielclusters an. Wählen Sie den Knotentyp, die Anzahl der Knoten und andere Einstellungen für den Zielcluster.
5. Prüfen Sie die Ladungen aus Ihren ETL-Prozessen, die nach der Erstellung des Snapshots des Quellclusters aufgetreten sind. Achten Sie darauf, die Daten in der gleichen Reihenfolge erneut in den Zielcluster zu laden. Wenn Datenladevorgänge laufen, wiederholen Sie diesen Prozess mehrmals, bis die Daten im Quell- und Zielcluster identisch sind.
6. Halten Sie alle laufenden Abfragen auf dem Quellcluster an. Hierzu können Sie den Cluster erneut starten oder sich als Superuser anmelden und die Befehle PG_CANCEL_BACKEND und PG_TERMINATE_BACKEND verwenden. Der Neustart des Clusters ist die einfachste Möglichkeit, um sicherzustellen, dass der Cluster nicht verfügbar ist.
7. Benennen Sie den Quellcluster um. Beispielsweise von `examplecluster` zu `examplecluster-source`.
8. Geben Sie dem Zielcluster den vorherigen Namen des Quellclusters. Benennen Sie beispielsweise den Zielcluster als `examplecluster`. Von diesem Punkt an verbinden sich alle Anwendungen, die den Endpunkt mit `examplecluster` verwenden, mit dem Zielcluster.
9. Löschen Sie nach dem Wechsel zum Zielcluster den Quellcluster, und prüfen Sie, ob alle Prozesse wie erwartet ausgeführt werden.

Alternativ können Sie den Quell- und den Zielcluster umbenennen, bevor Sie Daten erneut in den Zielcluster laden. Dieser Ansatz funktioniert, wenn es nicht erforderlich ist, dass alle abhängigen Systeme und Berichte sofort denen des Ziel-Clusters entsprechen. In diesem Fall wird Schritt 6 an das Ende des oben beschriebenen Prozesses verschoben.

Die Umbenennung ist nur erforderlich, wenn die Anwendungen weiterhin den selben Endpunkt für die Verbindung zum Cluster verwenden müssen. Wenn dies nicht erforderlich ist, können Sie stattdessen alle Anwendungen, die sich mit dem Cluster verbinden, so aktualisieren, dass sie den Endpunkt des Zielclusters verwenden, ohne den Cluster umzubenennen.

Die Wiederverwendung eines Clusternamens bietet eine Reihe von Vorteilen. Zunächst müssen Sie dann keine Anwendungsverbindungszeichenfolgen aktualisieren, da der Endpunkt gleich bleibt, obwohl sich der zugrunde liegende Cluster ändert. Zweitens sind verwandte Elemente wie CloudWatch Amazon-Alarme und Amazon Simple Notification Service (Amazon SNS) - Benachrichtigungen an den Clusternamen gebunden. Durch diese Verknüpfung können Sie weiterhin die Alarme und Benachrichtigungen verwenden, die Sie für den Cluster eingerichtet haben. Diese fortgesetzte Verwendung ist besonders in Produktionsumgebungen relevant, in denen Sie die Flexibilität benötigen, die Größe des Clusters anzupassen, ohne zugehörige Elemente wie Alarme und Benachrichtigungen neu zu konfigurieren.

Anhalten und Fortsetzen von Clustern

Wenn Sie über einen Cluster verfügen, der nur zu bestimmten Zeiten verfügbar sein muss, können Sie den Cluster anhalten und ihn später fortsetzen. Während der Cluster angehalten ist , wird die On-Demand-Abrechnung unterbrochen. Nur für den Speicher des Clusters fallen Gebühren an. Weitere Informationen zu Preisen finden Sie unter Amazon Redshift – Preise.

Wenn Sie einen Cluster anhalten, erstellt Amazon Redshift einen Snapshot, beendet Abfragen und versetzt den Cluster in einen Pause-Status. Wenn Sie einen angehaltenen Cluster löschen, ohne einen endgültigen Snapshot anzufordern, können Sie den Cluster nicht wiederherstellen. Sie können eine Pausierungs- oder Fortsetzungsoperation nicht mehr abbrechen oder zurücksetzen, nachdem sie gestartet wurde.

Sie können einen Cluster auf der Amazon Redshift Redshift-Konsole, mit den oder mit den AWS CLI Amazon Redshift Redshift-API-Vorgängen anhalten und wieder aufnehmen.

Sie können Aktionen zum Anhalten und Fortsetzen eines Clusters planen. Wenn Sie die neue Amazon-Redshift-Konsole verwenden, um einen wiederkehrenden Zeitplan zum Anhalten und Fortsetzen zu erstellen, werden zwei geplante Aktionen für den ausgewählten Datumsbereich erstellt. Die Namen der geplanten Aktion werden mit `-pause` und `-resume` suffigiert. Die Gesamtlänge des Namens muss innerhalb der maximalen Größe eines geplanten Aktionsnamens liegen.

Die folgenden Clustertypen können nicht angehalten werden:

- EC2-Classic-Cluster.

- Cluster, die nicht aktiv sind, z. B. ein Cluster, der derzeit geändert wird.
- HSM (Hardware Security Module-Cluster
- Cluster, für die automatisierte Snapshots deaktiviert sind.

Berücksichtigen Sie bei der Entscheidung, einen Cluster anzuhalten, Folgendes:

- Verbindungen oder Abfragen zum Cluster sind nicht verfügbar.
- Die Informationen zur Abfrageüberwachung eines angehaltenen Clusters auf der Amazon-Redshift-Konsole können nicht angezeigt werden.
- Sie können einen angehaltenen Cluster nicht ändern. Alle geplanten Aktionen auf dem Cluster werden nicht ausgeführt. Dazu gehören das Erstellen von Snapshots, die Größenanpassung von Clustern und Clusterwartungsoperationen.
- Hardware-Metriken werden nicht erstellt. Aktualisieren Sie Ihre CloudWatch Alarme, wenn Sie Alarme für fehlende Messwerte eingerichtet haben.
- Sie können die letzten automatisierten Snapshots eines angehaltenen Clusters nicht in manuelle Snapshots kopieren.
- Wenn ein Cluster angehalten ist, kann er erst fortgesetzt werden, wenn die Pausierungsoperation abgeschlossen ist.
- Wenn Sie einen Cluster anhalten, wird die Abrechnung unterbrochen. Die Pausierungsoperation wird jedoch in der Regel innerhalb von 15 Minuten abgeschlossen, je nach Größe des Clusters.
- Prüfprotokolle werden archiviert und beim Fortsetzen nicht wiederhergestellt.
- Nachdem ein Cluster angehalten wurde, sind Ablaufverfolgungen und Protokolle möglicherweise nicht für die Behandlung von Problemen verfügbar, die vor dem Anhalten aufgetreten sind.
- Tabellen ohne Backup im Cluster werden beim Fortsetzen nicht wiederhergestellt. Weitere Informationen zu Tabellen ohne Backup finden Sie unter Ausschluss von Tabellen von Snapshots.
- Wenn Sie Ihre Administratoranmeldedaten mithilfe Ihres Clusters verwalten AWS Secrets Manager und diesen pausieren, wird der geheime Schlüssel Ihres Clusters nicht gelöscht und der geheime Schlüssel wird Ihnen weiterhin in Rechnung gestellt. Weitere Informationen zur Verwaltung Ihres Redshift-Admin-Passworts mit finden Sie AWS Secrets Manager unterVerwaltung von Amazon Redshift Redshift-Administratorkennwörtern mit AWS Secrets Manager.

Wenn Sie einen Cluster fortsetzen, sollten Sie Folgendes beachten:

- Die Clusterversion des fortgesetzten Clusters wird basierend auf dem Wartungsfenster des Clusters auf die Wartungsversion aktualisiert.
- Wenn Sie das Subnetz löschen, das einem angehaltenen Cluster zugeordnet ist, haben Sie möglicherweise ein inkompatibles Netzwerk. Stellen Sie in diesem Fall den Cluster aus dem neuesten Snapshot wieder her.
- Wenn Sie eine Elastic IP-Adresse löschen, während der Cluster angehalten ist, wird eine neue Elastic IP-Adresse angefordert.
- Wenn Amazon Redshift den Cluster mit seiner vorherigen Elastic-Network-Schnittstelle nicht fortsetzen kann, versucht Amazon Redshift, einen neuen zu reservieren.
- Wenn Sie einen Cluster fortsetzen, können sich die IP-Adressen des Knotens ändern. Möglicherweise müssen Sie Ihre VPC-Einstellungen aktualisieren, um diese neuen IP-Adressen für Funktionen wie COPY from Secure Shell (SSH) oder COPY from Amazon EMR zu unterstützen.
- Wenn Sie versuchen, einen Cluster fortzusetzen, der nicht angehalten ist, gibt die Fortsetzungsoperation einen Fehler zurück. Wenn die Fortsetzungsoperation Teil einer geplanten Aktion ist, ändern oder löschen Sie die geplante Aktion, um zukünftige Fehler zu vermeiden.
- Je nach der Größe des Clusters kann es einige Minuten dauern, bis ein Cluster bei seiner Fortsetzung wieder Abfragen verarbeiten kann. Darüber hinaus kann die Abfrageleistung für einen gewissen Zeitraum beeinträchtigt sein, während der Cluster nach Abschluss der Fortsetzungsoperation erneut hydriert wird.

Umbenennen von Clustern

Sie können einen Cluster nach Wunsch umbenennen. Da der Endpunkt Ihres Clusters den Clusternamen (auch als Cluster-Kennung bezeichnet) enthält, verwendet der Endpunkt nach der Umbenennung den neuen Namen. Zum Beispiel: Wenn Sie einen Cluster mit der Bezeichnung `examplecluster` haben und diesen in `newcluster` umbenennen, verwendet der Endpunkt die ID `newcluster`. Alle mit dem Cluster verbundenen Anwendungen müssen mit dem neuen Endpunkt aktualisiert werden.

Sie können einen Cluster umbenennen, wenn Sie den Cluster ändern möchten, mit dem sich Ihre Anwendungen verbinden, ohne dass der Endpunkt in diesen Anwendungen geändert werden muss. In diesem Fall müssen Sie zuerst den ursprünglichen Cluster umbenennen und dann den zweiten Cluster ändern, damit dieser den Namen des ursprünglichen Clusters vor der Umbenennung verwendet. Dies ist erforderlich, da die Cluster-ID innerhalb Ihres Kontos und Ihrer Region eindeutig sein muss und der ursprüngliche und der zweite Cluster daher nicht denselben Namen haben

dürfen. Sie können dies tun, wenn Sie einen Cluster aus einem Snapshot wiederherstellen und die Verbindungseigenschaften der davon abhängigen Anwendungen nicht ändern möchten.

> **Note**
>
> Wenn Sie den ursprünglichen Cluster löschen, sind Sie für die Löschung aller nicht benötigten Cluster-Snapshots verantwortlich.

Wenn Sie einen Cluster umbenennen, wechselt dessen Status bis zum Abschluss des Vorgangs zu `renaming`. Der alte von dem Cluster verwendete DNS-Name wird sofort gelöscht, kann aber noch einige Minuten im Zwischenspeicher aufbewahrt werden. Der neue DNS-Name für den umbenannten Cluster wird nach etwa 10 Minuten wirksam. Der umbenannte Cluster ist erst verfügbar, wenn der neue Name wirksam ist. Der Cluster wird neu gestartet, und alle bestehenden Verbindungen zu dem Cluster werden getrennt. Wenn dies abgeschlossen ist, verwendet der Endpunkt den neuen Namen. Daher sollten Sie alle laufenden Abfragen anhalten, bevor Sie die Umbenennung beginnen, und diese nach Abschluss des Vorgangs neu starten.

Cluster-Snapshots werden beibehalten, und alle mit einem Cluster verbundenen Snapshot sind dies auch nach Abschluss der Umbenennung. Nehmen Sie beispielsweise an, Sie haben einen Cluster für Ihre Produktionsdatenbank, für den mehrere Snapshots vorliegen. Wenn Sie den Cluster umbenennen und dann in der Produktionsumgebung durch einen Snapshot ersetzen, sind dem umbenannten Cluster nach wie vor diese vorhandenen Snapshots zugeordnet.

CloudWatch Amazon-Alarme und Amazon Simple Notification Service (Amazon SNS) - Ereignisbenachrichtigungen sind mit dem Namen des Clusters verknüpft. Wenn Sie den Cluster umbenennen, müssen Sie diese entsprechend aktualisieren. Sie können die CloudWatch Alarme in der CloudWatch Konsole aktualisieren, und Sie können die Amazon SNS SNS-Ereignisbenachrichtigungen in der Amazon Redshift Redshift-Konsole im Bereich Ereignisse aktualisieren. Die Lade- und Abfragedaten für den Cluster zeigen nach wie vor Daten von vor und von nach der Umbenennung an. Die Leistungsdaten werden jedoch nach der Umbenennung zurückgesetzt.

Weitere Informationen finden Sie unter Modifizieren eines Clusters.

Schließen und Löschen von Clustern

Sie können Ihren Cluster schließen, wenn er nicht weiter betrieben und Kosten verursachen soll. Wenn Sie dies tun, können Sie optional einen abschließenden Snapshot erstellen. Wenn Sie einen

abschließenden Snapshot erstellen, erstellt Amazon Redshift einen manuellen Snapshot Ihres Clusters, bevor es ihn schließt. Sie können diesen Snapshot später wiederherstellen, wenn Sie die Ausführung des Clusters fortsetzen und Daten abfragen möchten.

Wenn Sie Ihren Cluster und dessen Daten nicht mehr benötigen, können Sie ihn schließen, ohne einen abschließenden Snapshot zu erstellen. In diesem Fall werden Cluster und Daten dauerhaft gelöscht. Für weitere Informationen zum Schließen und Löschen von Clustern vgl. Löschen eines Clusters.

Unabhängig davon, ob Sie Ihren Cluster mit einem abschließenden Snapshot schließen, werden alle mit dem Cluster verbundenen automatisierten Snapshots nach dem Schließen des Clusters gelöscht. Alle mit dem Cluster verbundenen manuellen Snapshots werden beibehalten. Alle beibehaltenen manuellen Snapshots, einschließlich des optionalen abschließenden Snapshots, unterliegen der Speichergebühr von Amazon Simple Storage Service, wenn Sie beim Schließen des Clusters keine weiteren aktiven Cluster haben oder wenn Sie den zur Ausführung Ihrer Amazon-Redshift-Cluster bereitgestellten kostenlosen Speicherplatz überschreiten. Weitere Informationen zu den Gebühren für die Speicherung von Snapshots finden Sie auf der Seite Amazon Redshift – Preise.

Durch das Löschen eines Clusters werden auch alle zugehörigen Geheimnisse gelöscht. AWS Secrets Manager

Ihren Cluster verlagern

Durch Verwendung von relocation (Verschiebung) in Amazon Redshift ermöglichen Sie Amazon Redshift, einen Cluster ohne Datenverlust oder Änderungen an Ihren Anwendungen in eine andere Availability Zone (AZ) zu verschieben. Mit der Verschiebung können Sie den Betrieb mit minimalen Auswirkungen fortsetzen, wenn es eine Serviceunterbrechung für den Cluster gibt.

Wenn Clusterverschiebung aktiviert ist, kann Amazon Redshift in einigen Situationen entscheiden, Cluster zu verschieben. Das geschieht insbesondere, wenn Probleme in der aktuellen Availability Zone einen optimalen Clusterbetrieb verhindern, oder um die Serviceverfügbarkeit zu verbessern. Sie können die Verschiebungsfunktion auch aufrufen, wenn Clustervorgänge durch Ressourceneinschränkungen in einer bestimmten Availability Zone beeinträchtigt sind. Ein Beispiel ist die Möglichkeit, einen Cluster fortzusetzen oder zu skalieren. Amazon Redshift bietet die Verschiebungsfunktion ohne zusätzliche Kosten an.

Wenn ein Amazon-Redshift-Cluster in eine neue Availability Zone verschoben wird, hat der neue Cluster denselben Endpunkt wie der ursprüngliche Cluster. Ihre Anwendungen können sich wieder mit dem Endpunkt verbinden und den Betrieb ohne Datenänderungen oder -verlust fortsetzen.

Aufgrund möglicher Ressourceneinschränkungen in einer bestimmten Availability Zone ist eine Verschiebung jedoch nicht immer möglich.

Die Amazon-Redshift-Clusterverschiebung wird nur für die RA3-Instance-Typen unterstützt, z. B. ra3.16xlarge, ra3.4xlarge und ra3.xlplus. RA3-Instance-Typen nutzen Redshift Managed Storage (RMS) als dauerhafte Speicherschicht. Die neueste Kopie der Daten eines Clusters ist immer in anderen Availability Zones in einer AWS Region verfügbar. Mit anderen Worten: Sie können einen Amazon-Redshift-Cluster ohne Datenverlust in eine andere Availability Zone verschieben.

Wenn Sie die Verschiebung für Ihren Cluster aktivieren, migriert Amazon Redshift Ihren Cluster so, dass er sich hinter einem Proxy befindet. Dadurch wird ein standortunabhängiger Zugriff auf die Rechenressourcen eines Clusters implementiert. Die Migration bewirkt, dass der Cluster neu gestartet wird. Wenn ein Cluster in eine andere Availability Zone verschoben wird, tritt ein Ausfall auf, bis der neue Cluster in der neuen Availability Zone wieder online ist. Sie müssen jedoch keine Änderungen an Ihren Anwendungen vornehmen, da der Clusterendpunkt auch nach dem Verschieben des Clusters in die neue Availability Zone unverändert bleibt.

Die Cluster-Verschiebung ist standardmäßig auf allen RA3-Clustern deaktiviert. Amazon Redshift weist beim Erstellen eines bereitgestellten Clusters 5439 als Standardport zu. Sie können zu einem anderen Port aus dem Portbereich 5431–5455 oder 8191–8215 wechseln. (Wechseln Sie nicht zu einem Port außerhalb der Bereiche. Dies führt zu einem Fehler.) Um den Standardport für einen bereitgestellten Cluster zu ändern, verwenden Sie die Amazon Redshift Redshift-Konsole oder die Amazon Redshift Redshift-API. AWS CLI Um den Standardport für eine serverlose Arbeitsgruppe zu ändern, verwenden Sie die AWS CLI oder die Amazon Redshift Serverless API.

Wenn Sie die Verschiebung aktivieren und derzeit für den Zugriff auf Ihren Cluster die IP-Adresse des Führungsknotens verwenden, passen Sie diesen Zugriff an. Verwenden Sie stattdessen die IP-Adresse, die dem VPC-Endpunkt (Virtual Private Cloud) des Clusters zugeordnet ist. Um diese Cluster-IP-Adresse zu finden, suchen und verwenden Sie den VPC-Endpunkt im Bereich Network and security (Netzwerk und Sicherheit) auf der Cluster-Detailseite. Melden Sie sich bei der Amazon-VPC-Konsole an, um weitere Informationen zum VPC-Endpunkt zu erhalten.

Sie können auch den Befehl AWS Command Line Interface (AWS CLI) verwenden`describe-vpc-endpoints`, um die dem Endpunkt zugeordnete elastic network interface abzurufen. Sie können den Befehl `describe-network-interfaces` verwenden, um zugeordnete IP-Adresse abzurufen. Weitere Informationen zu Amazon Redshift AWS CLI Redshift-Befehlen finden Sie unter Verfügbare Befehle in der AWS CLI Befehlsreferenz.

> **Note**
>
> Zur Erinnerung: Die Cluster-Verschiebung ist keine Voraussetzung für die Konfiguration von zusätzlichen Redshift-Netzwerk-Features, wie beispielsweise den Features, die für die Notfallwiederherstellung oder andere Zwecke verwendet werden. Sie können sie beispielsweise durch regionsübergreifendes Kopieren von Snapshots ergänzen, um die Ausfallsicherheit Ihrer Umgebung zu erhöhen, sie ist jedoch nicht erforderlich. Sie muss auch nicht aktiviert werden, um die folgenden Features zu aktivieren:
>
> - Verbindung von einer konto- oder regionsübergreifenden VPC zu Redshift herstellen — Sie können eine Verbindung von einer AWS Virtual Private Cloud (VPC) zu einer anderen herstellen, die eine Redshift-Datenbank enthält. Dies erleichtert beispielsweise die Verwaltung des Client-Zugriffs von unterschiedlichen Konten oder VPCs aus, ohne dass lokaler VPC-Zugriff auf Identitäten bereitgestellt werden muss, die eine Verbindung zur Datenbank herstellen. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Amazon Redshift Serverless von einem Redshift-VPC-Endpunkt in einem anderen Konto oder einer anderen Region aus.
> - Einrichtung eines benutzerdefinierten Domain-Namens – Sie können für Ihren Amazon-Redshift-Cluster oder Ihre Amazon-Redshift-Serverless-Arbeitsgruppe einen benutzerdefinierten Domain-Namen (auch als benutzerdefinierte URL bezeichnet) erstellen, um den Endpunktnamen einprägsamer und einfacher zu gestalten. Weitere Informationen finden Sie unter Verwendung eines benutzerdefinierten Domain-Namens für Client-Verbindungen.

Einschränkungen

Beachten Sie die folgenden Einschränkungen, wenn Sie die Amazon-Redshift-Verschiebung verwenden:

- Aufgrund potenzieller Ressourceneinschränkungen in einer bestimmten Availability Zone ist die Clusterverschiebung unter Umständen nicht in allen Szenarien möglich. In diesem Fall verändert Amazon Redshift den ursprünglichen Cluster nicht.
- Die Verschiebung wird auf den Instance-Familien DC1, DC2 und DS2 nicht unterstützt.
- Sie können keinen regionsübergreifenden Umzug durchführen. AWS
- Die Amazon-Redshift-Verschiebung verwendet standardmäßig die Portnummer 5439. Sie können auch zu einem anderen Port in den Bereichen 5431–5455 oder 8191–8215 wechseln.

- Eine Verschiebung ist in folgenden Regionen verfügbar:
  - Region USA Ost (Ohio) (us-east-2)
  - Region USA Ost (Nord-Virginia) (us-east-1)
  - Region USA West (Nordkalifornien) (us-west-1)
  - Region USA West (Oregon) (us-west-2)
  - Region Asien-Pazifik (Melbourne) (ap-southeast-4)
  - Region Asien-Pazifik (Mumbai) (ap-south-1)
  - Region Asien-Pazifik (Seoul) (ap-northeast-2)
  - Region Asien-Pazifik (Singapur) (ap-southeast-1)
  - Region Asien-Pazifik (Sydney) (ap-southeast-2)
  - Region Asien-Pazifik (Tokio) (ap-northeast-1)
  - Region Kanada (Zentral) (ca-central-1)
  - Region Kanada West (Calgary) (ca-west-1)
  - Region Europa (Frankfurt) (eu-central-1)
  - Region Europa (Irland) (eu-west-1)
  - Region Europa (London) (eu-west-2)
  - Region Europa (Paris) (eu-west-3)
  - Region Europa (Stockholm) (eu-north-1)
  - Region Israel (Tel Aviv) (il-central-1)
  - Region Südamerika (São Paulo) (sa-east-1)

Aktivieren der Clusterverschiebung

Sie können die Cluster-Verlagerung über die Amazon Redshift Redshift-Konsole und die Amazon Redshift AWS CLI Redshift-API aktivieren und verwalten.

Um die Clusterverschiebung zu aktivieren, definieren Sie eine Subnetzgruppe, die mehrere Availability Zones umfasst. Wenn Amazon Redshift mehr als eine verfügbare Availability Zone identifiziert, wählt Amazon Redshift automatisch aus der Liste der verfügbaren Availability Zones, um den Cluster zu verschieben.

Nachdem die Verschiebung abgeschlossen ist, verwenden Sie denselben Endpunkt, um auf den Cluster zuzugreifen. Amazon Redshift löscht die Computing-Ressourcen des ursprünglichen Clusters und gibt sie an den Ressourcenpool zurück.

Verwalten der Verschiebung über die Konsole

Sie können die Einstellungen für die Clusterverschiebung über die Amazon-Redshift-Konsole verwalten.

Aktivieren der Verschiebung beim Erstellen eines neuen Clusters

Gehen Sie wie folgt vor, um die Verschiebung beim Erstellen eines neuen Clusters zu aktivieren.

So aktivieren Sie die Verschiebung für einen neuen Cluster

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus.
3. Wählen Sie Create cluster (Cluster erstellen), um einen neuen Cluster zu erstellen. Weitere Informationen zum Erstellen eines Clusters finden Sie unter Erstellen eines Amazon-Redshift-Beispielclusters im Handbuch Erste Schritte mit Amazon Redshift.
4. Wählen Sie unter Backup (Sicherung) bei Cluster relocation (Clusterverschiebung) Enabled (Aktiviert) aus. Standardmäßig ist die Verschiebung deaktiviert.
5. Wählen Sie Create cluster (Cluster erstellen).

Ändern der Verschiebung für einen vorhandenen Cluster

Gehen Sie wie folgt vor, um die Verschiebungseinstellungen eines vorhandenen Clusters zu ändern.

So ändern Sie die Verschiebungseinstellungen für einen vorhandenen Cluster

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Die Cluster für Ihr Konto in der aktuellen AWS Region werden aufgelistet. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie in der Liste den Namen des Clusters aus, den Sie ändern möchten. Die Cluster-Detailseite wird angezeigt.
4. Wählen Sie die Registerkarte Maintenance (Wartung) und dann im Bereich Backup details (Backup-Details) Edit (Bearbeiten).
5. Wählen Sie unter Backup (Sicherung) Enabled (Aktiviert) aus. Standardmäßig ist die Verschiebung deaktiviert.

6. Wählen Sie Modify Cluster (Cluster bearbeiten).

Verschieben eines Clusters

Gehen Sie wie folgt vor, um einen Cluster manuell in eine andere Availability Zone zu verschieben. Das ist besonders dann nützlich, wenn Sie Ihre Netzwerkeinrichtung in sekundären Availability Zones testen möchten oder wenn in der aktuellen Availability Zone Ressourceneinschränkungen auftreten.

So verschieben Sie einen Cluster in eine andere Availability Zone

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Die Cluster für Ihr Konto in der aktuellen AWS Region werden aufgelistet. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie in der Liste den Namen des Clusters aus, den Sie verschieben möchten. Die Cluster-Detailseite wird angezeigt.
4. Wählen Sie unter Actions (Aktionen) die Option Relocate (Verschieben). Die Seite Relocate cluster (Cluster verschieben) wird angezeigt.
5. (Optional) Wählen Sie eine Availability Zone aus. Wenn Sie keine Availability Zone auswählen, wählt Amazon Redshift diese für Sie aus.

Amazon Redshift startet die Verschiebung und zeigt den Cluster als „relocating“ (wird verschoben) an. Nach Abschluss der Verschiebung ändert sich der Clusterstatus zu „available“ (verfügbar).

Verwalten der Verschiebung mit der Amazon-Redshift-CLI

Sie können die Einstellungen für die Clusterverschiebung über die AWS -Befehlszeilenschnittstelle (Command Line Interface, CLI) verwalten.

Mit der AWS CLI erstellt der folgende Beispielbefehl einen Amazon Redshift Redshift-Cluster mit dem Namen**`mycluster`**, für den Relocation aktiviert ist.

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

Wenn Ihr aktueller Cluster einen anderen Port verwendet, müssen Sie die Einstellung so ändern, dass der Cluster einen Port aus dem Portbereich 5431–5455 oder 8191–8215 verwendet, bevor Sie ihn ändern, um die Verschiebung zu aktivieren. Der Standardwert ist 5439. Mit dem folgenden Beispielbefehl ändern Sie den Port, wenn Ihr Cluster keinen Port aus dem angegebenen Bereich verwendet.

```
aws redshift modify-cluster --cluster-identifier mycluster --port 5439
```

Der folgende Beispielbefehl enthält den availability-zone-relocation Parameter auf dem Amazon Redshift Redshift-Cluster.

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

Der folgende Beispielbefehl deaktiviert den availability-zone-relocation Parameter auf dem Amazon Redshift Redshift-Cluster.

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

Der folgende Beispielbefehl startet die Verschiebung für den Amazon-Redshift-Cluster.

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

Amazon-Redshift-Snapshots und -Sicherungen

Themen

- Übersicht über Snapshots
- Automatisierte Snapshots
- Zeitpläne für automatisierte Snapshots
- Format von Snapshot-Zeitplänen
- Manuelle Snapshots
- Verwalten der Snapshot-Speicherung
- Ausschluss von Tabellen von Snapshots
- Kopieren von Snapshots in eine andere AWS -Region

- Wiederherstellen eines Clusters aus einem Snapshot
- Wiederherstellen einer Tabelle aus einem Snapshot
- Freigeben eines Snapshots
- Verwalten von Snapshots mithilfe der Konsole
- Verwaltung von Snapshots mithilfe der AWS CLI und der Amazon Redshift Redshift-API
- Arbeiten mit AWS Backup

Übersicht über Snapshots

Snapshots sind point-in-time Backups eines Clusters. Es gibt zwei Arten von Snapshots: automatisierte und manuelle. Amazon Redshift speichert diese Snapshots intern in Amazon S3 unter Verwendung einer verschlüsselten Secure Sockets Layer (SSL)-Verbindung.

Amazon Redshift erstellt in regelmäßigen Abständen inkrementelle Snapshots und verfolgt so Änderungen am Cluster seit dem letzten automatisierten Snapshot nach. Automatisierte Snapshots speichern alle Daten, die erforderlich sind, um einen Cluster anhand eines Snapshots wiederherzustellen. Sie können mit einem Snapshot-Zeitplan steuern, wann automatisierte Snapshots erzeugt werden, oder jederzeit einen manuellen Snapshot erstellen.

Wenn Sie anhand eines Snapshots eine Wiederherstellung durchführen, erstellt Amazon Redshift einen neuen Cluster und stellt diesen bereit, bevor alle Daten geladen werden, sodass Sie umgehend mit dem Abfragen des neuen Clusters beginnen können. Der Cluster streamt auf Anfrage Daten vom Snapshot als Reaktion auf aktive Abfragen und lädt danach die restlichen Daten im Hintergrund.

Wenn Sie einen Cluster starten, können Sie den Aufbewahrungszeitraum für automatische und manuelle Snapshots festlegen. Sie können den standardmäßigen Aufbewahrungszeitraum für automatisierte und manuelle Snapshots ändern, indem Sie den Cluster modifizieren. Sie können den Aufbewahrungszeitraum für manuelle Snapshots festlegen, wenn Sie den Snapshot erstellen, und ihn ändern, indem Sie den Snapshot modifizieren.

Sie können den Fortschritt von Snapshots überwachen AWS Management Console, indem Sie die Snapshot-Details in der anzeigen oder die CLI- oder DescribeClusterSnapshotsAPI-Aktion aufrufen describe-cluster-snapshots. Für einen Snapshot in Bearbeitung werden Informationen wie die Größe des schrittweisen Snapshot, die Übertragungsrate, die verstrichene Zeit und die geschätzte Restzeit angezeigt.

Amazon Redshift speichert Snapshots in einem intern verwalteten Amazon-S3-Bucket, der von Amazon Redshift verwaltet wird, um sicherzustellen, dass Ihre Backups dem Cluster immer zur

Verfügung stehen. Um die Speichergebühren zu verwalten, schätzen Sie ab, wie viele Tage Sie automatisierte Snapshots behalten müssen, und konfigurieren Sie dann den Aufbewahrungszeitraum entsprechend. Löschen Sie manuelle Snapshots, die nicht mehr benötigt werden. Weitere Informationen zu den Kosten von Backup-Speicher finden Sie auf der Seite Amazon Redshift – Preise.

Arbeiten mit Snapshots und Backups in Amazon Redshift Serverless

Amazon Redshift Serverless ermöglicht es Ihnen, wie ein bereitgestellter Cluster, ein Backup als point-in-time Repräsentation der Objekte und Daten im Namespace zu erstellen. In Amazon Redshift Serverless gibt es zwei Arten von Backups: Snapshots, die manuell erstellt werden, und Wiederherstellungspunkte, die Amazon Redshift Serverless automatisch erstellt. Weitere Informationen zum Arbeiten mit Snapshots für Amazon Redshift Serverless finden Sie unter Arbeiten mit Snapshots und Wiederherstellungspunkten.

Sie können auch einen Snapshot aus einem bereitgestellten Cluster in einem serverlosen Namespace wiederherstellen. Weitere Informationen finden Sie unter Einen serverlosen Namespace aus einem Snapshot wiederherstellen.

Automatisierte Snapshots

Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Amazon Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erzeugt Amazon Redshift ungefähr alle acht Stunden oder nach 5 GB geänderten Daten pro Knoten einen Snapshot, je nachdem, was zuerst auftritt. Wenn Ihre Daten größer als 5 GB * der Anzahl der Knoten sind, beträgt die kürzeste Zeitspanne zwischen der Erstellung von automatisierten Snapshots 15 Minuten. Sie können alternativ mit einem Snapshot-Zeitplan steuern, wann automatisierte Snapshots erzeugt werden. Wenn Sie benutzerdefinierte Zeitpläne verwenden, beträgt die Mindestzeit zwischen automatisierten Snapshots eine Stunde. Automatisierte Snapshots werden standardmäßig aktiviert, wenn Sie einen Cluster erstellen.

Automatisierte Snapshots werden nach Ablauf eines Aufbewahrungszeitraums gelöscht. Der Standard-Aufbewahrungszeitraum beträgt einen Tag. Sie können ihn jedoch mit der Amazon-Redshift-Konsole oder programmgesteuert mit der Amazon Redshift API oder CLI ändern.

Zum Deaktivieren von automatischen Snapshots setzen Sie den Wert für den Aufbewahrungszeitraum auf null. Wenn Sie automatisierte Snapshots deaktivieren, erstellt Amazon Redshift keine Snapshots mehr und löscht alle vorhandenen automatisierten Snapshots für den Cluster. Sie können automatische Snapshots für RA3-Knotentypen nicht deaktivieren. Sie können

einen automatisierten Aufbewahrungszeitraum für den RA3-Knotentyp zwischen 1 und 35 Tagen festlegen.

Nur Amazon Redshift kann einen automatisierten Snapshot löschen. Sie können ihn manuell nicht löschen. Amazon Redshift löscht automatisierte Snapshots nach Ablauf ihres Aufbewahrungszeitraums, wenn Sie automatisierte Snapshots für den Cluster deaktivieren oder wenn Sie den Cluster löschen. Amazon Redshift behält den neuesten automatisierten Snapshot, bis Sie automatisierte Snapshots deaktivieren oder den Cluster löschen.

Wenn Sie einen automatisierten Snapshot für einen längeren Zeitraum behalten möchten, können Sie eine Kopie hiervon als einen manuellen Snapshot erstellen. Der automatisierte Snapshot wird bis zum Ende des Aufbewahrungszeitraums aufbewahrt, aber der entsprechende manuelle Snapshot wird aufbewahrt, bis Sie ihn manuell löschen oder das Ende des Aufbewahrungszeitraums erreicht ist.

Zeitpläne für automatisierte Snapshots

Erstellen Sie einen Snapshot-Zeitplan und fügen ihn an einen oder mehrere Cluster an, um präzise zu steuern, wann Snapshots erzeugt werden. Wenn Sie einen Snapshot-Zeitplan ändern, wird der Zeitplan für alle verknüpften Cluster angepasst. Ein Cluster ohne angefügten Snapshot-Zeitplan verwendet den standardmäßigen Zeitplan für automatisierte Snapshots.

Ein Snapshot-Zeitplan besteht aus einer Reihe von Zeitplanregeln. Sie können einen einfachen Zeitplan definieren, indem Sie Abstände festlegen, beispielsweise alle 8 oder 12 Stunden. Sie können auch Regeln hinzufügen, damit an bestimmten Wochentagen, zu festgelegten Zeiten oder während bestimmter Zeiträume Snapshots erstellt werden. Die Regeln können auch mithilfe von Unix-ähnlichen Cron-Ausdrücken definiert werden.

Format von Snapshot-Zeitplänen

Sie können in der Amazon-Redshift-Konsole einen Snapshot-Zeitplan erstellen. Fügen Sie einem Cluster einen Zeitplan an, um die Erstellung eines System-Snapshots auszulösen. Ein Zeitplan kann mehreren Clustern angefügt werden. Außerdem kann ein Zeitplan mehrere Cron-Definitionen zum Auslösen von Snapshots enthalten.

Sie können einen Plan für Snapshots mit einer Cron-Syntax definieren. Die Definition dieser Zeitpläne nutzt eine modifizierte, Unix-ähnliche cron-Syntax. Verwenden Sie die UTC-Zeitzone (Coordinated Universal Time), um die Zeit anzugeben. Zeitpläne können mit einer maximalen Häufigkeit von einer Stunde und einer Mindestgenauigkeit von einer Minute erstellt werden.

Modifizierte cron-Ausdrücke für Amazon Redshift haben 3 Pflichtfelder, die durch Leerzeichen voneinander getrennt sind.

Syntax

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

Felder	Werte	Platzhalter
Minuten	0-59	, - * /
Stunden	0–23	, - * /
D ay-of-month	1-31	, - * ? / L W
Monat	1-12 oder JAN-DEZ	, - * /
D ay-of-week	1-7 oder SUN-SAT	, - * ? / L #
Jahr	1970-2199	, - * /

Platzhalter

- Das Platzhalterzeichen , (Komma) schließt zusätzliche Werte ein. Im Feld `Day-of-week` würde `MON,WED,FRI` Montag, Mittwoch und Freitag abdecken. Die Gesamtwerte sind auf 24 pro Feld begrenzt.
- Das Platzhalterzeichen - (Bindestrich) gibt einen Bereich an. Im Feld `Hour` steht 1–15 für die Stunden 1 bis 15 des angegebenen Tags.
- Das Platzhalterzeichen * (Sternchen) steht für alle Werte im Feld. Im Feld `Hours` steht * für alle Stunden.
- Das Platzhalterzeichen / (Schrägstrich) steht für schrittweise Steigerungen. Im Feld `Hours` können Sie **`1/10`** eingeben, um jede 10. Stunde anzugeben, beginnend mit der ersten Stunde des Tages (z. B. 01:00, 11:00 und 21:00).
- Das Platzhalterzeichen ? (Fragezeichen) steht für einen Wert. In das `Day-of-month` Feld könntest du 7 eingeben, und wenn es dir egal wäre, welcher Wochentag der siebte war, könntest du eingeben? im ay-of-week D-Feld.

- Das Platzhalterzeichen L in den Feldern für `Day-of-month` oder `Day-of-week` gibt den letzten Tag des Monats oder der Woche an.
- Das Platzhalterzeichen W im Feld `Day-of-month` gibt einen Wochentag an. Im Feld `Day-of-month` gibt den `3W` den Tag an, der dem dritten Tag des Monats am nächsten ist.
- Der Platzhalter # im ay-of-week Feld D gibt eine bestimmte Instanz des angegebenen Wochentags innerhalb eines Monats an. Beispiel: 3#2 steht für den zweiten Dienstag des Monats: Die 3 bezieht sich auf Dienstag, da dies der dritte Tag jeder Woche ist, und die 2 bezieht sich auf den zweiten Tag dieses Typs innerhalb des Monats.

> **Note**
>
> Wenn Sie das Zeichen '#' verwenden, können Sie nur einen Ausdruck in dem day-of-week Feld definieren. Beispielsweise ist "3#1,6#3" ungültig, da dies als zwei Ausdrücke interpretiert wird.

Einschränkungen

- Es ist nicht möglich, die Felder `Day-of-month` und `Day-of-week` im gleichen Cron-Ausdruck anzugeben. Wenn Sie einen Wert in einem der Felder angeben, müssen Sie in dem anderen Feld ein ? (Fragezeichen) eingeben.
- Snapshot-Zeitpläne unterstützen folgende Häufigkeiten nicht:
  - Häufiger als einmal pro Stunde geplante Snapshots.
  - Seltener als einmal pro Tag (24 Stunden) geplante Snapshots.

  Wenn Zeitpläne sich so überschneiden, dass Snapshots innerhalb eines Fensters von 1 Stunde geplant werden, wird ein Validierungsfehler erzeugt.

Wenn Sie einen Zeitplan erstellen, können Sie die folgenden Beispiel-Cron-Strings verwenden.

Minuten	Stunden	Wochentag	Bedeutung			
0	14-20/1	TUE	Jede Stunde zwischen 14:00 und 20:00 Uhr am Dienstag.			

Minuten	Stunden	Wochentag	Bedeutung
0	21	MO-FR	Von Montag bis Freitag jeden Abend um 21.00 Uhr.
30	0/6	SAT-SUN	Inkrementell alle 6 Stunden am Samstag und Sonntag, beginnend 30 Minuten nach Mitternacht (00:30) an diesem Tag. Das Ergebnis ist ein Snapshot um [00:30, 06:30, 12:30 und 18:30] Uhr am jeweiligen Tag.
30	12/4	*	Inkrementell alle 4 Stunden jeden Tag, beginnend um 12:30 Uhr. Das ergibt [12:30, 16:30, 20:30] Uhr.

Beispiel: Sie möchten einen Zeitplan jeden Tag beginnend um 15:15 Uhr inkrementell alle 2 Stunden ausführen. Das ergibt [15:15, 17:15, 19:15, 21:15, 23:15] Uhr. Geben Sie dafür Folgendes an:

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

Sie können einem Zeitplan mehrere Cron-Zeitplandefinitionen hinzufügen. Der folgende AWS CLI Befehl enthält beispielsweise zwei Cron-Zeitpläne in einem Zeitplan.

```
create-snapshot-schedule --schedule-identifier "my-test" --schedule-definition "cron(0
 17 SAT,SUN)" "cron(0 9,17 MON-FRI)"
```

Manuelle Snapshots

Sie können jederzeit einen manuellen Snapshot erstellen. Manuelle Snapshots werden standardmäßig sogar nach dem Löschen Ihres Clusters beliebig lange aufbewahrt. Sie können den Aufbewahrungszeitraum für manuelle Snapshots festlegen, wenn Sie den Snapshot erstellen, und ihn ändern, indem Sie den Snapshot modifizieren. Weitere Informationen zum Ändern des Aufbewahrungszeitraums finden Sie unter Ändern des Aufbewahrungszeitraums für manuelle Snapshots.

Nachdem Sie einen Snapshot gelöscht haben, können Sie keine neuen Operationen starten, die auf diesen Snapshot verweisen. Wenn jedoch ein Wiederherstellungsvorgang läuft, wird dieser Wiederherstellungsvorgang vollständig abgeschlossen.

Amazon Redshift hat ein Kontingent, das die Gesamtzahl der manuellen Snapshots begrenzt, die Sie erstellen können. Dieses Kontingent gilt pro AWS AWS Konto und Region. Das Standardkontingent ist unter Kontingente und Limits in Amazon Redshift aufgeführt.

Verwalten der Snapshot-Speicherung

Da für Snapshots Speicherkosten anfallen, ist es wichtig, sie zu löschen, wenn Sie sie nicht mehr benötigen. Amazon Redshift löscht automatisierte und manuelle Snapshots nach Ablauf ihres jeweiligen Aufbewahrungszeitraums. Sie können manuelle Snapshots auch mit dem AWS Management Console oder mit dem batch-delete-cluster-snapshotsCLI-Befehl löschen.

Sie können den Aufbewahrungszeitraum für einen manuellen Snapshots ändern, indem Sie die Einstellungen für manuelle Snapshots anpassen.

Informationen zu dem von Ihren Snapshots belegten Speicher erhalten Sie über die Amazon-Redshift-Konsole oder über den CLI-Befehl describe-storage.

Ausschluss von Tabellen von Snapshots

Standardgemäß sind alle benutzerdefinierten, dauerhaften Tabellen in Snapshots enthalten. Wenn eine Tabelle wie die Staging-Tabelle nicht gesichert werden muss, können Sie die Zeit, die zum Erstellen von Snapshots und zum Wiederherstellen aus Snapshots erforderlich ist, beträchtlich reduzieren. Sie können auch den Speicherplatz auf Amazon S3 reduzieren, indem Sie keine Sicherungstabelle verwenden. Zum Erstellen einer Tabelle ohne Sicherung berücksichtigen Sie den

BACKUP NO-Parameter beim Erstellen der Tabelle. Weitere Informationen finden Sie unter CREATE TABLE und CREATE TABLE AS im Datenbankentwicklerhandbuch zu Amazon Redshift.

Kopieren von Snapshots in eine andere AWS -Region

Sie können Amazon Redshift so konfigurieren, dass Snapshots (automatisiert oder manuell) für einen Cluster automatisch in eine andere AWS Region kopiert werden. Wenn ein Snapshot in der primären AWS Region des Clusters erstellt wird, wird er in eine sekundäre AWS Region kopiert. Die beiden AWS Regionen werden jeweils als AWS Quellregion und AWS Zielregion bezeichnet. Wenn Sie eine Kopie Ihrer Snapshots in einer anderen AWS Region speichern, können Sie Ihren Cluster aus aktuellen Daten wiederherstellen, falls sich etwas auf die primäre AWS Region auswirkt. Sie können Ihren Cluster so konfigurieren, dass Snapshots jeweils nur in eine AWS Zielregion kopiert werden. Die Liste der Amazon-Redshift-Regionen finden Sie unter Regionen und Endpunkte in der Allgemeine Amazon Web Services-Referenz.

Wenn Sie Amazon Redshift aktivieren, um Snapshots automatisch in eine andere AWS Region zu kopieren, geben Sie die AWS Zielregion an, in die die Snapshots kopiert werden sollen. Für automatisierte Snapshots können Sie auch den Aufbewahrungszeitraum angeben, in dem sie in der Zielregion aufbewahrt werden sollen. AWS Nachdem ein automatisierter Snapshot in die AWS Zielregion kopiert wurde und dort den Aufbewahrungszeitraum erreicht hat, wird er aus der AWS Zielregion gelöscht. Dadurch bleibt Ihre Snapshot-Nutzung gering. Um die automatisierten Snapshots für einen kürzeren oder längeren Zeitraum in der AWS Zielregion aufzubewahren, ändern Sie diesen Aufbewahrungszeitraum.

Die Aufbewahrungsdauer, die Sie für automatische Snapshots festlegen, die in die AWS Zielregion kopiert werden, unterscheidet sich von der Aufbewahrungsdauer für automatische Snapshots in der Quellregion. AWS Der Standardaufbewahrungszeitraum für kopierte Snapshots beträgt sieben Tage. Dieser Zeitraum von sieben Tagen gilt nur für automatisierte Snapshots. Sowohl in der Quell- als auch in der Ziel- AWS -Region werden manuelle Snapshots nach Ablauf des Snapshot-Aufbewahrungszeitraums gelöscht bzw. dann, wenn Sie sie manuell löschen.

Sie können die automatische Snapshot-Kopie für einen Cluster jederzeit deaktivieren. Wenn Sie diese Funktion deaktivieren, werden Snapshots nicht mehr von der AWS Quellregion in die Zielregion kopiert. AWS Alle automatisierten Snapshots, die in die AWS Zielregion kopiert wurden, werden gelöscht, sobald sie die Aufbewahrungsfrist erreicht haben, es sei denn, Sie erstellen manuelle Snapshot-Kopien von ihnen. Diese manuellen Snapshots und alle manuellen Snapshots, die aus der AWS Zielregion kopiert wurden, werden in der AWS Zielregion aufbewahrt, bis Sie sie manuell löschen.

Um die AWS Zielregion zu ändern, in die Sie Snapshots kopieren, deaktivieren Sie zunächst die automatische Kopierfunktion. Aktivieren Sie sie dann wieder unter Angabe der neuen AWS -Zielregion.

Nachdem ein Snapshot in die AWS Zielregion kopiert wurde, wird er aktiv und steht für Wiederherstellungszwecke zur Verfügung.

Um Snapshots für AWS KMS—verschlüsselte Cluster in eine andere AWS Region zu kopieren, gewähren Sie Amazon Redshift die Nutzung eines vom Kunden verwalteten Schlüssels in der Zielregion. AWS Wählen Sie dann diesen Zuschuss aus, wenn Sie das Kopieren von Snapshots in der Quellregion aktivieren. AWS Weitere Informationen zur Konfiguration von Erteilungen von Snapshots-Kopien finden Sie unter Kopieren von —verschlüsselten Snapshots in eine andere Region AWS KMSAWS.

Wiederherstellen eines Clusters aus einem Snapshot

Ein Snapshot enthält Daten aus Datenbanken, die auf Ihrem Cluster ausgeführt werden. Dazu enthält er Informationen zu Ihrem Cluster, darunter die Anzahl der Knoten, den Knotentyp und den Admin-Benutzernamen. Wenn Sie einen Cluster aus einem Snapshot wiederherstellen, verwendet Amazon Redshift die Cluster-Informationen zur Erstellung eines neuen Clusters. Dann werden alle Datenbanken aus den Snapshot-Daten wiederhergestellt.

Für den aus dem ursprünglichen Snapshot wiederhergestellten neuen Cluster können Sie die Konfiguration auswählen, etwa den Knotentyp und die Anzahl der Knoten. Der Cluster wird in derselben AWS -Region und in einer zufällig vom System ausgewählten Availability Zone wiederhergestellt, es sei denn, Sie geben in Ihrer Anforderung eine andere Availability Zone an. Wenn Sie einen Cluster anhand eines Snapshots wiederherstellen, können Sie optional eine kompatible Wartungsspur für den neuen Cluster auswählen.

> **Note**
>
> Wenn Sie einen Snapshot zu einem Cluster mit einer anderen Konfiguration wiederherstellen, muss der Snapshot auf einem Cluster mit Clusterversion 1.0.10013 oder höher erstellt worden sein.

Während eine Wiederherstellung ausgeführt wird, werden Ereignisse in der Regel in der folgenden Reihenfolge ausgegeben:

1. RESTORE_STARTED – REDSHIFT-EVENT-2008 wird gesendet, wenn der Wiederherstellungsprozess beginnt.
2. RESTORE_SUCCEEDED – REDSHIFT-EVENT-3003 wird gesendet, wenn der neue Cluster erstellt wurde.

   Der Cluster ist für Abfragen verfügbar.
3. DATA_TRANSFER_COMPLETED — REDSHIFT-EVENT-3537 wird gesendet, wenn die Datenübertragung abgeschlossen ist.

> **Note**
>
> RA3-Cluster geben nur RESTORE_STARTED- und RESTORE_SUCCEEDED-Ereignisse aus. Es gibt keine explizite Datenübertragung, die erfolgen muss, nachdem ein RESTORE erfolgreich war, da RA3-Knotentypen Daten in von Amazon Redshift verwaltetem Speicher speichern. Bei RA3-Knoten werden Daten im Rahmen der normalen Abfrageverarbeitung kontinuierlich zwischen RA3-Knoten und dem von Amazon Redshift verwalteten Speicher übertragen. RA3-Knoten speichern aktive Daten lokal und weniger häufig abgefragte Blöcke automatisch in von Amazon Redshift verwaltetem Speicher.

Sie können den Fortschritt einer Wiederherstellung überwachen, indem Sie entweder den DescribeClustersAPI-Vorgang aufrufen oder die Clusterdetails in der AWS Management Console anzeigen. Für eine Wiederherstellung in Bearbeitung werden Informationen wie die Größe der Snapshot-Daten, die Übertragungsrate, die verstrichene Zeit und die geschätzte Restzeit angezeigt. Eine Beschreibung dieser Metriken finden Sie unter RestoreStatus.

Sie können einen Snapshot nicht zum Wiederherstellen eines aktiven Clusters in einen vorherigen Status verwenden.

> **Note**
>
> Wenn Sie einen Snapshot in einen neuen Cluster wiederherstellen, werden die Standardsicherheitsgruppe und -parametergruppe verwendet, sofern Sie keine anderen Werte angeben.

Möglicherweise möchten Sie aus den folgenden Gründen einen Snapshot zu einem Cluster mit einer anderen Konfiguration wiederherstellen:

- Wenn ein Cluster aus kleineren Knotentypen besteht und Sie ihn zu einem größeren Knotentyp mit weniger Knoten konsolidieren möchten.
- Wenn Sie Ihre Workloads beobachtet haben und feststellen, dass Sie einen Knotentyp mit mehr CPU-Leistung und Speicherplatz benötigen.
- Wenn Sie die Leistung von Test-Workloads mit anderen Knotentypen messen möchten.

Für die Wiederherstellung gelten die folgenden Einschränkungen:

- Die neue Knotenkonfiguration muss über genügend Speicherplatz für vorhandene Daten verfügen. Auch wenn Sie Knoten hinzufügen, verfügt Ihre neue Konfiguration möglicherweise aufgrund der Verteilung der Daten nicht über ausreichend Speicherplatz.
- Der Wiederherstellungsvorgang überprüft, ob der Snapshot auf einer Cluster-Version erstellt wurde, die mit der Cluster-Version des neuen Clusters kompatibel ist. Wenn die Versionsebene des neuen Clusters zu früh ist, schlägt der Wiederherstellungsvorgang fehl und weitere Informationen werden in einer Fehlermeldung ausgegeben.
- Welche möglichen Konfigurationen (Knotenanzahl und Knotentyp) Sie wiederherstellen können, ist von der Anzahl der Knoten im ursprünglichen Cluster und dem Zielknotentyp des neuen Clusters abhängig. Um die möglichen verfügbaren Konfigurationen zu ermitteln, können Sie die Amazon Redshift Redshift-Konsole oder den `describe-node-configuration-options` AWS CLI Befehl mit `action-type restore-cluster` verwenden. Weitere Informationen zur Wiederherstellung mithilfe der Amazon-Redshift-Konsole finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot.

Die folgenden Schritte basieren auf einem Cluster mit zahlreichen Knoten und konsolidieren diesen zu einem größeren Knotentyp mit einer geringeren Zahl von Knoten mit AWS CLI. Für dieses Beispiel beginnen wir mit einem Quell-Cluster mit 24 `ds2.xlarge`-Knoten. Für diesen Fall nehmen wir an, dass wir bereits einen Snapshot dieses Clusters erstellt haben und diesen jetzt zu einem größeren Knotentyp wiederherstellen möpchten.

1. Führen Sie den folgenden Befehl aus, um die Details zu unserem 24-Knoten-`ds2.xlarge`-Cluster abzurufen.

```
aws redshift describe-clusters --region eu-west-1 --cluster-identifier
 mycluster-123456789012
```

2. Führen Sie den folgenden Befehl aus, um die Details des Snapshots abzurufen.

```
aws redshift describe-cluster-snapshots --region eu-west-1 --snapshot-identifier
 mycluster-snapshot
```

3. Führen Sie den folgenden Befehl aus, um die für diesen Snapshot verfügbaren Optionen zu beschreiben.

```
aws redshift describe-node-configuration-options --snapshot-identifier mycluster-
snapshot --region eu-west-1 --action-type restore-cluster
```

Dieser Befehl gibt eine Optionenliste mit empfohlenen Knotentypen, der Knotenanzahl und der Festplattennutzung für jede Option aus. Bei diesem Beispiel listet der obige Befehl die folgenden möglichen Knotenkonfigurationen auf. Wir entscheiden uns für die Wiederherstellung zu einem `ds2.8xlarge`-Cluster mit drei Knoten.

```
{
    "NodeConfigurationOptionList": [
        {
            "EstimatedDiskUtilizationPercent": 65.26134808858235,
            "NodeType": "ds2.xlarge",
            "NumberOfNodes": 24
        },
        {
            "EstimatedDiskUtilizationPercent": 32.630674044291176,
            "NodeType": "ds2.xlarge",
            "NumberOfNodes": 48
        },
        {
            "EstimatedDiskUtilizationPercent": 65.26134808858235,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 3
        },
        {
            "EstimatedDiskUtilizationPercent": 48.94601106643677,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 4
        },
```

```
        {
            "EstimatedDiskUtilizationPercent": 39.156808853149414,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 5
        },
        {
            "EstimatedDiskUtilizationPercent": 32.630674044291176,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 6
        }
    ]
}
```

4. Führen Sie den folgenden Befehl aus, um den Snapshot zu der von uns gewählten Clusterkonfiguration wiederherzustellen. Nach der Wiederherstellung dieses Clusters haben wir denselben Inhalt wie der Quell-Cluster, wobei die Daten aber in drei `ds2.8xlarge`-Knoten konsolidiert wurden.

```
aws redshift restore-from-cluster-snapshot --region eu-west-1 --snapshot-identifier
 mycluster-snapshot --cluster-identifier mycluster-123456789012-x --node-type
 ds2.8xlarge --number-of-nodes 3
```

Wenn Sie reservierte Knoten haben, zum Beispiel reservierte DS2- oder DC2-Knoten, können Sie auf reservierte RA3-Knoten aktualisieren. Sie können dies tun, wenn Sie eine Wiederherstellung von einem Snapshot oder eine elastische Größenänderung durchführen. Sie können die Konsole verwenden, um sich durch den Prozess führen zu lassen. Weitere Informationen zum Aktualisieren auf RA3-Knoten finden Sie unter Migration zu RA3-Knotentypen.

Wiederherstellen einer Tabelle aus einem Snapshot

Sie können eine einzelne Tabelle aus einem Snapshot anstellen eines gesamten Clusters wiederherstellen. Wenn Sie eine einzelne Tabelle aus eine Snapshot wiederherstellen, geben Sie Quell-Snapshot, -Datenbank, -Schema und -Tabellennamen sowie Ziel-Datenbank und -Schema und einen neuen Tabellennamen für die wiederhergestellte Tabelle an.

Der neue Tabellenname kann nicht identisch sein mit dem Namen einer bestehenden Tabelle. Um eine bestehende Tabelle durch eine wiederhergestellte Tabelle aus einem Snapshot zu ersetzen, sollten Sie die Tabelle umbenennen oder die bestehende Tabelle ablegen, bevor Sie die Tabelle aus dem Snapshot wiederherstellen.

Die Zieltabelle wird mithilfe der Spaltendefinitionen, Tabellenattribute und Spaltenattribute der Quelltabelle erstellt. Eine Ausnahme gilt für Fremdschlüssel. Um Konflikte aufgrund von Abhängigkeiten zu vermeiden, übernimmt die Zieltabelle keine Fremdschlüssel von der Quelltabelle. Alle Abhängigkeiten, wie z. B. Ansichten oder Berechtigungen, die für die Quelltabelle gewährt wurden, gelten nicht für die Zieltabelle.

Wenn der Eigentümer der Quelltabelle existiert, dann ist der Datenbankbenutzer der Eigentümer der wiederhergestellten Tabelle, vorausgesetzt, dieser Benutzer verfügt über ausreichend Berechtigungen, um der Eigentümer einer Beziehung in der angegebenen Datenbank und dem Schema zu sein. Anderenfalls ist die wiederhergestellte Tabelle Besitz des Adminbenutzers, der beim Starten des Clusters angelegt wurde.

Die wiederhergestellte Tabelle wird wieder in den Status zurückgesetzt, in dem sie sich zum Zeitpunkt der Sicherung befunden hat. Dazu gehören Sichtbarkeitsregeln für die Transaktion, die durch die Einhaltung der serialisierbaren Isolation durch Amazon Redshift definiert sind. Das heißt, dass Daten für derzeit übertragene Transaktionen, die nach dem Backup gestartet wurden, sofort sichtbar sind.

Die Wiederherstellung einer Tabelle aus einem Snapshot unterliegt folgenden Beschränkungen:

- Sie können eine Tabelle aus dem aktuellen, aktiv laufenden Cluster und aus einem Snapshot wiederherstellen, der aus diesem Cluster erstellt wurde.
- Sie können jeweils nur eine Tabelle wiederherstellen.
- Sie können keine Tabelle aus einem Cluster-Snapshot wiederherstellen, der erstellt wurde, bevor die Größe des Clusters verändert wurde. Eine Ausnahme ist jedoch, dass Sie eine Tabelle nach einer elastischen Größenänderung wiederherstellen können, wenn sich der Knotentyp nicht geändert hat.
- Alle Abhängigkeiten, wie z. B. Ansichten oder Berechtigungen, die für die Quelltabelle gewährt wurden, gelten nicht für die Zieltabelle.
- Wenn die Sicherheit auf Zeilenebene für die Wiederherstellung einer Tabelle aktiviert ist, stellt Amazon Redshift die Tabelle wieder her, wobei die Sicherheit auf Zeilenebene aktiviert ist.

So stellen Sie eine Tabelle aus einem Snapshot wieder her:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.

2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster aus, den Sie zur Wiederherstellung einer Tabelle verwenden möchten.
3. Wählen Sie für Actions (Aktionen) Restore table (Tabelle wiederherstellen) aus, um die Seite Restore table (Tabelle wiederherstellen) anzuzeigen.
4. Geben Sie die Informationen darüber ein, welchen Snapshot, welche Quelltabelle und welche Zieltabelle Sie verwenden möchten. Wählen Sie dann Restore table (Tabelle wiederherstellen) aus.

Example Beispiel: Wiederherstellen einer Tabelle aus einem Snapshot mithilfe des AWS CLI

Im folgenden Beispiel wird der `restore-table-from-cluster-snapshot` AWS CLI Befehl verwendet, um die `my-source-table` Tabelle aus dem `sample-database` Schema in der wiederherzustellen`my-snapshot-id`. Sie können den AWS CLI Befehl verwenden`describe-table-restore-status`, um den Status Ihres Wiederherstellungsvorgangs zu überprüfen. Bei diesem Beispiel wird der Snapshot in das Cluster `mycluster-example` mit einem neuen Tabellennamen `my-new-table` wiederhergestellt.

```
aws redshift restore-table-from-cluster-snapshot --cluster-identifier mycluster-
example
                                                 --new-table-name my-new-table
                                                 --snapshot-identifier my-snapshot-id
                                                 --source-database-name sample-
database
                                                 --source-table-name my-source-table
```

Freigeben eines Snapshots

Sie können einen vorhandenen manuellen Snapshot mit anderen AWS Kundenkonten teilen, indem Sie den Zugriff auf den Snapshot autorisieren. Sie können bis zu 20 für jeden Snapshot und 100 für jeden AWS Key Management Service (AWS KMS) Schlüssel autorisieren. Das heißt, wenn Sie über 10 Snapshots verfügen, die mit einem einzigen KMS-Schlüssel verschlüsselt sind, können Sie 10 AWS Konten für die Wiederherstellung jedes Snapshots autorisieren oder andere Kombinationen, die bis zu 100 Konten hinzufügen und 20 Konten pro Snapshot nicht überschreiten. Eine Person, die als ein Benutzer in einem der genehmigten Konten angemeldet ist, kann dann den Snapshot beschreiben oder ihn wiederherstellen, um einen neuen Amazon-Redshift-Cluster unter ihrem Konto zu erstellen. Wenn Sie beispielsweise separate AWS Kundenkonten für Produktion und Test

verwenden, kann sich ein Benutzer mit dem Produktionskonto anmelden und einen Snapshot mit Benutzern im Testkonto teilen. Jemand, der sich als Testkonto-Benutzer angemeldet hat, kann dann den Snapshot wiederherstellen, um einen neuen Cluster für Test- oder Diagnosearbeiten zu erstellen, der Eigentum des Testkontos ist.

Ein manueller Snapshot gehört dauerhaft dem AWS Kundenkonto, unter dem er erstellt wurde. Nur Benutzer im Konto, dem der Snapshot gehört, könnten anderen Konten die Berechtigung zum Zugriff auf den Snapshot gewähren oder solche Berechtigung wieder entziehen. Benutzer in den genehmigten Konten können nur einen Snapshot beschreiben oder wiederherstellen, der für sie freigegeben wurde; sie können keine Snapshots kopieren oder löschen, die für sie freigegeben wurden. Eine Berechtigung bleibt gültig, bis der Eigentümer des Snapshot sie widerruft. Wird eine Berechtigung widerrufen, verliert der zuvor autorisierte Benutzer die Sichtbarkeit für den Snapshot und kann keine neuen Aktionen starten, die auf den Snapshot verweisen. Wenn das Konto dabei ist, den Snapshot wiederherzustellen, wenn der Zugriff widerrufen wird, wird die Wiederherstellung vollständig abgeschlossen. Sie können keinen Snapshot löschen, während aktive Berechtigungen vorliegen; Sie müssen zuerst alle Berechtigungen widerrufen.

AWS Kundenkonten sind immer berechtigt, auf Snapshots zuzugreifen, die dem Konto gehören. Bei Versuchen, den Zugriff zum Eigentümerkonto zu genehmigen oder zu widerrufen, erscheint eine Fehlermeldung. Sie können einen Snapshot, der einem inaktiven AWS Kundenkonto gehört, nicht wiederherstellen oder beschreiben.

Nachdem Sie den Zugriff auf ein AWS Kundenkonto autorisiert haben, können Benutzer dieses Kontos keine Aktionen an dem Snapshot ausführen, es sei denn, sie übernehmen eine Rolle mit Richtlinien, die ihnen dies ermöglichen.

- Benutzer im Snapshot-Besitzerkonto können nur dann den Zugriff auf einen Snapshot genehmigen oder widerrufen, wenn sie eine Rolle mit einer IAM-Richtlinie übernehmen, die ihnen die Durchführung solcher Aktionen mit einer Ressourcenspezifikation erlauben, die den Snapshot beinhaltet. Die folgende Richtlinie ermöglicht es beispielsweise einem Benutzer oder einer Rolle in einem AWS Konto, anderen Konten `012345678912` den Zugriff auf einen Snapshot mit dem Namen `my-snapshot20130829` zu autorisieren:

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
```

```
          "redshift:AuthorizeSnapshotAccess",
          "redshift:RevokeSnapshotAccess"
          ],
      "Resource":[
           "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-snapshot20130829"
          ]
    }
  ]
}
```

- Benutzer in einem AWS Konto, mit dem ein Snapshot geteilt wurde, können keine Aktionen für diesen Snapshot ausführen, es sei denn, sie verfügen über die entsprechenden Berechtigungen. Weisen Sie dazu die Richtlinie einer Rolle zu und übernehmen Sie die Rolle.
  - Um einen Snapshot aufzulisten oder zu beschreiben, muss eine IAM-Richtlinie vorliegen, die die `DescribeClusterSnapshots`-Aktion erlaubt. Der folgende Code zeigt ein Beispiel dafür:

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

  - Um einen Snapshot wiederherzustellen, muss ein Benutzer eine Rolle mit einer IAM-Richtlinie übernehmen, die die Aktion `RestoreFromClusterSnapshot` erlaubt, und über ein Ressourcenelement verfügen, das sowohl den Cluster, den er versucht zu erstellen, als auch den Snapshot abdeckt. Wenn beispielsweise ein Benutzer in einem Konto `012345678912` den Snapshot `my-snapshot20130829` für Konto `219876543210` freigegeben hat, um durch Wiederherstellen des Snapshot einen Cluster zu erstellen, muss ein Benutzer im Konto `219876543210` eine Rolle mit einer Richtlinie wie die folgende übernehmen:

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

- Nachdem einem AWS Konto der Zugriff auf einen Snapshot entzogen wurde, können keine Benutzer in diesem Konto auf den Snapshot zugreifen. Dies ist auch der Fall, wenn diese Konten über IAM-Richtlinien verfügen, die Aktionen für die zuvor freigegebene Snapshot-Ressource zulassen.

Verwalten von Snapshots mithilfe der Konsole

Amazon Redshift erstellt regelmäßig automatische inkrementelle Snapshots Ihrer Daten und speichert diese in Amazon S3. Sie können natürlich außerdem bei Bedarf jederzeit manuell Snapshots Ihrer Daten erstellen. In diesem Abschnitt erfahren Sie, wie Sie Ihre Snapshots von der Amazon-Redshift-Konsole aus verwalten. Weitere Informationen zu -Snapshots finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.

Ausgangspunkt aller Snapshot-Aufgaben in der Amazon-Redshift-Konsole ist die Snapshot-Liste. Sie können diese Liste nach einem Zeitbereich, dem Snapshottyp und dem Cluster des Snapshots filtern. Außerdem können Sie die Liste nach Datum, Größe und Snapshot-Typ sortieren. Abhängig vom ausgewählten Snapshot-Typ stehen Ihnen möglicherweise verschiedene Optionen für die Arbeit mit dem Snapshot zur Verfügung.

Themen

- Erstellen eines Snapshot-Zeitplans
- Erstellen eines manuellen Snapshot
- Ändern des Aufbewahrungszeitraums für manuelle Snapshots
- Löschen von manuellen Snapshots

- Kopieren eines automatisierten Snapshot
- Wiederherstellen eines Clusters aus einem Snapshot
- Wiederherstellen eines Serverless-Namespace aus einem Snapshot
- Freigeben eines Cluster-Snapshots
- Konfigurieren von regionenübergreifenden Snapshot-Kopien für nicht verschlüsselte Cluster
- Konfigurieren Sie die regionsübergreifende Snapshot-Kopie für einen AWS KMS—verschlüsselten Cluster
- Ändern des Aufbewahrungszeitraums für regionenübergreifende Snapshot-Kopien

Erstellen eines Snapshot-Zeitplans

Erstellen Sie einen Snapshot-Zeitplan und fügen ihn an einen oder mehrere Cluster an, um präzise zu steuern, wann Snapshots erzeugt werden. Sie können einen Zeitplan anfügen, wenn Sie einen Cluster erstellen oder indem Sie den Cluster ändern. Weitere Informationen finden Sie unter Zeitpläne für automatisierte Snapshots.

So erstellen Sie einen Snapshot-Zeitplan

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster), Snapshots und dann die Registerkarte Snapshot schedules (Snapshot-Zeitpläne) aus. Die Snapshot-Zeitpläne werden angezeigt.
3. Wählen Sie Add schedule (Zeitplan hinzufügen) aus, um die Seite zum Hinzufügen eines Zeitplans anzuzeigen.
4. Geben Sie die Eigenschaften der Zeitplandefinition ein und wählen Sie dann Add schedule (Zeitplan hinzufügen) aus.
5. Auf der angezeigten Seite können Sie Cluster an Ihren neuen Snapshot-Plan zuweisen und dann OK auswählen.

Erstellen eines manuellen Snapshot

Gehen Sie zum Erstellen eines manuellen Snapshots eines Clusters aus der Snapshotliste wie folgt vor. Bei einer alternative Methode zum Erstellen eines Clustersnapshots wird als Ausgangspunkt anstelle der Snapshotliste der Ausschnitt zur Konfigurierung der Cluster gewählt. Weitere Informationen finden Sie unter Erstellen eines Snapshots eines Clusters.

So erstellen Sie einen manuellen Snapshot

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster), Snapshots und dann Create snapshot (Snapshot erstellen) aus. Die Snapshot-Seite zum Erstellen eines manuellen Snapshots wird angezeigt.
3. Geben Sie die Eigenschaften der Snapshot-Definition ein und wählen Sie dann Create snapshot (Snapshot erstellen) aus. Es kann einige Zeit dauern, bis der Snapshot verfügbar ist.

Ändern des Aufbewahrungszeitraums für manuelle Snapshots

Sie können den Aufbewahrungszeitraum für einen manuellen Snapshots ändern, indem Sie die Einstellungen für Snapshots anpassen.

So ändern Sie den Aufbewahrungszeitraum für manuelle Snapshots

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster), Snapshots und dann den manuellen Snapshot aus, der geändert werden soll.
3. Wählen Sie für Actions (Aktionen) Manual snapshot settings (Manuelle Snapshot-Einstellungen) aus, um die Eigenschaften des manuellen Snapshots anzuzeigen.
4. Geben Sie die überarbeiteten Eigenschaften der Snapshot-Definition ein und wählen Sie dann Save (Speichern) aus.

Löschen von manuellen Snapshots

Sie können manuelle Snapshots löschen, indem Sie einen oder mehrere Snapshots in der Liste der Snapshots auswählen.

So löschen Sie einen manuellen Snapshot

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster), Snapshots und dann den zu löschenden Snapshot aus.

3. Wählen Sie für Actions (Aktionen) Delete snapshot (Snapshot löschen) aus, um den Snapshot zu löschen.
4. Bestätigen Sie das Löschen der aufgelisteten Snapshots und wählen Sie dann Delete (Löschen) aus.

Kopieren eines automatisierten Snapshot

Automatisierte Snapshots werden nach Ablauf ihrer Verwahrdauer automatisch gelöscht. Außerdem werden automatisierte Snapshots gelöscht, wenn Sie die Funktion zur automatischen Aufnahme von Snapshots deaktivieren oder wenn Sie den Cluster löschen, der sie enthält. Wenn Sie einen automatisierten Snapshot dauerhaft behalten möchten, kopieren Sie ihn in einen manuellen Snapshot.

So kopieren Sie einen automatisierten Snapshot

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster), Snapshots und dann den zu kopierenden Snapshot aus.
3. Wählen Sie für Actions (Aktionen) Copy automated snapshot (Automatischen Snapshot kopieren) aus, um den Snapshot zu kopieren.
4. Aktualisieren Sie die Eigenschaften des neuen Snapshots und wählen Sie dann Copy (Kopieren) aus.

Wiederherstellen eines Clusters aus einem Snapshot

Wenn Sie einen Cluster anhand eines Snapshots wiederherstellen, erstellt Amazon Redshift einen neuen Cluster mit allen Snapshot-Daten.

So stellen Sie einen Cluster mithilfe eines Snapshots wieder her

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster), Snapshots und dann den wiederherzustellenden Snapshot aus.

3. Wählen Sie Restore from snapshot (Aus Snapshot Wiederherstellen) aus, um die Werte Cluster configuration (Cluster-Konfiguration) und Cluster details (Cluster-Details) des neuen zu erstellenden Clusters unter Verwendung der Snapshot-Informationen anzuzeigen.
4. Aktualisieren Sie die Eigenschaften des neuen Clusters und wählen Sie dann Restore cluster from snapshot (Cluster aus Snapshot wiederherstellen) aus.

Falls wir das Admin-Passwort Ihres Clusters AWS Secrets Manager nicht verwaltet haben, können Sie es Ihren wiederhergestellten Cluster verwalten lassen, indem Sie AWS Secrets Manager im Abschnitt Cluster-Konfiguration die Option Administratoranmeldedaten verwalten auswählen und einen KSM-Schlüssel angeben. Andernfalls wird der Cluster mit den Administratoranmeldeinformationen wiederhergestellt, die er zum Zeitpunkt der Snapshot-Erstellung verwendet hat. Sie können die Administratoranmeldeinformationen des Clusters nach der Wiederherstellung auf der Seite mit den Cluster-Details aktualisieren.

Wenn Sie zum Zeitpunkt der Aufnahme des Screenshots das Admin-Passwort Ihres Clusters AWS Secrets Manager verwaltet haben, müssen Sie es weiterhin verwenden, AWS Secrets Manager um das Admin-Passwort zu verwalten. Sie haben die Möglichkeit, die Verwendung von Secrets nach der Wiederherstellung des Clusters durch Aktualisierung der Administratoranmeldeinformationen des Clusters auf der Seite mit den Cluster-Details zu deaktivieren.

Wenn Sie reservierte Knoten haben, zum Beispiel reservierte DS2- oder DC2-Knoten, können Sie auf reservierte RA3-Knoten aktualisieren. Sie können dies tun, wenn Sie eine Wiederherstellung von einem Snapshot oder eine elastische Größenänderung durchführen. Sie können die Konsole verwenden, um sich durch den Prozess führen zu lassen. Weitere Informationen zum Aktualisieren auf RA3-Knoten finden Sie unter Migration zu RA3-Knotentypen.

Wiederherstellen eines Serverless-Namespace aus einem Snapshot

Beim Wiederherstellen eines Serverless-Namespaces aus einem Snapshot werden alle Datenbanken des Namespaces durch Datenbanken im Snapshot ersetzt. Weitere Informationen zu Serverless-Snapshots finden Sie unter Arbeiten mit Snapshots und Wiederherstellungspunkten. Amazon Redshift konvertiert Tabellen mit verschachtelten Schlüsseln automatisch in zusammengesetzte Schlüssel, wenn Sie einen bereitgestellten Cluster-Snapshot in einem Amazon Redshift Serverless-Namespace wiederherstellen. Weitere Informationen zu Sortierschlüsseln finden Sie unter Arbeiten mit Sortierschlüsseln.

So stellen Sie einen Snapshot von Ihrem bereitgestellten Cluster in Ihrem Serverless-Namespace wieder her.

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster), Snapshots und dann den zu verwendenden Snapshot aus.
3. Wählen Sie Restore from snapshot (Aus Snapshot wiederherstellen), Restore to serverless namespace (In Serverless-Namespace wiederherstellen).
4. Wählen Sie den Namespace, in dem Sie wiederherstellen möchten.
5. Bestätigen Sie, dass Sie von Ihrem Snapshot aus wiederherstellen möchten. Wählen Sie restore (Wiederherstellen) aus. Diese Aktion ersetzt alle Datenbanken im Serverless-Namespace durch die Daten aus Ihrem bereitgestellten Cluster.

Freigeben eines Cluster-Snapshots

Sie können anderen Benutzern die Berechtigung erteilen, auf ausgewählte manuelle Snapshots von Ihnen zuzugreifen, und Sie können diese Berechtigungen auch wieder entziehen, wenn sie nicht mehr benötigt werden.

So geben Sie einen Snapshot für ein anderes -Konto frei

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster), Snapshots und dann den manuellen Snapshot aus, der freigegeben werden soll.
3. Wählen Sie für Actions (Aktionen) Manual snapshot settings (Manuelle Snapshot-Einstellungen) aus, um die Eigenschaften des manuellen Snapshots anzuzeigen.
4. Geben Sie im Abschnitt Manage access (Zugriff verwalten) das oder die Konten ein, für die Sie freigeben möchten. Wählen Sie dann Save (Speichern) aus.

Sicherheitsüberlegungen für das Teilen verschlüsselter Snapshots

Wenn Sie Zugriff auf einen verschlüsselten Snapshot gewähren, verlangt Redshift, dass der AWS vom Kunden verwaltete KMS-Schlüssel, der zur Erstellung des Snapshots verwendet wurde, mit dem Konto oder den Konten geteilt wird, die die Wiederherstellung durchführen. Wenn der Schlüssel nicht freigegeben ist, führt der Versuch, den Snapshot wiederherzustellen, zu dem Fehler „Zugriff verweigert“. Das empfangende Konto benötigt keine zusätzlichen Berechtigungen, um einen freigegebenen Snapshot wiederherzustellen. Wenn Sie Snapshot-Zugriff autorisieren und

den Schlüssel freigeben, muss die Identität, die den Zugriff autorisiert, über `kms:DescribeKey`-Berechtigungen für den Schlüssel verfügen, der zum Verschlüsseln des Snapshots verwendet wurde. Diese Berechtigung wird unter AWS KMS -Berechtigungen ausführlicher beschrieben. Weitere Informationen finden Sie DescribeKeyin der Referenzdokumentation zur Amazon Redshift Redshift-API.

Die vom Kunden verwaltete Schlüsselrichtlinie kann programmgesteuert oder in der Konsole aktualisiert werden. AWS Key Management Service

Erlaubt den Zugriff auf den AWS KMS-Schlüssel für einen verschlüsselten Snapshot

Um den vom Kunden verwalteten AWS KMS-Schlüssel für einen verschlüsselten Snapshot gemeinsam zu nutzen, aktualisieren Sie die Schlüsselrichtlinie, indem Sie die folgenden Schritte ausführen:

1. Aktualisieren Sie die KMS-Schlüsselrichtlinie mit dem Amazon-Ressourcennamen (ARN) des AWS Kontos, für das Sie Inhalte teilen, wie `Principal` in der KMS-Schlüsselrichtlinie angegeben.
2. Erlauben Sie die `kms:Decrypt`-Aktion.

Im folgenden Beispiel für eine Schlüsselrichtlinie ist Benutzer `111122223333` der Besitzer des KMS-Schlüssels, und Benutzer `444455556666` ist das Konto, für das der Schlüssel freigegeben wird. Diese Schlüsselrichtlinie gewährt dem AWS Konto Zugriff auf den KMS-Beispielschlüssel, indem sie den ARN für die AWS Stammkontoidentität für den Benutzer `444455556666` als `Principal` für die Richtlinie einschließt und die `kms:Decrypt` Aktion zulässt.

```
{
    "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": "*"
        }
    ]
}
```

Nachdem der Zugriff auf den vom Kunden verwalteten KMS-Schlüssel gewährt wurde, muss das Konto, das den verschlüsselten Snapshot wiederherstellt, eine AWS Identity and Access Management (IAM-) Rolle oder einen Benutzer erstellen, falls es noch keinen hat. Darüber hinaus muss dieses AWS Konto dieser IAM-Rolle oder diesem IAM-Benutzer eine IAM-Richtlinie zuordnen, die es dem Benutzer ermöglicht, mithilfe Ihres KMS-Schlüssels einen verschlüsselten Datenbanksnapshot wiederherzustellen.

Weitere Informationen zur Gewährung des Zugriffs auf einen AWS KMS Schlüssel finden Sie im AWS Key Management Service Entwicklerhandbuch unter Erlauben der Verwendung eines KMS-Schlüssels für Benutzer mit anderen Konten.

Einen Überblick über die wichtigsten Richtlinien finden Sie unter So verwendet AWS KMS Amazon Redshift.

Konfigurieren von regionenübergreifenden Snapshot-Kopien für nicht verschlüsselte Cluster

Sie können Amazon Redshift so konfigurieren, dass Snapshots für einen Cluster in eine andere AWS Region kopiert werden. Um die regionsübergreifende Snapshot-Kopie zu konfigurieren, müssen Sie diese Kopierfunktion für jeden Cluster aktivieren und konfigurieren, wo Snapshots kopiert werden sollen und wie lange kopierte automatische oder manuelle Snapshots in der Zielregion aufbewahrt werden sollen. AWS Wenn das regionsübergreifende Kopieren für einen Cluster aktiviert ist, werden alle neuen manuellen und automatisierten Snapshots in die angegebene Region kopiert. AWS Den Namen der kopierten Snapshots wird jeweils das Präfix vorangestellt **`copy:`**.

So konfigurieren Sie einen regionenübergreifenden Snapshot

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster aus, für den Sie Snapshots verschieben möchten.
3. Wählen Sie bei Actions (Aktionen) Configure cross-region snapshot (Regionsübergreifenden Snapshot konfigurieren) aus.

Das Dialogfeld „Configure cross-Region“ (Regionsübergreifenden Snapshot konfigurieren) wird angezeigt.

4. Wählen Sie bei Copy snapshots (Snapshots kopieren) Yes (Ja) aus.
5. Wählen Sie unter AWS Zielregion die AWS Region aus, in die Snapshots kopiert werden sollen.
6. Wählen Sie unter Aufbewahrungszeitraum für automatisierte Snapshots (Tage) die Anzahl der Tage aus, für die automatische Snapshots in der AWS Zielregion aufbewahrt werden sollen, bevor sie gelöscht werden.
7. Wählen Sie unter Aufbewahrungszeitraum für manuelle Snapshots den Wert aus, der die Anzahl der Tage angibt, für die manuelle Snapshots in der AWS Zielregion aufbewahrt werden sollen, bevor sie gelöscht werden. Wenn Sie Custom value (Benutzerdefinierter Wert) auswählen, muss der Aufbewahrungszeitraum zwischen 1 und 3 653 Tagen liegen.
8. Wählen Sie Save (Speichern) aus.

Konfigurieren Sie die regionsübergreifende Snapshot-Kopie für einen AWS KMS—verschlüsselten Cluster

Wenn Sie einen Amazon Redshift Redshift-Cluster starten, können Sie ihn mit einem Root-Schlüssel aus AWS Key Management Service ()AWS KMS verschlüsseln. AWS KMS Schlüssel sind spezifisch für eine AWS Region. Wenn Sie die regionsübergreifende Snapshot-Kopie für einen mit AWS KMS —verschlüsselten Clustern aktivieren möchten, müssen Sie eine Zuweisung für Snapshot-Kopien für einen Root-Schlüssel in der AWS Zielregion konfigurieren. Dadurch ermöglichen Sie Amazon Redshift die Durchführung von Verschlüsselungsvorgängen in der AWS -Zielregion.

Im folgenden Verfahren wird beschrieben, wie Sie die regionsübergreifende Snapshot-Kopie für einen AWS KMS-verschlüsselten Cluster aktivieren. Weitere Informationen zur Verschlüsselung in Amazon Redshift und zu Snapshot-Kopie-Berechtigungen finden Sie unter Kopieren von —verschlüsselten Snapshots in eine andere Region AWS KMSAWS.

So konfigurieren Sie einen regionsübergreifenden Snapshot für einen —verschlüsselten Cluster AWS KMS

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster aus, für den Sie Snapshots verschieben möchten.

3. Wählen Sie bei Actions (Aktionen) Configure cross-region snapshot (Regionsübergreifenden Snapshot konfigurieren) aus.

   Das Dialogfeld „Configure cross-Region“ (Regionsübergreifenden Snapshot konfigurieren) wird angezeigt.
4. Wählen Sie bei Copy snapshots (Snapshots kopieren) Yes (Ja) aus.
5. Wählen Sie unter AWS Zielregion die AWS Region aus, in die Snapshots kopiert werden sollen.
6. Wählen Sie unter Aufbewahrungszeitraum für automatisierte Snapshots (Tage) die Anzahl der Tage aus, für die automatische Snapshots in der AWS Zielregion aufbewahrt werden sollen, bevor sie gelöscht werden.
7. Wählen Sie unter Aufbewahrungszeitraum für manuelle Snapshots den Wert aus, der die Anzahl der Tage angibt, für die manuelle Snapshots in der AWS Zielregion aufbewahrt werden sollen, bevor sie gelöscht werden. Wenn Sie Custom value (Benutzerdefinierter Wert) auswählen, muss der Aufbewahrungszeitraum zwischen 1 und 3 653 Tagen liegen.
8. Wählen Sie Save (Speichern) aus.

Ändern des Aufbewahrungszeitraums für regionenübergreifende Snapshot-Kopien

Möglicherweise möchten Sie bestimmte Einstellungen ändern, nachdem Sie regionenübergreifende Snapshot-Kopien konfiguriert haben. Sie können die Aufbewahrungsfrist ganz einfach ändern, indem Sie eine andere Anzahl an Tagen auswählen und dann die Änderungen speichern.

> **Warning**
>
> Sie können die AWS Zielregion nicht mehr ändern, nachdem die regionsübergreifende Snapshot-Kopie konfiguriert wurde.
> Wenn Sie Snapshots in eine andere AWS Region kopieren möchten, deaktivieren Sie zunächst das regionsübergreifende Kopieren von Snapshots. Aktivieren Sie es dann erneut mit einer neuen AWS Zielregion und einer neuen Aufbewahrungsfrist. Alle kopierten automatisierten Snapshots werden gelöscht, nachdem Sie die regionenübergreifende Snapshot-Kopie deaktiviert haben. Daher sollten Sie überlegen, ob es welche gibt, die Sie behalten möchten, und sie in manuelle Snapshots kopieren, bevor Sie die regionenübergreifende Snapshot-Kopie deaktivieren.

So ändern Sie einen regionenübergreifenden Snapshot

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster aus, für den Sie Snapshots ändern möchten.
3. Wählen Sie unter Actions (Aktionen) die Option Configure cross-region snapshot (Regionsübergreifenden Snapshot konfigurieren), um die Eigenschaften des Snapshots anzuzeigen.
4. Geben Sie die überarbeiteten Eigenschaften der Snapshot-Definition ein und wählen Sie dann Save (Speichern) aus.

Verwaltung von Snapshots mithilfe der AWS CLI und der Amazon Redshift Redshift-API

Sie können zur Verwaltung von Snapshots die folgenden Amazon-Redshift-CLI-Vorgänge verwenden.

- 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-Zeitraum
- restore-from-cluster-snapshot
- revoke-snapshot-access

Sie können zur Verwaltung von Snapshots die folgenden Amazon-Redshift-API-Aktionen verwenden.

- AuthorizeSnapshotAccess
- CopyClusterSnapshot
- CreateClusterSnapshot

- DeleteClusterSnapshot
- DescribeClusterSnapshots
- DisableSnapshotCopy
- EnableSnapshotCopy
- ModifySnapshotCopyRetentionPeriod
- RestoreFromClusterSnapshot
- RevokeSnapshotAccess

Weitere Informationen über Amazon-Redshift-Snapshots finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.

Arbeiten mit AWS Backup

AWS Backup ist ein vollständig verwalteter Service, der das Zentralisieren und Automatisieren des Datenschutzes in AWS-Services, in der Cloud sowie On-Premises erleichtert.

Mithilfe von AWS Backup für Amazon Redshift können Sie Datenschutzrichtlinien konfigurieren und die Aktivitäten für verschiedene Amazon-Redshift-Ressourcen zentral überwachen. Sie können auch Snapshots in von Amazon Redshift bereitgestellten Clustern erstellen und speichern. Auf diese Weise können Sie Sicherungsaufgaben, die Sie zuvor separat erledigen mussten, automatisieren und konsolidieren, ohne dass manuelle Prozesse erforderlich sind.

Eine Sicherung oder ein Wiederherstellungspunkt stellt den Inhalt einer Ressource, etwa eines Amazon-Redshift-Clusters, zu einem bestimmten Zeitpunkt dar. Sicherung bezieht sich im Allgemeinen auf die verschiedenen Sicherungen in AWS-Services, wie z. B. Amazon-Redshift-Snapshots. AWS Backup speichert Sicherungen in Sicherungstresoren, die Sie Ihren Geschäftsanforderungen entsprechend organisieren können. Die Begriffe Wiederherstellungspunkt und Sicherung werden gleichbedeutend verwendet. Weitere Informationen über AWS Backup finden Sie unter Arbeiten mit Sicherungen.

Amazon Redshift ist nativ in AWS Backup integriert. Somit können Sie Ihre Sicherungspläne definieren und diesen Plänen Amazon-Redshift-Ressourcen zuweisen. AWS Backup automatisiert die Erstellung von manuellen Amazon-Redshift-Snapshots und speichert diese sicher in einem verschlüsselten Sicherungstresor, den Sie in Ihrem Sicherungsplan festlegen. Informationen zu den Tresoren finden Sie unter Arbeiten mit Sicherungstresoren. In dem Sicherungsplan können Sie die Häufigkeit der Sicherungen, das Zeitfenster für die Sicherungen, den Sicherungslebenszyklus

oder den Sicherungstresor definieren. Weitere Informationen zu Sicherungsplänen finden Sie unter Verwalten von Sicherungen mithilfe von Sicherungsplänen.

Themen

- Überlegungen zur Verwendung von AWS Backup mit Amazon Redshift
- Verwalten von AWS Backup mit Amazon Redshift

Überlegungen zur Verwendung von AWS Backup mit Amazon Redshift

In den folgenden Abschnitten werden Überlegungen und Einschränkungen im Zusammenhang mit der Verwendung von AWS Backup mit Amazon Redshift erörtert.

Überlegungen zur Verwendung von AWS Backup mit Amazon Redshift

Im Folgenden sind einige Überlegungen zur Verwendung von AWS Backup mit Amazon Redshift aufgeführt:

- AWS Backup für Amazon Redshift ist verfügbar, wenn sowohl AWS Backup als auch Amazon Redshift in denselben AWS-Regionen verfügbar sind. Informationen darüber, wo AWS Backup verfügbar ist, finden Sie unter Verfügbarkeit der Funktionen nach AWS-Regionen.
- Vergewissern Sie sich, dass Sie alle Voraussetzungen erfüllt haben, um mit der Verwendung von AWS Backup zu beginnen. Weitere Informationen finden Sie unter Voraussetzungen.
- Melden Sie sich unter Erteilen Ihrer Einwilligung für den AWS Backup-Service an. Die Anmeldeoptionen gelten für das jeweilige Konto und die jeweilige AWS-Region. Möglicherweise müssen Sie sich bei mehreren Regionen mit demselben Konto anmelden. Weitere Informationen finden Sie unter Erste Schritte 1: Serviceanmeldung.
- In der Amazon-Redshift-Konsole können Sie manuelle und automatisierte Snapshots erstellen. AWS Backup unterstützt zurzeit nur manuelle Snapshots.
- Sobald Sie AWS Backup zur Verwaltung der Snapshot-Einstellungen verwenden, haben Sie nicht mehr die Möglichkeit, manuelle Snapshot-Einstellungen mit Amazon Redshift zu verwalten. Sie können die Einstellungen jedoch weiterhin mithilfe eines AWS Backup-Plans verwalten. Weitere Informationen finden Sie unter Verwalten von Sicherungen mithilfe von Sicherungsplänen.
- Um Speicherkosten zu sparen, wenn Sie versionierungsfähige Amazon-S3-Buckets sichern möchten, empfehlen wir Ihnen, eine Lebenszyklusablaufregel festzulegen. Informationen zur Angabe einer Lebenszyklusregel finden Sie unter Beispiel 6: Spezifikation einer Lebenszyklus-Konfigurationsregel für einen Bucket mit Versioning Wenn Sie keinen Lebenszyklusablaufzeitraum

festlegen, könnten Ihre Amazon-Redshift-Speicherkosten steigen, da AWS Backup alle Versionen Ihrer Amazon-Redshift-Daten beibehält.

Einschränkungen

Bei Verwendung von AWS Backup in Amazon Redshift gelten folgende Einschränkungen:

- Sie können AWS Backup nicht zur Verwaltung von automatisierten Amazon-Redshift-Snapshots verwenden. Verwenden Sie Tags, um automatisierte Snapshots zu verwalten. Weitere Informationen über das Markieren von Ressourcen finden Sie unter Markieren von Ressourcen in Amazon Redshift.
- AWS Backup unterstützt Amazon Redshift Serverless nicht.

Verwalten von AWS Backup mit Amazon Redshift

Sie können Ressourcen in Ihren von Amazon Redshift bereitgestellten Clustern über die AWS Backup-Konsole oder programmgesteuert über die AWS Backup-API oderAWS Command Line Interface (AWS CLI) schützen. Wenn Sie eine Ressource wiederherstellen müssen, können Sie entweder die AWS Backup-Konsole oder AWS CLI verwenden, um die benötigte Ressource zu suchen und wiederherzustellen. Weitere Informationen finden Sie unter AWS Command Line Interface.

Sie können die folgenden Aktionen mit AWS Backup für Amazon Redshift ausführen:

- Erstellen von regelmäßigen Sicherungen, die automatisch Amazon-Redshift-Snapshots initiieren. Regelmäßige Sicherungen sind nützlich, um Ihre Anforderungen an die langfristige Datenaufbewahrung zu erfüllen. Weitere Informationen finden Sie unter Amazon-Redshift-Sicherungen.
- Automatisieren der Planung und Aufbewahrung von Sicherungen durch die zentrale Konfiguration von Sicherungsplänen.
- Wiederherstellen eines Clusters in der von Ihnen ausgewählten gespeicherten Sicherung. Sie legen fest, wie oft Ihre Ressourcen gesichert werden sollen. Weitere Informationen finden Sie unter Wiederherstellen eines Amazon-Redshift-Clusters.

Konfigurieren einer Multi-AZ-Bereitstellung

Amazon Redshift unterstützt Bereitstellungen in mehreren Availability Zones (Multi-AZ-Bereitstellungen) für bereitgestellte RA3-Cluster. Durch die Verwendung von Multi-AZ-Bereitstellungen kann Ihr Amazon Redshift Data Warehouse auch in Fehlersituationen in Betrieb bleiben, wenn es in einer Availability Zone zu einem unerwarteten Ereignis kommt. Bei einer Multi-AZ-Bereitstellung werden Rechenressourcen in zwei Availability Zones (AZ) bereitgestellt. Auf diese Rechenressourcen kann über einen einzelnen Endpunkt zugegriffen werden. Bei einem Ausfall einer gesamten Availability Zone stehen die verbleibenden Rechenressourcen in der zweiten Availability Zone zur weiteren Verarbeitung von Workloads zur Verfügung. Bei Ausführung eines Multi-AZ-Data-Warehouse berechnet Amazon Redshift für RA3 dieselben Stundensätze. Die Speicherkosten bleiben gleich, da sie über alle Availability Zones innerhalb einer AWS-Region verteilt sind.

Derzeit unterstützt Amazon Redshift Zero Recovery Point Objective (RPO), sodass Daten auch up-to-date bei einem Ausfall aktuell sind. Mit der Multi-AZ-Bereitstellung verbessert Amazon Redshift seine bestehenden Wiederherstellungsfunktionen weiter und verringert sein Recovery Time Objective (RTO). Dies ist möglich, da eine Multi-AZ-Bereitstellung nach einem Ausfall oder einer Katastrophe schneller wiederhergestellt werden kann, sodass ein Service Level Agreement (SLA) von 99,99 % für Amazon Redshift erreicht wird, verglichen mit 99,9 % bei einem Single-AZ-Data-Warehouse.

Einrichten einer Multi-AZ-Bereitstellung

Wählen Sie zum Einrichten einer Multi-AZ-Bereitstellung die Option Multi-AZ aus und geben Sie die Anzahl der Rechenknoten an, die in jeder Availability Zone bereitgestellt werden sollen. Amazon Redshift stellt automatisch gleiche Rechenressourcen in zwei Availability Zones bereit. Alle Rechenressourcen sind dabei während des normalen Betriebs stets sowohl für die Lese- als auch für die Schreibverarbeitung verfügbar. Auf diese Weise kann eine Multi-AZ-Bereitstellung als einzelnes Data Warehouse mit einem einzigen Endpunkt fungieren, sodass im Notfall keine Anwendungsänderungen erforderlich sind. Eine Multi-AZ-Bereitstellung verarbeitet zwar eine einzelne Abfrage unter Verwendung der Rechenressourcen von nur einer Availability Zone, kann aber die Verarbeitung mehrerer gleichzeitiger Abfragen automatisch auf beide Availability Zones verteilen, um den Gesamtdurchsatz bei Workloads mit hoher Nebenläufigkeit zu erhöhen.

Sie können auch ein vorhandenes Single-AZ-Data-Warehouse in ein Multi-AZ-Data-Warehouse umwandeln oder umgekehrt. Alles bleibt gleich, es werden lediglich zusätzliche Rechenressourcen in der zweiten Availability Zone bereitgestellt. Wenn Sie von einem vorhandenen Single-AZ-Cluster zu Multi-AZ migrieren, müssen Sie möglicherweise die benötigte Anzahl der Cluster-Knoten verdoppeln, damit die Leistung einer einzelnen Abfrage erhalten bleiben kann. Bei den meisten

Workloads ist bei einem Multi-AZ-Data-Warehouse eine Erhöhung des Gesamtdurchsatzes bei der Abfrageverarbeitung zu beobachten, da doppelt so viele Rechenressourcen zur Verfügung stehen.

Im Falle eines Ausfalls in einer Availability Zone setzt Amazon Redshift den Betrieb fort und verwendet automatisch die Ressourcen in der verbleibenden Availability Zone. Benutzerverbindungen könnten jedoch getrennt werden und müssen erneut hergestellt werden. Darüber hinaus können Abfragen, die gerade in der ausgefallenen Availability Zone ausgeführt wurden, fehlschlagen und müssen wiederholt werden. Sie können jedoch erneut eine Verbindung zu Ihrem Cluster herstellen und Abfragen sofort neu planen und Amazon Redshift verarbeitet die Abfragen in der verbleibenden Availability Zone. Bei Abfragen, die bei einem Ausfall oder danach ausgegeben wurden, kann es während der Wiederherstellung des Multi-AZ-Data-Warehouse zu Laufzeitverzögerungen kommen.

> **Note**
>
> Um eine bessere Leistung und höhere Verfügbarkeit zu erzielen, empfehlen wir Ihnen, SNAPSHOT ISOLATION mit Ihren Multi-AZ-Clustern zu verwenden. Weitere Informationen finden Sie unter CREATE DATABASE.

Einschränkungen

Ein Multi-AZ-Data-Warehouse bietet dieselben funktionalen Möglichkeiten wie ein Single-AZ-Data-Warehouse, mit Ausnahme der folgenden Einschränkungen, die für ein Multi-AZ-Data-Warehouse gelten:

- Sie können kein unverschlüsseltes Multi-AZ-Data-Warehouse erstellen. Achten Sie darauf, eine Verschlüsselung hinzuzufügen, wenn Sie ein neues Multi-AZ-Data-Warehouse erstellen oder ein Single-AZ-Data-Warehouse in ein Multi-AZ-Data-Warehouse umwandeln.
- Sie können für keinen der RA3-Instance-Typen eine Einzelknoten-Multi-AZ-Bereitstellung erstellen. Wählen Sie beim Erstellen einer Multi-AZ-Bereitstellung 2 oder mehr Knoten pro Availability Zone aus.
- Null-ETL-Integrationen werden in Ziel-Data-Warehouses, die für eine Multi-AZ-Bereitstellung konfiguriert sind, nicht unterstützt.
- Amazon Redshift erfordert keine Subnetzkonfiguration, die weniger als drei Availability Zones unterstützen kann. Mit anderen Worten, die konfigurierte Subnetzgruppe benötigt drei weitere Subnetze.

- Sie können eine Multi-AZ-Bereitstellung nicht in eine andere Availability Zone verschieben. Bei Verwendung einer Multi-AZ-Bereitstellung wird die Verschiebung automatisch von Amazon Redshift bestimmt und durchgeführt.
- Sie können eine Multi-AZ-Bereitstellung nicht anhalten oder fortsetzen.
- Sie können Ihre Multi-AZ-Bereitstellung nicht außerhalb der unterstützten Portbereiche 5431 bis 5455 und 8191 bis 8215 ausführen.
- Sie können STL-, SVCS-, SVL-, SVV- und STV-Ansichten nicht mit Multi-AZ-Bereitstellungen verwenden, da diese nur Systemüberwachungsansichten (SYS_*-Ansichten) unterstützen. Ändern Sie Ihre Überwachungsanfragen so, dass sie Systemüberwachungsansichten (SYS_*-Ansichten) verwenden.
- Sie können einem vorhandenen Cluster mit aktiviertem Multi-AZ keine Elastic IP-Adresse zuordnen.
- Sie können einen Cluster mit einer angehängten Elastic IP-Adresse nicht von Single-AZ in Multi-AZ konvertieren.
- Die Amazon Redshift Multi-AZ-Bereitstellung ist wie folgt verfügbar: AWS-Regionen
  - USA Ost (Ohio): (us-east-2)
  - USA Ost (Nord-Virginia): (us-east-1)
  - USA West (Oregon): (us-west-2)
  - Afrika (Kapstadt) (af-south-1)
  - Asien-Pazifik (Hongkong) (ap-east-1)
  - Asien-Pazifik (Hyderabad) (ap-south-2)
  - Asien-Pazifik (Jakarta) (ap-southeast-3)
  - Asien-Pazifik (Melbourne) (ap-southeast-4)
  - Asien-Pazifik (Mumbai): (ap-south-1)
  - Asien-Pazifik (Osaka) (ap-northeast-3)
  - Asien-Pazifik (Seoul): (ap-northeast-2)
  - Asien-Pazifik (Singapur): (ap-southeast-1)
  - Asien-Pazifik (Sydney): (ap-southeast-2)
  - Asien-Pazifik (Tokyo) (ap-northeast-1)
  - Kanada (Zentral): (ca-central-1)
  - Europa (Frankfurt) (eu-central-1)
  - Europa (Irland) (eu-west-1)

- Europa (Mailand) (eu-south-1)
- Europa (Paris) (eu-west-3)
- Europa (Spanien) (eu-south-2)
- Europa (Stockholm) (eu-north-1)
- Europa (Zürich) (eu-central-2)
- Israel (Tel Aviv) (il-central-1)
- Naher Osten (Bahrain) (me-south-1)
- Naher Osten (VAE) (me-central-1)

Themen

- Verwalten der Multi-AZ-Bereitstellung
- Failover bei einer Multi-AZ-Bereitstellung
- Abfrageüberwachung für Multi-AZ

Verwalten der Multi-AZ-Bereitstellung

Amazon Redshift Multi-AZ unterstützt zwei Availability Zones gleichzeitig. Amazon Redshift wählt die Availability Zones automatisch auf der Grundlage der ausgewählten Subnetzgruppen-Konfiguration aus. Sie können ein vorhandenes Data Warehouse in einer einzelnen Availability Zone in ein Multi-AZ-Data-Warehouse umwandeln oder es aus einem Snapshot wiederherstellen, um es zu einem Multi-AZ-Data-Warehouse zu konfigurieren.

Über die Amazon-Redshift-Konsole können Sie ganz einfach neue Multi-AZ-Bereitstellungen erstellen. Um eine neue Multi-AZ-Bereitstellung unter Verwendung der Amazon-Redshift-Konsole zu erstellen, wählen Sie bei Erstellung des Data Warehouse die Option „Multi-AZ“ aus. Geben Sie die Anzahl der in einer einzelnen Availability Zone erforderlichen Rechenknoten an. Amazon Redshift stellt dann die betreffende Knotenanzahl in jeder der beiden Availability Zones bereit. Alle Knoten werden während des normalen Betriebs für die Verarbeitung von Lese- und Schreib-Workloads verwendet werden. Sie können den AWS CLI `create-cluster` Befehl auch verwenden, um mithilfe des Parameters ein neues Multi-AZ-Data Warehouse zu erstellen. `multi-az`

Sie können ein vorhandenes Single-AZ-Data Warehouse in ein Multi-AZ-Data Warehouse konvertieren. Sie können entweder die Amazon Redshift Redshift-Konsole oder den AWS CLI `modify-cluster` Befehl mit dem Parameter verwenden. `multi-az` Oder Sie können aus einem Snapshot wiederherstellen, um ein Single-AZ-Data Warehouse in ein Multi-AZ-Data Warehouse

zu konfigurieren, indem Sie entweder die Amazon Redshift Redshift-Konsole oder den AWS CLI `restore-from-cluster-snapshot` Befehl verwenden, der den Parameter verwendet. `multi-az`

Die Multi-AZ-Bereitstellung unterstützt nur RA3-Knotentypen, die Amazon Redshift Managed Storage (RMS) verwenden. Amazon Redshift speichert Daten in RMS, das Amazon S3 verwendet und in allen Availability Zones in einem zugänglich ist AWS-Region, ohne dass die Daten auf Amazon Redshift Redshift-Ebene repliziert werden müssen.

Einrichten von Multi-AZ beim Erstellen eines neuen Clusters

Sie können eine Multi-AZ-Bereitstellung beim Erstellen eines neuen Clusters über die Amazon-Redshift-Konsole oder die AWS Command Line Interface einrichten.

Verwenden der Konsole

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Provisioned clusters dashboard (Dashboard für bereitgestellte Cluster) und dann Clusters (Cluster) aus. Die aktuellen Cluster für Ihr Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie die Schaltfläche Cluster erstellen aus, um die Seite zum Erstellen von Clustern zu öffnen.
4. Geben Sie Eigenschaften für Ihren Cluster ein. Allgemeine Informationen zum Erstellen von Clustern finden Sie unter Erstellen eines Clusters.
5. Wählen Sie einen der RA3-Knotentypen aus der Dropdown-Liste Node type (Knotentyp) aus. Die Multi-AZ-Konfigurationsoption ist nur verfügbar, wenn Sie einen RA3-Knotentyp ausgewählt haben.
6. Wählen Sie unter AZ-Konfiguration die Option Multi-AZ aus.
7. Geben Sie unter Anzahl der Knoten pro AZ mindestens zwei Knoten für Ihren Cluster ein.
8. Sie haben die Möglichkeit, Beispieldaten zu laden oder Ihre eigenen Daten bereitzustellen:

   - Wählen Sie unter Sample data (Beispieldaten) Load sample data (Beispieldaten laden) aus, um den Beispieldatensatz in Ihren Amazon-Redshift-Cluster zu laden. Amazon Redshift lädt den Beispieldatensatz Tickit in die standardmäßige dev-Datenbank und das öffentliche Schema. Amazon Redshift lädt den Beispieldatensatz automatisch in Ihren Amazon-Redshift-Cluster. Sie können jetzt anfangen, mit dem Abfrage-Editor v2 Daten abzufragen.

- Um Ihre eigenen Daten in Ihren Amazon-Redshift-Cluster einzubinden, folgen Sie den Schritten unter Eigene Daten in Amazon Redshift einbinden.

9. Scrollen Sie zu Additional configurations (Zusätzliche Konfigurationen), erweitern Sie Network and security (Netzwerk und Sicherheit) und akzeptieren Sie entweder die standardmäßige Cluster subnet group (Cluster-Subnetzgruppe) oder wählen Sie eine andere aus. Wenn Sie eine andere Cluster-Subnetzgruppe auswählen, stellen Sie sicher, dass in der ausgewählten Subnetzgruppe 3 Availability Zones vorhanden sind.
10. Erweitern Sie unter Additional configurations (Zusätzliche Konfigurationen) den Bereich Database configurations (Datenbankkonfigurationen).
11. Um einen benutzerdefinierten AWS KMS Schlüssel anstelle des AWS Key Management Service Standardschlüssels zu verwenden, klicken Sie unter Datenbankverschlüsselung auf Verschlüsselungseinstellungen anpassen.
12. Unter KMS-Schlüssel auswählen können Sie entweder einen AWS Key Management Service Schlüssel auswählen oder einen ARN eingeben. Oder Sie können in der AWS Key Management Service Konsole auf AWS Key Management Service Schlüssel erstellen klicken. Weitere Informationen zum Erstellen von KMS-Schlüsseln finden Sie unter Erstellen von Schlüsseln im AWS Key Management Service -Entwicklerhandbuch.
13. Klicken Sie auf Create cluster. Bei erfolgreicher Clustererstellung können Sie die Details auf der Seite mit den Clusterdetails einsehen. Sie können Ihren SQL-Client zum Laden und Abfragen von Daten verwenden.

Mit dem AWS Command Line Interface

Zur Einrichtung von Multi-AZ bei der Erstellung eines Clusters mit dem AWS Command Line Interface

- AWS CLI Verwenden Sie ab dann den `create-cluster` Befehl und den `multi-az` Parameter wie folgt.

```
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
```

Umwandeln eines Single-AZ-Data-Warehouse in ein Multi-AZ-Data-Warehouse

Durch die Umwandlung eines Single-AZ-Data-Warehouse in ein Multi-AZ-Data-Warehouse wird Ihr Data Warehouse mit einer SLA-Garantie von 99,99 % hochverfügbar. Die Leistung einer einzelnen Abfrage bleibt auch bei einem Multi-AZ-Data-Warehouse gleich. Bei Workloads mit höherer Nebenläufigkeit werden Sie eine Erhöhung des Gesamtdurchsatzes feststellen, da Amazon Redshift Anforderungen unter Verwendung von Rechenressourcen in zwei Availability Zones ausführen kann.

> **Note**
>
> Während der Umwandlung von Single-AZ zu Multi-AZ oder umgekehrt ist es in Amazon Redshift nicht möglich, vorhandene Rechenressourcen aufzuteilen. rDieser Vorgang wird nicht unterstützt, um eine konsistente Leistung einzelner Abfragen aufrechtzuerhalten.

Verwenden der Konsole

So wandeln Sie einen Single-AZ-Cluster über die Konsole in ein Multi-AZ-Data-Warehouse um

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Provisioned clusters dashboard (Dashboard für bereitgestellte Cluster) und dann Clusters (Cluster) aus. Die aktuellen Cluster für Ihr Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie den Cluster aus, den Sie in eine Multi-AZ-Bereitstellung umwandeln möchten. Die Cluster-Detailseite wird angezeigt.
4. Wählen Sie unter Aktionen die Option Multi-AZ aktivieren aus. Die Zusammenfassung der Änderungen wird angezeigt. Klicken Sie auf Multi-AZ aktivieren.
5. Führen Sie im Falle eines Fehlers einen der folgenden Schritte aus und klicken Sie dann auf Multi-AZ aktivieren.

- Clusterverschlüsselung – Wählen Sie Eigenschaften aus, um die Verschlüsselungseinstellungen im Abschnitt „Datenbankkonfiguration“ auf der Registerkarte „Eigenschaften“ der Seite „Cluster-Details“ zu bearbeiten.
- Subnetzgruppe – Wählen Sie Subnetzgruppe aus, um die Einstellungen der Cluster-Subnetzgruppe zu bearbeiten, indem Sie auf den Link zur Subnetzgruppe klicken. Wenn Sie eine andere Cluster-Subnetzgruppe auswählen, stellen Sie sicher, dass in der ausgewählten Subnetzgruppe 3 Availability Zones vorhanden sind.
- Porteinstellungen – Wählen Sie Eigenschaften aus, um die Porteinstellung im Abschnitt „Datenbankkonfiguration“ auf der Registerkarte „Eigenschaften“ der Seite „Cluster-Details“ zu bearbeiten.

6. Sie können Ihren SQL-Client zum Laden und Abfragen von Daten verwenden.

Mit dem AWS Command Line Interface

- Verwenden Sie von der AWS CLI aus den `modify-cluster` Befehl und den `multi-az` Parameter wie folgt.

```
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
```

Umwandeln eines Multi-AZ-Data-Warehouse in ein Single-AZ-Data-Warehouse

Wenn Sie ein Multi-AZ-Data-Warehouse in ein Single-AZ-Data-Warehouse umwandeln, erreicht Ihr Data Warehouse nicht die SLA-Garantie von 99,99 %, die Multi-AZ bietet. Die Leistung einer einzelnen Abfrage bleibt gleich, doch der Gesamtdurchsatz wird beeinträchtigt, da die Rechenressourcen in der zweiten Availability Zone nicht verfügbar sind. Sie haben die Möglichkeit, Nebenläufigkeitsskalierung zu aktivieren, um den Durchsatz automatisch zu skalieren und so eine gleichbleibende Leistung auch bei Single-AZ zu erzielen.

> **Note**
>
> Während der Umwandlung von Single-AZ zu Multi-AZ oder umgekehrt ist es in Amazon Redshift nicht möglich, vorhandene Rechenressourcen aufzuteilen. rDieser Vorgang wird nicht unterstützt, um eine konsistente Leistung einzelner Abfragen aufrechtzuerhalten.

Verwenden der Konsole

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Provisioned clusters dashboard (Dashboard für bereitgestellte Cluster) und dann Clusters (Cluster) aus. Die aktuellen Cluster für Ihr Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie den Cluster aus, den Sie in eine Multi-AZ-Bereitstellung umwandeln möchten. Die Cluster-Detailseite wird angezeigt.
4. Wählen Sie unter Aktionen die Option Multi-AZ deaktivieren aus. Die Zusammenfassung der Änderungen wird angezeigt. Klicken Sie auf Multi-AZ deaktivieren.

Mit dem AWS Command Line Interface

- Verwenden Sie von der AWS CLI aus den `modify-cluster` Befehl und den `no-multi-az` Parameter wie folgt.

```
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
```

Sobald Ihr Data Warehouse in ein Single-AZ-Data-Warehouse umgewandelt wurde, gilt die SLA-Garantie von 99,99 % nicht mehr. Der Gesamtdurchsatz wird ebenfalls beeinträchtigt. Wenn die Änderungen gespeichert wurden, können Sie die Details auf der Seite „Cluster-Details“ einsehen.

Anpassen der Größe eines Multi-AZ-Data-Warehouse

Sie können die Größe eines Multi-AZ-Data-Warehouse anpassen und eine Anzahl von Knoten oder einen Knotentyp angeben, die/der sich von der aktuellen Konfiguration des Data Warehouse unterscheidet.

Verwenden der Konsole

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Provisioned clusters dashboard (Dashboard für bereitgestellte Cluster) und dann Clusters (Cluster) aus. Die aktuellen Cluster für Ihr Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie den Cluster aus, für den Sie die Größe des Multi-AZ-Data-Warehouse anpassen möchten. Die Cluster-Detailseite wird angezeigt.
4. Wählen Sie für Actions (Aktionen) Resize (Größe ändern) aus. Die Seite Resize cluster (Cluster-Größe ändern) wird angezeigt.
5. Folgen Sie den Anweisungen auf der Seite. Sie können die Größe des Clusters jetzt, einmal zu einer bestimmten Zeit, ändern oder die Größe Ihres Clusters nach einem Zeitplan vergrößern und verkleinern.
6. Wählen Sie unter Neue Konfiguration einen der RA3-Knotentypen aus der Dropdown-Liste „Knotentyp“ aus.
7. Klicken Sie auf Größe des Clusters anpassen.

Mit dem AWS Command Line Interface

Um die Größe eines Multi-AZ-Data Warehouse zu ändern, verwenden Sie AWS Command Line Interface

- Verwenden Sie von der aus den `resize-cluster` Befehl AWS CLI, um die Anzahl der Knoten für eine einzelne Availability Zone wie folgt zu ändern.

```
aws redshift resize-cluster \
    --cluster-identifier test-maz-11
    --cluster-type multi-node
    --node-type ra3.4xlarge
```

```
    --number-of-nodes 6
```

Einrichtung von Multi-AZ für ein Data Warehouse, das von einem Snapshot wiederhergestellt wurde

Sie können einen neuen Multi-AZ-Cluster auch erstellen, indem Sie ihn von einem Snapshot wiederherstellen.

Verwenden der Konsole

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster), Snapshots und dann den zu verwendenden Snapshot aus.
3. Wählen Sie Restore snapshot (Snapshot wiederherstellen), Restore to a provisioned cluster (In einem bereitgestellten Cluster wiederherstellen) aus.
4. Geben Sie Eigenschaften für Ihren Cluster ein. Allgemeine Informationen zum Erstellen von Clustern finden Sie unter Erstellen eines Clusters.
5. Wählen Sie einen der RA3-Knotentypen aus der Dropdown-Liste Node type (Knotentyp) aus. Die Multi-AZ-Konfigurationsoption ist nur verfügbar, wenn Sie einen RA3-Knotentyp ausgewählt haben.
6. Wählen Sie unter AZ-Konfiguration die Option Multi-AZ aus.
7. Geben Sie unter Anzahl der Knoten pro AZ mindestens zwei Knoten für Ihren Cluster ein.
8. Sie haben die Möglichkeit, Beispieldaten zu laden oder Ihre eigenen Daten bereitzustellen:

   - Wählen Sie unter Sample data (Beispieldaten) Load sample data (Beispieldaten laden) aus, um den Beispieldatensatz in Ihren Amazon-Redshift-Cluster zu laden. Amazon Redshift lädt den Beispieldatensatz Tickit in die standardmäßige dev-Datenbank und das öffentliche Schema. Amazon Redshift lädt den Beispieldatensatz automatisch in Ihren Amazon-Redshift-Cluster. Sie können jetzt anfangen, mit dem Abfrage-Editor v2 Daten abzufragen.
   - Um Ihre eigenen Daten in Ihren Amazon-Redshift-Cluster einzubinden, folgen Sie den Schritten unter Eigene Daten in Amazon Redshift einbinden.
9. Scrollen Sie zu Additional configurations (Zusätzliche Konfigurationen), erweitern Sie Network and security (Netzwerk und Sicherheit) und akzeptieren Sie entweder die standardmäßige Cluster subnet group (Cluster-Subnetzgruppe) oder wählen Sie eine andere aus. Wenn Sie

eine andere Cluster-Subnetzgruppe auswählen, stellen Sie sicher, dass in der ausgewählten Subnetzgruppe 3 Availability Zones vorhanden sind.

10. Erweitern Sie unter Additional configurations (Zusätzliche Konfigurationen) den Bereich Database configurations (Datenbankkonfigurationen).
11. Um unter Datenbankverschlüsselung einen anderen benutzerdefinierten KMS-Schlüssel als den AWS Key Management Service Standardschlüssel zu verwenden, klicken Sie auf Verschlüsselungseinstellungen anpassen. Diese Option ist standardmäßig ausgewählt.
12. Unter KMS-Schlüssel auswählen können Sie entweder einen AWS Key Management Service Schlüssel auswählen oder einen ARN eingeben. Oder Sie können in der AWS Key Management Service Konsole auf AWS Key Management Service Schlüssel erstellen klicken. Weitere Informationen zum Erstellen von KMS-Schlüsseln finden Sie unter Erstellen von Schlüsseln im AWS Key Management Service -Entwicklerhandbuch.
13. Klicken Sie auf Restore Cluster from snapshot (Cluster von Snapshot wiederherstellen). Bei erfolgreicher Clusterwiederherstellung können Sie die Details auf der Seite mit den Clusterdetails einsehen.

Mit dem AWS Command Line Interface

- Verwenden Sie von der AWS CLI aus den `restore-from-cluster-snapshot` Befehl wie folgt.

```
aws redshift restore-from-cluster-snapshot
--region eu-west-1
--multi-az
--snapshot-identifier test-snap1
--cluster-identifier test-saz-11
--endpoint-url https://redshift.eu-west-1.amazonaws.com/
```

Failover bei einer Multi-AZ-Bereitstellung

Ihr Multi-AZ-Data-Warehouse ist eine Sammlung von Rechenressourcen, die gleichzeitig in zwei Availability Zones bereitgestellt werden. Die in der primären Availability Zone bereitgestellten Rechenressourcen werden als primäre Rechenressourcen und die in den sekundären Availability Zones bereitgestellten Rechenressourcen als sekundäre Rechenressourcen bezeichnet. Ein Multi-AZ-Data-Warehouse kann in dem unwahrscheinlichen Fall, dass eine Availability Zone oder die Infrastruktur ausfällt, ohne Eingreifen des Benutzers automatisch wiederhergestellt werden. Der

Wiederherstellungsprozess umfasst ein Failover von den primären Rechenressourcen zu den sekundären Rechenressourcen und die Zuweisung sekundärer Rechenressourcen als primär. Darüber hinaus werden neue sekundäre Rechenressourcen in einer dritten Availability Zone bereitgestellt. Der automatische Wiederherstellungsprozess wird anhand von RTO und RPO gemessen.

- Recovery Time Objective (RTO) – Die Zeit, die ein System benötigt, um nach einem Notfall in einen arbeitsfähigen Zustand zurückzukehren. Mit anderen Worten: RTO misst die Ausfallzeit.
- Recovery Point Objective (RPO) – Die Datenmenge, die verloren gehen kann (gemessen in Zeit). Für ein Multi-AZ-Data-Warehouse von Amazon Redshift gilt in der Regel ein RPO von null, da alle Daten in Amazon Redshift Managed Storage (RMS) gespeichert werden, unterstützt von Amazon Simple Storage Service, einer standardmäßig äußerst dauerhaften und hochverfügbaren Lösung.

> **Note**
>
> Die Leistung einer einzelnen Abfrage ändert sich nach einem Failover nicht. Der Gesamtdurchsatz Ihres Data Warehouse wird für kurze Zeit geringer sein, da Rechenressourcen in einer der Availability Zones nicht verfügbar sind. Amazon Redshift erwirbt jedoch automatisch Kapazität in einer anderen Availability Zone, um sicherzustellen, dass die bisherige Data-Warehouse-Verarbeitungskapazität wiederhergestellt wird.

Zusätzlich zum automatischen Wiederherstellungsprozess können Sie diesen Prozess über die Option Failover für primäre Rechenleistung auch manuell für Ihr Data Warehouse auslösen. Mit dieser Vorgehensweise können Sie testen, wie Multi-AZ Ihrer Anwendung zu größerer Hochverfügbarkeit und besserer Kontinuität verhelfen würde.

Verwenden der Konsole

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Wählen Sie unter Clusters (Cluster) einen Cluster aus. Die Cluster-Detailseite wird angezeigt.
   - Wählen Sie im Cluster-Dashboard einen Cluster aus.
3. Wählen Sie unter Aktionen die Option Failover für primäre Rechenleistung aus.

4. Klicken Sie bei der entsprechenden Aufforderung auf Confirm (Bestätigen).

Verwenden Sie den AWS Command Line Interface

- Verwenden Sie von der AWS CLI aus den `failover-primary-compute` Befehl wie folgt.

```
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
```

Nach Bestätigung des obigen Vorgangs führt Amazon Redshift dieselben Schritte wie bei einer automatischen Wiederherstellung nach dem Ausfall einer Availability Zone oder Infrastruktur aus. Das Vorgehen führt dazu, dass die Rechenknoten in der primären Availability Zone nicht mehr verfügbar sind und Rechenressourcen in der sekundären Availability Zone als primäre Rechenressourcen ausgewiesen werden. Bei erfolgreichem Abschluss der Cluster-Wiederherstellung wird die Multi-AZ-Bereitstellung verfügbar. Ihr Multi-AZ-Data-Warehouse stellt außerdem automatisch neue sekundäre Rechenressourcen in einer dritten Availability Zone bereit, sobald diese verfügbar sind.

Während dieses Vorgangs wird als Clusterstatus in der Konsole die ganze Zeit „Modifying“ (Wird geändert) angezeigt, da der Cluster automatisch wiederhergestellt und auf die Multi-AZ-Bereitstellung zurückkonfiguriert wird. Der Cluster kann sofort neue Verbindungen akzeptieren. Bestehende Verbindungen und In-Flight-Anfragen werden möglicherweise entfernt. Sie können sie sofort erneut versuchen.

Abfrageüberwachung für Multi-AZ

Sie können Informationen zu Abfragen, die in den letzten 7 Tagen ausgeführt wurden, unabhängig von Typ, Größe und Status (Pause oder Fortsetzung) Ihres Clusters einsehen.

Anzeigen von Abfragen und Ladevorgängen für Multi-AZ-Data-Warehouses

Die auf der Seite „Queries and loads“ (Abfragen und Ladevorgänge) angezeigten Informationen sind mit Informationen aus Amazon-Redshift-Systemtabellen (SYS_*-Ansichten) gefüllt. Diese Informationen bieten Ihnen die Möglichkeit, zusätzliche Informationen zu Ihren Abfragen anzeigen, und ermöglichen eine gleitende Aufbewahrungszeit von 7 Tagen. Es wird eine schnellere Abfragediagnose ermöglicht, da Sie Daten nach Datenbank, Benutzername oder SQL-Anweisungstyp

filtern können. Um diese zusätzlichen Filter und Informationen zu allen ausgeführten Abfragen anzeigen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Sie müssen eine Verbindung zu einer Datenbank herstellen und dazu Connect to database (Verbindung zur Datenbank herstellen) auswählen.
- Ihr Datenbankbenutzer muss über die Rollen sys:operator oder sys:monitor und Berechtigungen zur Durchführung einer Abfrageüberwachung verfügen. Informationen zu Systemrollen finden Sie unter Systemdefinierte Amazon-Redshift-Rollen im Datenbankentwicklerhandbuch zu Amazon Redshift.

Sie werden diese zusätzlichen Filter und Abfrageinformationen sehen, sobald Sie eine Verbindung zu einer Datenbank herstellen.

So zeigen Sie Abfrageleistungsdaten von „Queries and loads“ (Abfragen und Ladevorgänge) aus an

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Queries and loads (Abfragen und Ladevorgänge) aus, um die Liste der Abfragen für Ihr Konto anzuzeigen.
3. Möglicherweise müssen Sie eine Verbindung zu einer Datenbank herstellen, um zusätzliche Filter zu sehen. Falls erforderlich, klicken Sie auf Connect to database (Verbindung zur Datenbank herstellen) und folgen Sie den Anweisungen, um eine Verbindung zu einer Datenbank herzustellen.

   Standardmäßig zeigt die Liste Abfragen für alle Ihre Cluster der letzten 24 Stunden an. Sie können den Bereich des angezeigten Datums in der Konsole ändern.

So zeigen Sie Abfrageleistungsdaten von „Query monitoring“ (Abfrageüberwachung) aus an

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Wählen Sie unter Clusters (Cluster) einen Cluster aus.
3. Wählen Sie Query Monitoring (Abfrageüberwachung) aus.
4. Je nach Konfiguration oder Version Ihres Clusters müssen Sie möglicherweise eine Verbindung zu einer Datenbank herstellen, um zusätzliche Filter zu sehen. Falls erforderlich, klicken Sie auf

Connect to database (Verbindung zur Datenbank herstellen) und folgen Sie den Anweisungen, um eine Verbindung zu einer Datenbank herzustellen.

Überwachen einer Abfrage in einer Multi-AZ-Bereitstellung

Eine Multi-AZ-Bereitstellung verwendet Rechenressourcen, die in beiden Availability Zones bereitgestellt werden, und kann den Betrieb fortsetzen, falls die Ressourcen in einer bestimmten Availability Zone nicht verfügbar sind. Alle Rechenressourcen werden zu jeder Zeit genutzt. Dies ermöglicht den vollständigen Betrieb in zwei Availability Zones auf aktiv-aktive Weise sowohl für Lese- als auch für Schreibvorgänge.

Sie können SYS_-Ansichten im Schema pg_catalog abfragen, um die Abfragelaufzeit in einer Multi-AZ-Bereitstellung zu überwachen. Die SYS_-Ansichten zeigen Abfragelaufzeitaktivitäten oder Statistiken von primären und sekundären Clustern an. Eine Liste der Überwachungsansichten finden Sie unter Überwachungsansichten.

Gehen Sie wie folgt vor, um die Abfragelaufzeit für jede Availability Zone innerhalb der Multi-AZ-Bereitstellung zu überwachen:

1. Navigieren Sie zur Amazon-Redshift-Konsole, stellen Sie eine Verbindung zu der Datenbank in Ihrer Multi-AZ-Bereitstellung her und führen Sie Abfragen über den Abfrage-Editor aus.
2. Führen Sie eine beliebige Beispielabfrage für die Multi-AZ-Amazon-Redshift-Bereitstellung aus.
3. Für eine Multi-AZ-Bereitstellung können Sie eine Abfrage und die Availability Zone, in der diese ausgeführt wird, mithilfe der Spalte compute_type in der Tabelle SYS_QUERY_HISTORY ermitteln. primary (primär) steht für Abfragen, die in der Multi-AZ-Bereitstellung auf dem primären Cluster ausgeführt werden, und secondary (sekundär) steht für Abfragen, die in der Multi-AZ-Bereitstellung auf dem sekundären Cluster ausgeführt werden.

   Die folgende Abfrage verwendet die Spalte compute_type zum Überwachen einer Abfrage.

```
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;
```

Beenden einer Abfrage für Cluster

Beenden einer Abfrage für Cluster

Das Vorgehen gilt sowohl für Multi-AZ- als auch für Single-AZ-Cluster.

So beenden Sie eine Abfrage

Sie können außerdem die Seite Queries (Abfragen) verwenden, um eine gerade ausgeführt Abfrage zu beenden.

Ihr Datenbankbenutzer muss über die Rolle sys:operator und über Berechtigungen zum Beenden einer laufenden Abfrage verfügen. Informationen zu Systemrollen finden Sie unter Systemdefinierte Amazon-Redshift-Rollen im Datenbankentwicklerhandbuch zu Amazon Redshift.

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Queries and loads (Abfragen und Ladevorgänge) aus, um die Liste der Abfragen für Ihr Konto anzuzeigen.
3. Wählen Sie die laufende Abfrage aus, die Sie in der Liste beenden möchten. Wählen Sie dann Terminate query (Abfrage beenden) aus.

Verwalten von Clustern mithilfe der Konsole

Verwenden Sie zum Erstellen, Ändern, Anpassen der Größe, Löschen, Neustarten und Sichern von Clustern den Bereich Clusters (Cluster) in der Amazon-Redshift-Konsole.

So zeigen Sie Cluster an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Die Cluster für Ihr Konto in der aktuellen AWS Region werden aufgelistet. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt. Wenn Sie keine Cluster haben, wählen Sie Create cluster (Cluster erstellen) aus, um einen Cluster zu erstellen.
3. Wählen Sie den Cluster-Namen in der Liste aus, um weitere Details zu einem Cluster anzuzeigen.

Themen

- Erstellen eines Clusters
- Erstellen eines Vorschau-Clusters
- Modifizieren eines Clusters
- Löschen eines Clusters
- Neustart eines Clusters
- Größenanpassung eines Clusters
- Upgrade der Release-Version eines Clusters
- Abruf von Informationen zur Clusterkonfiguration
- Anzeige einer Übersicht über den Cluster-Status
- Erstellen eines Snapshots eines Clusters
- Erstellen oder Bearbeiten eines Speicherplatzalarms
- Arbeiten mit Cluster-Leistungsdaten

Erstellen eines Clusters

Bevor Sie einen Cluster erstellen, lesen Sie Überblick über Amazon Redshift und Cluster und Knoten in Amazon Redshift.

So erstellen Sie einen Cluster

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Die Cluster für Ihr Konto in der aktuellen AWS Region werden aufgelistet. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie Create cluster (Cluster erstellen) aus, um einen Cluster zu erstellen.
4. Folgen Sie den Anweisungen auf der Konsolenseite, um die Eigenschaften für die Cluster configuration (Clusterkonfiguration) einzugeben.

   Der folgende Schritt beschreibt eine Amazon Redshift Redshift-Konsole, die auf einer läuft AWS-Region , die RA3-Knotentypen unterstützt. Eine Liste der AWS-Regionen unterstützten RA3-Knotentypen finden Sie unter Überblick über RA3-Knotentypen im Amazon Redshift Management Guide.

Wenn Sie nicht wissen, wie groß Ihr Cluster sein sollte, wählen Sie Help me choose (Hilfe bei der Auswahl) aus. Dadurch wird ein Größenbestimmungsrechner gestartet, der Ihnen Fragen zur Größe und zu Abfragemerkmalen der Daten stellt, die Sie in Ihrem Data Warehouse speichern möchten. Wenn Sie die erforderliche Größe Ihres Clusters kennen (d. h. den Knotentyp und die Anzahl der Knoten), wählen Sie I'll choose (Ich entscheide) aus. Wählen Sie den Node type (Knotentyp) und die Anzahl der Nodes (Knoten) aus, um die Größe Ihres Clusters für den Machbarkeitsnachweis zu bestimmen.

> **Note**
>
> Wenn Ihre Organisation berechtigt ist und Ihr Cluster in einem Gebiet erstellt wird, in AWS-Region dem Amazon Redshift Serverless nicht verfügbar ist, können Sie möglicherweise im Rahmen des kostenlosen Testprogramms von Amazon Redshift einen Cluster erstellen. Wählen Sie entweder Produktion oder Kostenlose Testversion als Antwort auf die Frage: Wofür möchten Sie diesen Cluster verwenden? Wenn Sie Kostenlose Testversion auswählen, erstellen Sie eine Konfiguration mit dem Knotentyp dc2.large. Weitere Informationen zur Auswahl einer kostenlosen Testversion finden Sie unter Kostenloses Testprogramm für Amazon Redshift. Eine Liste, AWS-Regionen wo Amazon Redshift Serverless verfügbar ist, finden Sie unter den für die Redshift Serverless API aufgelisteten Endpoints in der. Allgemeine Amazon Web Services-Referenz

5. Geben Sie im Bereich Datenbankkonfiguration einen Wert für Administrator-Benutzername ein. Für Administratorpasswort können Sie eine der folgenden Optionen auswählen:

   - Ein Passwort erstellen – Verwendung eines von Amazon Redshift generierten Passworts.
   - Administratorpasswort manuell hinzufügen – Verwendung Ihres eigenen Passworts.
   - Administratoranmeldedaten verwalten in AWS Secrets Manager — Amazon Redshift verwendet AWS Secrets Manager , um Ihr Administratorkennwort zu generieren und zu verwalten. Für AWS Secrets Manager die Generierung und Verwaltung Ihres Passworts fällt eine Gebühr an. Informationen zu den Preisen für AWS Secrets Manager finden Sie unter AWS Secrets Manager – Preise.

6. (Optional) Befolgen Sie die Anweisungen auf der Konsolenseite, um Eigenschaften für Cluster permissions (Clusterberechtigungen) einzugeben. Geben Sie Cluster-Berechtigungen an, wenn Ihr Cluster für Sie auf andere AWS Dienste zugreifen muss, z. B. um Daten von Amazon S3 zu laden.

7. Wählen Sie Create cluster (Cluster erstellen) aus, um den Cluster zu erstellen. Es kann einige Minuten dauern, bis der Cluster zur Verwendung bereit ist.

Zusätzliche Konfigurationen

Wenn Sie einen Cluster erstellen, können Sie zusätzliche Eigenschaften angeben, um ihn anzupassen. Weitere Details zu einigen dieser Eigenschaften finden Sie in der folgenden Liste.

IP-Adresstyp

Wählen Sie den IP-Adresstyp für Ihren Cluster aus. Sie können festlegen, dass Ihre Ressourcen nur über das IPv4-Adressierungsprotokoll kommunizieren sollen, oder den Dual-Stack-Modus auswählen, bei dem Ihre Ressourcen sowohl über IPv4 als auch über IPv6 kommunizieren können. Diese Funktion ist nur in den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) verfügbar. Weitere Informationen zu Regionen finden Sie unter AWS Regionen und Availability Zones.

Virtual Private Cloud (VPC)

Wählen Sie eine VPC mit einer Cluster-Subnetzgruppe aus. Nachdem der Cluster erstellt wurde, kann die Cluster-Subnetzgruppe nicht mehr geändert werden.

Parametergruppen

Wählen Sie eine Cluster-Parametergruppe aus, die dem Cluster zugeordnet werden soll. Wenn Sie keine auswählen, verwendet der Cluster die Standard-Parametergruppe.

Verschlüsselung

Wählen Sie, ob alle Daten in dem Cluster und seinen Snapshots verschlüsselt werden sollen. Wenn Sie die Standardeinstellung, None (Keine), unverändert lassen, wird die Verschlüsselung nicht aktiviert. Wenn Sie die Verschlüsselung aktivieren möchten, wählen Sie aus, ob Sie AWS Key Management Service (AWS KMS) oder ein Hardware-Sicherheitsmodul (HSM) verwenden möchten, und konfigurieren Sie dann die entsprechenden Einstellungen. Weitere Informationen zur Verschlüsselung in Amazon Redshift finden Sie unter Verschlüsselung von Amazon-Redshift-Datenbanken.

- KMS

  Wählen Sie Verwenden AWS Key Management Service (AWS KMS), wenn Sie die Verschlüsselung aktivieren und AWS KMS zur Verwaltung Ihres Verschlüsselungsschlüssels

verwenden möchten. Wählen Sie außerdem den zu verwendenden Schlüssel aus. Sie können einen Standardschlüssel, einen Schlüssel aus dem aktuellen Konto oder einen Schlüssel aus einem anderen Konto auswählen.

> **Note**
>
> Wenn Sie einen Schlüssel von einem anderen AWS Konto verwenden möchten, geben Sie den Amazon-Ressourcennamen (ARN) für den zu verwendenden Schlüssel ein. Sie müssen über die Berechtigung zur Verwendung des Schlüssels verfügen. Weitere Informationen zum Zugriff auf Schlüssel in AWS KMS finden Sie unter Steuern des Zugriffs auf Ihre Schlüssel im AWS Key Management Service Entwicklerhandbuch.

Weitere Informationen zur Verwendung von AWS KMS Verschlüsselungsschlüsseln in Amazon Redshift finden Sie unterDatenbankverschlüsselung für Amazon Redshift mithilfe von AWS KMS.

- HSM

  Wählen Sie HSM, wenn Sie die Verschlüsselung aktivieren und ein Hardware Security Module (HSM) zur Verwaltung Ihres Verschlüsselungsschlüssels verwenden möchten.

  Wenn Sie HSM auswählen, wählen Sie Werte aus HSM Connection und HSM Client Certificate aus. Diese Werte sind erforderlich, damit Amazon Redshift und das HSM eine Vertrauensverbindung eingehen können, über die der Cluster-Schlüssel weitergegeben werden kann. Die HSM-Verbindung und das Client-Zertifikat müssen in Amazon Redshift eingerichtet werden, bevor Sie einen Cluster starten. Für weitere Informationen zur Einrichtung von HSM-Verbindungen und Client-Zertifikaten vgl. Verschlüsselung für Amazon Redshift mit Hardwaresicherheitsmodulen.

Maintenance track (Wartungs-Track

Sie können auswählen, ob die verwendete Cluster-Version der Track Current, Trailing oder manchmal Preview ist.

Überwachung

Sie können wählen, ob Sie CloudWatch Alarme erstellen möchten.

Configure cross-region snapshot (Regionsübergreifenden Snapshot konfigurieren

Sie können auswählen, ob Sie regionsübergreifende Snapshots aktivieren möchten.

Automated Snapshot Retention Period (Automatisierter Snapshot-Aufbewahrungszeitraum)

Sie können die Anzahl der Tage (max. 35 Tage) auswählen, für die diese Snapshots aufbewahrt werden sollen. Wenn der Knotentyp DC2 oder DS2 ist, können Sie null (0) Tage wählen, um keine automatisierten Snapshots zu erstellen.

Manual snapshot retention period (Aufbewahrungszeitraum für manuelle Snaspshots)

Sie können die Anzahl der Tage, für die diese Snapshots aufbewahrt werden sollen, oder `Indefinitely` auswählen.

Erstellen eines Vorschau-Clusters

Sie können einen Amazon-Redshift-Cluster in der Vorschau erstellen, um neue Funktionen von Amazon Redshift zu testen. Sie haben nicht die Möglichkeit, diese Funktionen in der Produktion zu verwenden oder Ihren Vorschau-Cluster in einen Produktionscluster oder einen Cluster auf einem anderen Pfad zu verschieben. Weitere Informationen zu den Bedingungen für Vorschauversionen finden Sie unter Betas und Vorversionen in den AWS -Servicebedingungen.

Erstellen eines Clusters in der Vorschau

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Provisioned clusters dashboard (Dashboard für bereitgestellte Cluster) und dann Clusters (Cluster) aus. Die aktuellen Cluster für Ihr Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Auf der Seite mit der Clusterliste (Clusters) wird ein Banner angezeigt, das die Vorschau vorstellt. Wählen Sie die Schaltfläche Create preview cluster (Vorschau-Cluster erstellen) aus, um die Seite zum Erstellen von Clustern zu öffnen.
4. Geben Sie Eigenschaften für Ihren Cluster ein. Wählen Sie den Vorschaupfad (Preview track) aus, der die zu testenden Funktionen enthält. Wir empfehlen, einen Namen für den Cluster zu verwenden, der darauf hinweist, dass sich dieser auf einem Vorschaupfad befindet. Wählen Sie Optionen für Ihren Cluster, einschließlich Optionen mit der Bezeichnung -preview (Vorschau), für die zu testenden Funktionen. Allgemeine Informationen zum Erstellen von Clustern finden Sie unter Erstellen eines Clusters im Amazon-Redshift-Verwaltungshandbuch.
5. Wählen Sie Vorschau-Cluster erstellen aus, um einen Cluster in der Vorschau zu erstellen.

> **Note**
>
> Der `preview_2023`-Track ist der neueste verfügbare Vorschau-Track. Dieser Track unterstützt nur die Erstellung von Clustern mit RA3-Knotentypen. Die Knotentypen DC2 und DS2 sowie alle älteren Knotentypen werden nicht unterstützt.

6. Wenn Ihr Vorschau-Cluster verfügbar ist, verwenden Sie Ihren SQL-Client, um Daten zu laden und abzufragen.

Informationen zur Vorschau in Redshift-Serverless-Arbeitsgruppen finden Sie unter Erstellen einer Vorschau-Arbeitsgruppe.

Modifizieren eines Clusters

Wenn Sie einen Cluster modifizieren, werden Änderungen an den folgenden Optionen sofort angewendet:

- VPC-Sicherheitsgruppen
- Publicly accessible (Öffentlich zugänglich)
- Admin user password (Passwort des Administratorbenutzers)
- HSM-Verbindung
- HSM Client Certificate (HSM-Clientzertifikat
- Maintenance detail (Wartungsdetails
- Snapshot preferences (Snapshot-Voreinstellungen

Änderungen an den folgenden Optionen werden erst nach dem Neustart des Clusters wirksam:

- Cluster Identifier (Cluster-Kennung

  Amazon Redshift startet den Cluster automatisch neu, wenn Sie Cluster Identifier (Cluster-ID) ändern.
- Enhanced VPC routing (Erweitertes VPC-Routing

  Amazon Redshift startet den Cluster automatisch neu, wenn Sie Enhanced VPC Routing ändern.
- Cluster-Parametergruppe

- IP-Adresstyp

  Diese Funktion ist nur in den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) verfügbar. Weitere Informationen zu Regionen finden Sie unter AWS Regionen und Availability Zones.

Wenn Sie die Aufbewahrungszeit für automatisierte Snapshots verkürzen, werden automatisierte Snapshots, deren Einstellungen außerhalb des neuen Aufbewahrungszeitraums liegen, gelöscht. Weitere Informationen finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.

Weitere Informationen zu Cluster-Eigenschaften finden Sie unter Zusätzliche Konfigurationen.

So modifizieren Sie einen Cluster:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus.
3. Wählen Sie den zu ändernden Cluster aus.
4. Wählen Sie Edit. Die Seite Edit Cluster (Cluster bearbeiten) wird angezeigt.
5. Aktualisieren Sie die Cluster-Eigenschaften. Nachfolgend sind einige der Eigenschaften aufgeführt, die Sie ändern können:

   - Cluster Identifier (Cluster-Kennung)
   - Snapshot-Aufbewahrung
   - Cluster relocation (Cluster-Verschiebung)

   Die Konsole stellt Links zur entsprechenden Registerkarte mit Cluster-Details bereit, über die Sie die Einstellungen für Netzwerk und Sicherheit, Wartung und Datenbankkonfigurationen bearbeiten können.
6. Wählen Sie Save Changes (Änderungen speichern).

Löschen eines Clusters

Sie können Ihren Cluster löschen, falls Sie ihn nicht mehr benötigen. Wenn Sie die Bereitstellung eines neuen Clusters mit denselben Daten und derselben Konfiguration des Clusters planen, den Sie löschen, benötigen Sie einen manuellen Snapshot. Wenn Sie einen manuellen Snapshot verwenden,

können Sie ihn später wiederherstellen und dann damit den Cluster weiter betreiben. Wenn Sie Ihren Cluster ohne abschließenden Snapshot löschen, werden die Clusterdaten gelöscht. In beiden Fällen werden automatisierte Snapshots nach dem Löschen des Clusters gelöscht, manuelle Snapshots werden jedoch aufbewahrt, bis Sie sie löschen. Für manuelle Snapshots fallen möglicherweise Speichergebühren für Amazon Simple Storage Service an, je nach der Speichermenge, die Sie für Amazon-Redshift-Snapshots für Ihre Cluster verfügbar haben. Weitere Informationen finden Sie unter Schließen und Löschen von Clustern.

Durch das Löschen eines Clusters werden auch alle zugehörigen AWS Secrets Manager Geheimnisse gelöscht.

Löschen eines Clusters

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus.
3. Wählen Sie den zu löschenden Cluster aus.
4. Klicken Sie bei Actions auf Delete. Die Seite Delete cluster (Cluster löschen) wird angezeigt.
5. Wählen Sie Delete cluster (Cluster löschen) aus.

Neustart eines Clusters

Wenn Sie einen Cluster neu starten, wird sein Status auf `rebooting` gesetzt, und nach Abschluss des Neustarts wird ein Clusterereignis erstellt. Alle ausstehenden Cluster-Änderungen werden bei diesem Neustart angewendet.

So starten Sie einen Cluster neu:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus.
3. Wählen Sie den Cluster aus, den Sie neu starten möchten.
4. Wählen Sie für Actions (Aktionen) Reboot cluster (Cluster neu starten) aus. Die Seite Reboot cluster (Cluster neu starten) wird angezeigt.
5. Wählen Sie Reboot cluster (Cluster neu starten) aus.

Größenanpassung eines Clusters

Wenn Sie die Größe eines Clusters anpassen, geben Sie eine Anzahl von Knoten bzw. den Knotentyp an, die/der sich von der aktuellen Konfiguration des Clusters unterscheidet. Während die Größe des Clusters angepasst wird, können Sie keine Schreib- oder Lese-/Schreib-Abfragen auf dem Cluster ausführen, es sind lediglich Lese-Abfragen möglich.

Für weitere Informationen zur Größenanpassung von Clustern, einschließlich einer Erläuterung des Vorgehens bei der Größenanpassung von Clustern mit verschiedenen Konzepten, vgl. Größenanpassung von Clustern.

So passen Sie die Größe eines Clusters an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus.
3. Wählen Sie den Cluster aus, dessen Größe geändert werden soll.
4. Wählen Sie für Actions (Aktionen) Resize (Größe ändern) aus. Die Seite Resize cluster (Cluster-Größe ändern) wird angezeigt.
5. Folgen Sie den Anweisungen auf der Seite. Sie können die Größe des Clusters jetzt, einmal zu einer bestimmten Zeit, ändern oder die Größe Ihres Clusters nach einem Zeitplan vergrößern und verkleinern.
6. Wählen Sie je nach Ihrer Auswahl die Option Resize now (Große jetzt ändern) oder Schedule resize (Größenänderung planen) aus.

Wenn Sie reservierte Knoten haben, zum Beispiel reservierte DS2-Knoten, können Sie auf reservierte RA3-Knoten aktualisieren. Sie können dies tun, wenn Sie über die Konsole eine Wiederherstellung von einem Snapshot oder eine elastische Größenanpassung durchführen. Sie können die Konsole verwenden, um sich durch den Prozess führen zu lassen. Weitere Informationen zum Aktualisieren auf RA3-Knoten finden Sie unter Migration zu RA3-Knotentypen.

Upgrade der Release-Version eines Clusters

Sie können ein Upgrade der Wartungsversion eines Clusters durchführen, bei dem der Wert für Release Status (Versionsstatus) New release available (Neue Version verfügbar) lautet. Wenn Sie die Wartungsversion upgraden, können Sie auswählen, ob Sie sofort upgraden oder im nächsten Wartungsfenster upgraden möchten.

> **Important**
>
> Wenn Sie sofortige Aktualisierung auswählen, ist Ihr Cluster bis zum Abschluss der Aktualisierung offline.

So aktualisieren Sie einen Cluster auf eine neue Release-Version:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus.
3. Wählen Sie den zu aktualisierenden Cluster aus.
4. Wählen Sie für Actions (Aktionen) Upgrade cluster version (Cluster-Version upgraden) aus. Die Seite Upgrade cluster version (Cluster-Version upgraden) wird angezeigt.
5. Folgen Sie den Anweisungen auf der Seite.
6. Wählen Sie Upgrade cluster version (Clusterversion aktualisieren) aus.

Abruf von Informationen zur Clusterkonfiguration

So zeigen Sie Informationen zu einem Cluster an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster-Namen aus der Liste aus, um die Details zu dem Cluster aufzurufen. Die Details des Clusters werden möglicherweise einschließlich der Registerkarten Cluster performance (Cluster-Leistung), Query monitoring (Abfrageüberwachung), Databases (Datenbanken), Datashares, Schedules (Zeitpläne), Maintenance (Wartung) und Properties (Eigenschaften) angezeigt.
3. Wählen Sie die einzelnen Registerkarten aus, um weitere Details anzuzeigen.

Anzeige einer Übersicht über den Cluster-Status

So zeigen Sie den Status eines Clusters an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.

2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus.
3. Zeigt den Status des Clusters in der Spalte Status an.

Erstellen eines Snapshots eines Clusters

So erstellen Sie einen Snapshot eines Clusters:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus.
3. Wählen Sie den Cluster aus, für den Sie einen Snapshot erstellen möchten.
4. Wählen Sie für Actions (Aktionen) Create snapshot (Snapshot erstellen) aus. Die Seite Create snapshot (Snapshot erstellen) wird angezeigt.
5. Folgen Sie den Anweisungen auf der Seite.
6. Wählen Sie Create snapshot (Snapshot erstellen) aus.

Erstellen oder Bearbeiten eines Speicherplatzalarms

So erstellen Sie einen Speicherplatzalarm für einen Cluster

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Alarms (Alarme) aus.
3. Wählen Sie für Actions (Aktionen) Create alarm (Alarm erstellen) aus. Die Seite Create alarm (Alarm erstellen) wird angezeigt.
4. Folgen Sie den Anweisungen auf der Seite.
5. Wählen Sie Create Alarm (Alarm erstellen) aus.

Arbeiten mit Cluster-Leistungsdaten

In der neuen Konsole können Sie die Cluster-Leistung auf der Registerkarte Cluster performance (Cluster-Leistung) der Cluster-Detailseite bearbeiten.

Verwaltung von Clustern mithilfe der AWS CLI und der Amazon Redshift Redshift-API

Sie können die folgenden AWS CLI Operationen verwenden, um Cluster in Amazon Redshift zu verwalten.

- 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

Sie können zur Verwaltung von Clustern in Amazon Redshift die folgenden API-Operationen verwenden.

- CancelResize
- CreateCluster
- DeleteCluster
- DescribeClusters
- DescribeClusterVersions
- DescribeNodeConfigurationOptions
- DescribeResize
- DescribeOrderableClusterOptions
- ModifyCluster

- PauseCluster
- RebootCluster
- ResizeCluster
- ResumeCluster

Verwaltung von Clustern in einer VPC

Themen

- Übersicht
- Erstellen eines Clusters in einer VPC
- Verwalten von VPC-Sicherheitsgruppen für einen Cluster
- Konfigurieren der Kommunikationseinstellungen von Sicherheitsgruppen für einen Amazon-Redshift-Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe
- So funktioniert Amazon Redshift mit VPC-Freigabe für AWS-Ressourcen
- Amazon-Redshift-Cluster-Subnetzgruppen

Übersicht

Amazon Redshift unterstützt sowohl die Plattformen EC2-VPC als auch EC2-Classic, um einen Cluster in einer Virtual Private Cloud (VPC), basierend auf dem Amazon-VPC-Service, zu starten. Weitere Informationen finden Sie unter Verwenden von EC2-VPC beim Erstellen Ihres Clusters.

> **Note**
>
> Amazon Redshift unterstützt das Starten von Clustern in Dedicated-Tenancy-VPCs nicht. Weitere Informationen finden Sie unter Dedicated Instances im Amazon-VPC-Benutzerhandbuch.

Bei der Bereitstellung eines Clusters in einer VPC müssen Sie Folgendes tun:

- Stellen Sie VPC-Informationen bereit.

  Wenn Sie von Amazon Redshift die Erstellung eines Clusters in Ihrer VPC anfordern, müssen Sie Ihre VPC-Informationen durch die Erstellung einer Cluster-Subnetzgruppe bereitstellen. Diese

Informationen beinhalten die VPC-ID und eine Liste der Subnetze in Ihrer VPC. Wenn Sie einen Cluster starten, geben Sie die Cluster-Subnetzgruppe an, damit Amazon Redshift Ihren Cluster in einem der Subnetze in der VPC bereitstellen kann. Weitere Informationen zum Erstellen von Subnetzgruppen in Amazon Redshift finden Sie unter Amazon-Redshift-Cluster-Subnetzgruppen. Weitere Informationen zum Einrichten einer VPC finden Sie unter Erste Schritte mit Amazon VPC im Handbuch Erste Schritte mit Amazon VPC.

- Konfigurieren Sie optional die öffentlich zugänglichen Optionen.

  Wenn Sie Ihren Cluster so konfigurieren, dass er öffentlich zugänglich ist, verwendet Amazon Redshift eine Elastic-IP-Adresse für die externe IP-Adresse. Eine Elastic-IP-Adresse ist eine statische IP-Adresse. Sie gibt Ihnen die Möglichkeit, Ihre zugrunde liegende Konfiguration ohne Auswirkungen auf die IP-Adresse zu ändern, die Clients für Verbindungen zu Ihrem Cluster verwenden. Diese Vorgehensweise kann in Situationen wie der Wiederherstellung nach einem Ausfall sehr nützlich sein. Ob Sie eine Elastic-IP-Adresse erstellen, hängt von Ihrer Einstellung für die Availability-Zone-Verschiebung ab. Es gibt zwei Optionen:

  1. Wenn Sie die Availability-Zone-Verschiebung aktiviert haben und den öffentlichen Zugriff aktivieren möchten, geben Sie keine Elastic-IP-Adresse an. Eine Elastic-IP-Adresse, die von Amazon Redshift verwaltet wird, wird zugewiesen. Sie ist mit Ihrem AWS-Konto verknüpft.
  2. Wenn Sie die Availability-Zone-Verschiebung deaktiviert haben und den öffentlichen Zugriff aktivieren möchten, können Sie eine Elastic-IP-Adresse für die VPC in Amazon EC2 erstellen, bevor Sie Ihren Amazon-Redshift-Cluster starten. Wenn Sie keine IP-Adresse erstellen, stellt Amazon Redshift eine konfigurierte Elastic-IP-Adresse bereit, die für die VPC verwendet werden soll. Diese Elastic-IP-Adresse wird von Amazon Redshift verwaltet und ist Ihrem AWS-Konto nicht zugeordnet.

  Weitere Informationen finden Sie unter Elastische IP-Adressen im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

  In einigen Fällen kann es vorkommen, dass Sie einen öffentlich zugänglichen Cluster in einer VPC haben, die Sie mit ihm verbinden möchten, indem Sie die private IP-Adresse innerhalb der VPC verwenden. Wenn ja, legen Sie die folgenden VPC-Parameter auf fest `true`:

  - `DNS resolution`
  - `DNS hostnames`

  Angenommen, Sie haben einen öffentlich zugänglichen Cluster in einer VPC, setzen diese Parameter aber in der VPC nicht auf `true`. In diesen Fällen lösen Verbindungen aus der VPC heraus die Elastic IP-Adresse des Clusters statt die private IP-Adresse auf. Wir empfehlen, diese

Parameter auf `true` zu setzen und die private IP-Adresse für einen öffentlich zugänglichen Cluster bei Verbindungsherstellung aus der VPC heraus zu verwenden. Weitere Informationen finden Sie unter Verwendung von DNS in Ihrer VPC im Amazon VPC Benutzerhandbuch.

> **Note**
>
> Wenn Sie einen bestehenden öffentlich zugänglichen Cluster in einer VPC haben, verwenden Verbindungen innerhalb der VPC weiterhin die Elastic IP-Adresse, um sich mit dem Cluster zu verbinden, bis Sie die Größe des Clusters ändern. Dies geschieht auch bei den vorhergehenden Parametersätzen. Alle neuen Cluster folgen dem neuen Verhalten. Sie verwenden die private IP-Adresse bei der Verbindung mit dem öffentlich zugänglichen Cluster innerhalb derselben VPC.

Die Elastic IP-Adresse ist eine externe IP-Adresse für den Zugriff auf den Cluster außerhalb einer VPC. Er steht in keiner Verbindung zu den öffentlichen und privaten IP-Adressen des Cluster-Knotens, die in der Amazon-Redshift-Konsole unter Connection details (Verbindungsdetails) angezeigt werden. Die öffentlichen und privaten Cluster-Knoten-IP-Adressen werden unabhängig davon angezeigt, ob der Cluster öffentlich zugänglich ist oder nicht. Sie werden nur unter bestimmten Umständen verwendet, um Eingangsregeln auf dem Remote-Host zu konfigurieren. Diese Umstände treten auf, wenn Sie Daten von einer Amazon-EC2-Instance oder einem anderen Remote-Host über eine SSH-Verbindung laden. Weitere Informationen finden Sie unter Schritt 1: Abrufen des öffentlichen Schlüssels des Clusters und der IP-Adressen des Cluster-Knotens im Datenbankentwicklerhandbuch zu Amazon Redshift.

Die Option, einen Cluster mit einer Elastic IP-Adresse zu verknüpfen, ist verfügbar, wenn Sie den Cluster erstellen oder den Cluster aus einem Snapshot wiederherstellen. In einigen Fällen können Sie den Cluster mit einer Elastic IP-Adresse verknüpfen oder eine Elastic IP-Adresse ändern, die dem Cluster zugeordnet ist. Um eine elastische IP-Adresse anzufügen, nachdem der Cluster erstellt wurde, aktualisieren Sie zuerst den Cluster so, dass er nicht öffentlich zugänglich ist. Machen Sie ihn dann öffentlich zugänglich und fügen Sie im gleichen Vorgang eine elastische IP-Adresse hinzu.

- Weisen Sie eine VPC-Sicherheitsgruppe zu.

  Anschließend gewähren Sie den eingehenden Zugriff mithilfe einer VPC-Sicherheitsgruppe. Diese VPC-Sicherheitsgruppe muss den Zugriff über den Datenbankport für den Cluster gewähren, so dass Sie mithilfe von SQL-Client-Tools eine Verbindung herstellen können. Sie

können dies im Voraus konfigurieren oder nach dem Start des Clusters Regeln hinzufügen. Weitere Informationen finden Sie unter Konfiguration der Kommunikationseinstellungen für Sicherheitsgruppen für Amazon-Redshift-Cluster. Dort finden Sie Anleitungen zur Konfiguration eingehender und ausgehender Regeln zwischen einem Client und einem bereitgestellten Cluster oder einer Amazon-Redshift-Serverless-Arbeitsgruppe. Eine weitere Ressource, die Ihnen hilft, Sicherheitsgruppen zu verstehen, ist Sicherheit in Ihrer VPC im Amazon-VPC-Benutzerhandbuch. Beachten Sie, dass Sie die Amazon-Redshift-Cluster-Sicherheitsgruppen nicht benutzen können, um eingehenden Zugriff auf den Cluster zu gewähren.

Weitere Informationen zur Arbeit mit Clustern in einer VPC finden Sie unter Erstellen eines Clusters in einer VPC.

Wiederherstellen eines Cluster-Snapshots in einer VPC

Ein Snapshot eines Clusters in einer VPC kann nur in einer VPC, nicht außerhalb davon, wiederhergestellt werden. Sie können ihn in der selben VPC oder in einer anderen VPC in Ihrem Konto wiederherstellen. Weitere Informationen zu -Snapshots finden Sie unter Amazon-Redshift-Snapshots und -Sicherungen.

Erstellen eines Clusters in einer VPC

Nachfolgend finden Sie die allgemeinen Schritte für die Bereitstellung eines Clusters in Ihrer virtuellen Private Cloud (VPC).

So erstellen Sie einen Cluster in einer VPC:

1. Richten Sie eine VPC ein.

   Sie können Ihren Cluster entweder in der Standard-VPC für Ihr Konto oder, falls vorhanden, in einer von Ihnen erstellten VPC erstellen. Weitere Informationen finden Sie unter Verwenden von EC2-VPC beim Erstellen Ihres Clusters. Informationen zum Erstellen einer Standard-VPC finden Sie unter Erstellen einer VPC im Amazon-VPC-Benutzerhandbuch. Notieren Sie sich die VPC-ID, das Subnetz und die Availability Zone des Subnetzes. Diese Informationen benötigen Sie beim Start Ihres Clusters.

   > **Note**
   >
   > Sie müssen mindestens ein Subnetz in Ihrer VPC definiert haben, damit Sie dieses im nächsten Schritt der Cluster-Subnetzgruppe hinzufügen können. Weitere Informationen

zum Hinzufügen eines Subnetzes zu Ihrer VPC finden Sie unter Hinzufügen eines Subnetzes zu Ihrer VPC im Amazon-VPC-Benutzerhandbuch.

2. Erstellen Sie eine Amazon-Redshift-Cluster-Subnetzgruppe, um festzulegen, welches Subnetz Ihr Amazon-Redshift-Cluster in der VPC verwenden kann.

   Sie können eine Cluster-Subnetzgruppe entweder über die Amazon-Redshift-Konsole oder programmgesteuert erstellen. Weitere Informationen finden Sie unter Amazon-Redshift-Cluster-Subnetzgruppen.

3. Autorisieren Sie den Zugriff für eingehende Verbindungen in einer VPC-Sicherheitsgruppe, die Sie dem Cluster zuordnen.

   Sie können einem Client außerhalb der VPC (im öffentlichen Internet) die Verbindung zum Cluster ermöglichen. Dazu ordnen Sie den Cluster einer VPC-Sicherheitsgruppe zu, die eingehenden Zugriff auf den Port gewährt, den Sie beim Start des Clusters verwendet haben. Weitere Beispiele für Sicherheitsgruppenregeln finden Sie unter Sicherheitsgruppenregeln im Amazon-VPC-Benutzerhandbuch.

4. Folgen Sie den Schritten in Erste Schritte mit Amazon Redshift im Handbuch Erste Schritte mit Amazon Redshift, um einen Cluster zu erstellen. Nehmen Sie beim Anlegen Ihres Clusters die folgenden Änderungen vor:

   - Um den Abschnitt Additional configurations (Zusätzliche Konfigurationen) anzuzeigen, deaktivieren Sie Use defaults (Standardeinstellungen verwenden).
   - Geben Sie im Bereich Network and security (Netzwerk und Sicherheit) die Virtual Private Cloud (VPC), Cluster subnet group (Cluster-Subnetzgruppe) und VPC security group (VPC-Sicherheitsgruppe) an, die Sie eingerichtet haben.

Jetzt können Sie den Cluster verwenden. Sie können den Cluster anhand der „Erste Schritte“-Anweisungen testen, indem Sie Beispieldaten hochladen und Beispielabfragen versuchen.

Verwalten von VPC-Sicherheitsgruppen für einen Cluster

Wenn Sie einen Amazon-Redshift-Cluster bereitstellen, ist dieser standardmäßig gesperrt, so dass niemand darauf zugreifen kann. Um anderen Benutzern eingehenden Zugriff auf einen Amazon-Redshift-Cluster zu gewähren, ordnen Sie den Cluster einer Sicherheitsgruppe zu. Wenn Sie die EC2-VPC-Plattform nutzen, können Sie entweder eine bestehende Amazon-VPC-Sicherheitsgruppe verwenden oder eine neue definieren. Sie ordnen sie dann einem Cluster zu, wie im Folgenden

beschrieben. Wenn Sie auf der EC2 Classic-Plattform arbeiten, definieren Sie eine Cluster-Sicherheitsgruppe und verbinden sie mit einem Cluster. Weitere Informationen zur Verwendung von Cluster-Sicherheitsgruppen auf der EC2 Classic-Plattform finden Sie unter Amazon-Redshift-Cluster-Sicherheitsgruppen.

Eine VPC-Sicherheitsgruppe besteht aus einem Satz von Regeln, die den Zugriff auf eine Instance in der VPC, etwa Ihren Cluster, steuern. Einzelne Regeln steuern den Zugriff auf der Grundlage von Bereichen von IP-Adressen oder auf der Grundlage anderer VPC-Sicherheitsregeln. Wenn Sie eine VPC-Sicherheitsgruppe mit einem Cluster verbinden, steuern die in der VPC-Sicherheitsgruppe definierten Regeln den Zugriff auf den Cluster.

Jedem Cluster, den Sie auf der EC2-VPC-Plattform bereitstellen, sind eine oder mehrere Amazon-VPC-Sicherheitsgruppen zugeordnet. Amazon VPC stellt eine VPC-Sicherheitsgruppe namens „default“ (Standard) bereit, die beim Erstellen der VPC automatisch erstellt wird. Jedem Cluster, den Sie in der VPC starten, wird automatisch die VPC-Standardsicherheitsgruppe zugewiesen, wenn Sie beim Start des Clusters nicht eine andere VPC-Sicherheitsgruppe festlegen. Sie können eine VPC-Sicherheitsgruppe einem Cluster zuweisen, wenn Sie den Cluster erstellen, oder Sie können dies später tun, indem Sie den Cluster modifizieren.

Die folgende Tabelle beschreibt die Standardregeln für die VPC-Standardsicherheitsgruppe.

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The security group ID (sg-*xxxxxxxx*)	All	All	Allow inbound traffic from instances assigned to the same security group
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	All	All	Allow all outbound traffic

Sie können die Regeln für die Standard-VPC-Sicherheitsgruppe nach Bedarf für Ihren Amazon-Redshift-Cluster ändern.

Wenn die VPC-Standardsicherheitsgruppe für Ihre Zwecke ausreicht, müssen Sie keine weitere erstellen. Sie können jedoch optional weitere VPC-Sicherheitsgruppen erstellen, um den eingehenden Zugriff auf Ihren Cluster besser verwalten zu können. Nehmen wir beispielsweise an, Sie führen einen Service auf einem Amazon-Redshift-Cluster aus und bieten Ihren Kunden mehrere verschiedene Service-Levels an. Wenn Sie nicht für alle Service Levels den gleichen Zugriff gewähren möchten, können Sie separate VPC-Sicherheitsgruppen erstellen, jeweils eine für jeden Service Level. Anschließend können Sie diese VPC-Sicherheitsgruppen mit Ihrem Cluster verbinden.

Sie können bis zu 100 VPC-Sicherheitsgruppen für eine VPC erstellen und eine VPC-Sicherheitsgruppe vielen Clustern zuordnen. Sie können einem Cluster jedoch nur bis zu fünf VPC-Sicherheitsgruppen zuordnen.

Amazon Redshift wendet Änderungen auf eine VPC-Sicherheitsgruppe sofort an. Wenn Sie die VPC-Sicherheitsgruppe mit einem Cluster verbunden haben, werden daher eingehende Cluster-Zugriffsregeln in der aktualisierten VPC-Sicherheitsgruppe sofort angewendet.

Sie können VPC-Sicherheitsgruppen hier erstellen und ändern: https://console.aws.amazon.com/vpc/. Sie können VPC-Sicherheitsgruppen auch programmgesteuert mit der AWS CLI, der Amazon-EC2-CLI und den AWS Tools for Windows PowerShell verwalten. Weitere Informationen zur Arbeit mit VPC-Sicherheitsgruppen finden Sie unter Sicherheitsgruppen für Ihre VPC im Amazon-VPC-Benutzerhandbuch.

Konfigurieren der Kommunikationseinstellungen von Sicherheitsgruppen für einen Amazon-Redshift-Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe

Dieses Thema hilft Ihnen dabei, Ihre Sicherheitsgruppen so zu konfigurieren, dass Netzwerkverkehr ordnungsgemäß weitergeleitet und empfangen wird. Im Folgenden sind Beispiele für häufige Anwendungsfälle aufgeführt:

- Sie aktivieren den öffentlichen Zugriff für einen Amazon-Redshift-Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe, aber diese(r) empfängt keinen Datenverkehr. Sie müssen dafür eine Regel für eingehenden Datenverkehr konfigurieren, damit der Cluster/die Arbeitsgruppe Datenverkehr aus dem Internet erhält.
- Der Cluster ist nicht öffentlich zugänglich und Sie benutzen die vorkonfigurierte Standard-VPC-Sicherheitsgruppe, um eingehenden Datenverkehr zuzulassen. Sie müssen jedoch eine andere Sicherheitsgruppe als die Standardsicherheitsgruppe verwenden und diese benutzerdefinierte Sicherheitsgruppe lässt keinen eingehenden Datenverkehr zu. Sie müssen sie so konfigurieren, dass die Kommunikation zugelassen wird.

Die folgenden Abschnitte helfen Ihnen dabei, die richtige Antwort für jeden Anwendungsfall auszuwählen und zeigen Ihnen, wie der Netzwerkverkehr gemäß Ihren Anforderungen konfiguriert wird. Sie können die Schritte optional verwenden, um die Kommunikation mit anderen privaten Sicherheitsgruppen einzurichten.

> **Note**
>
> Die Einstellungen für den Netzwerkverkehr werden in Amazon Redshift in den meisten Fällen nicht automatisch konfiguriert. Dies liegt daran, dass sie auf granularer Ebene unterschiedlich sein können, je nachdem, ob die Quelle des Datenverkehrs das Internet oder eine private Sicherheitsgruppe ist, und weil die Sicherheitsanforderungen variieren.

Öffentlicher Zugriff mit Konfiguration der standardmäßigen oder einer benutzerdefinierten Sicherheitsgruppe

Wenn Sie einen Cluster erstellen oder bereits erstellt haben, führen Sie die folgenden Konfigurationsschritte durch, um den Cluster öffentlich zugänglich zu machen. Dies gilt sowohl für die Auswahl der Standardsicherheitsgruppe als auch für eine benutzerdefinierte Sicherheitsgruppe:

1. Suchen Sie nach den Netzwerkeinstellungen:

   - Wählen Sie für einen bereitgestellten Amazon-Redshift-Cluster die Registerkarte Eigenschaften und dann unter Netzwerk- und Sicherheitseinstellungen die VPC für Ihren Cluster aus.
   - Wählen Sie für eine Amazon-Redshift-Serverless-Arbeitsgruppe die Option Arbeitsgruppenkonfiguration aus. Wählen Sie die Arbeitsgruppe aus der Liste aus. Wählen Sie dann unter Datenzugriff im Fenster Netzwerk und Sicherheit die Option Bearbeiten aus.
2. Konfigurieren Sie das Internet-Gateway und die Routing-Tabelle für Ihre VPC. Sie starten die Konfiguration, indem Sie die VPC nach Namen auswählen. Das VPC-Dashboard wird geöffnet. Wenn über das Internet eine Verbindung mit einem öffentlich zugänglichen Cluster hergestellt werden soll, muss der Routing-Tabelle ein Internet-Gateway hinzugefügt werden. Sie können dies konfigurieren, indem Sie im VPC-Dashboard Routing-Tabellen auswählen. Bestätigen Sie, dass für das Ziel des Internet-Gateways die Quelle 0.0.0.0/0 oder eine öffentliche IP-CIDR-Adresse festgelegt ist. Die Routing-Tabelle muss der VPC zugeordnet sein, in der sich Ihr Cluster befindet. Weitere Informationen zur Einrichtung des Internetzugangs für eine VPC, wie hier beschrieben, finden Sie unter Aktivieren des Internetzugangs in der Amazon-VPC-Dokumentation. Weitere Informationen zum Konfigurieren einer Routing-Tabelle finden Sie unter Konfigurieren von Routing-Tabellen.
3. Nachdem Sie das Internet-Gateway und die Routing-Tabelle konfiguriert haben, kehren Sie zu den Netzwerkeinstellungen für Redshift zurück. Öffnen Sie den eingehenden Zugriff, indem Sie

die Sicherheitsgruppe und dann die Regeln für eingehenden Datenverkehr auswählen. Wählen Sie Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) aus.

4. Wählen Sie das Protokoll und den Port für die Regel für eingehenden Datenverkehr gemäß Ihren Anforderungen, um Datenverkehr von Clients zuzulassen. Wählen Sie für einen RA3-Cluster einen Port innerhalb der Bereiche 5431–5455 oder 8191–8215 aus. Wenn Sie damit fertig sind, speichern Sie die einzelnen Regeln.
5. Bearbeiten Sie die Einstellung Öffentlich zugänglich, um sie zu aktivieren. Sie können dies im Menü Aktionen Ihres Clusters oder Ihrer Arbeitsgruppe tun.

Wenn Sie die Einstellung für den öffentlichen Zugriff aktivieren, erstellt Redshift eine Elastic-IP-Adresse. Dabei handelt es sich um eine statische IP-Adresse, die mit Ihrem AWS-Konto verbunden ist. Clients außerhalb der VPC können damit eine Verbindung herstellen.

Weitere Informationen zum Konfigurieren Ihrer Sicherheitsgruppe finden Sie unter Amazon-Redshift-Cluster-Sicherheitsgruppen.

Sie können Ihre Regeln testen, indem Sie sich mit einem Client verbinden. Gehen Sie wie folgt vor, wenn Sie eine Verbindung zu Amazon Redshift Serverless herstellen. Nachdem Sie die Netzwerkkonfiguration abgeschlossen haben, stellen Sie eine Verbindung mit Ihrem Client-Tool wie etwa Amazon Redshift RSQL her. Geben Sie unter Verwendung Ihrer Serverless-Domäne von Amazon Redshift als Host Folgendes ein:

```
rsql -h workgroup-name.account-id.region.amazonaws.com -U admin -d dev -p 5439
```

Privater Zugriff mit Konfiguration der standardmäßigen oder einer benutzerdefinierten Sicherheitsgruppe

Wenn Sie nicht über das Internet mit Ihrem Cluster oder Ihrer Arbeitsgruppe kommunizieren, wird diese(r) als privat zugänglich bezeichnet. Wenn Sie bei der Erstellung die Standardsicherheitsgruppe ausgewählt haben, beinhaltetdie Sicherheitsgruppe die folgenden Standardkommunikationsregeln:

- Eine Regel, die eingehenden Datenverkehr von allen Ressourcen zulässt, die der Sicherheitsgruppe zugewiesen sind.
- Eine Regel, die den gesamten ausgehenden Datenverkehr zulässt. Das Ziel für diese Regel ist 0.0.0.0/0. In der CIDR-Notation (Classless Inter-Domain Routing) steht dies für alle möglichen IP-Adressen.

Sie können die Regeln in der Konsole anzeigen, indem Sie die Sicherheitsgruppe für Ihren Cluster oder Ihre Arbeitsgruppe auswählen.

Wenn Ihr Cluster oder Ihre Arbeitsgruppe und Ihr Client beide die Standardsicherheitsgruppe benutzen, ist keine zusätzliche Konfiguration erforderlich, um Netzwerkverkehr zuzulassen. Wenn Sie jedoch Regeln in der Standardsicherheitsgruppe für Redshift oder den Client löschen oder ändern, gilt dies nicht mehr. In diesem Fall müssen Sie Regeln konfigurieren, um eingehende und ausgehende Kommunikation zuzulassen. Eine gängige Konfiguration für Sicherheitsgruppen ist die folgende:

- Für eine Amazon-EC2-Client-Instance:
  - Eine Regel für eingehenden Datenverkehr, die die IP-Adresse des Clients zulässt.
  - Eine Regel für ausgehenden Datenverkehr, die den IP-Adressbereich (CIDR-Block) aller Subnetze zulässt, die für die Redshift-Nutzung bereitgestellt werden. Oder Sie können 0.0.0.0/0 angeben, was alle IP-Adressbereiche umfasst.
- Für Ihren Redshift-Cluster oder Ihre Arbeitsgruppe:
  - Eine Regel, die eingehenden Datenverkehr von der Client-Sicherheitsgruppe zulässt.
  - Eine Regel, die ausgehenden Datenverkehr zu 0.0.0.0/0 zulässt. Typischerweise lässt die Regel allen ausgehenden Datenverkehr zu. Optional können Sie eine Regel für ausgehenden Datenverkehr hinzufügen, um den Datenverkehr zur Client-Sicherheitsgruppe zuzulassen. In diesem optionalen Fall ist eine Regel für ausgehenden Datenverkehr nicht immer erforderlich, da der Antwortdatenverkehr für jede Anfrage die Instance erreichen darf. Weitere Informationen zum Anfrage- und Antwortverhalten finden Sie unter Sicherheitsgruppen im Amazon VPC-Benutzerhandbuch.

Wenn Sie die Konfiguration für Subnetze oder Sicherheitsgruppen ändern, die für die Verwendung von Redshift angegeben sind, müssen Sie möglicherweise die Datenverkehrsregeln entsprechend ändern, um die Kommunikation aufrechtzuerhalten. Weitere Informationen zum Erstellen von Regeln für eingehenden und ausgehenden Datenverkehr finden Sie unter VPC-CIDR-Blöcke im Amazon-VPC-Benutzerhandbuch. Weitere Informationen zum Verbinden mit Amazon Redshift von einem Client aus finden Sie unter Konfigurieren von Verbindungen in Amazon Redshift.

So funktioniert Amazon Redshift mit VPC-Freigabe für AWS-Ressourcen

Mit VPC-Freigabe können Sie AWS-Anwendungsressourcen wie Amazon-EC2-Instances und andere AWS-Services in einer Virtual Private Cloud (VPC) erstellen. Das Konto, das die VPC besitzt (der Besitzer) gibt ein oder mehrere Subnetze für andere Konten (Teilnehmer) frei, die zur selben

AWS-Organisation gehören. Hier wird beschrieben, wie Sie einen Amazon-Redshift-Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe in einer gemeinsam genutzten VPC erstellen und verwenden können.

Zu den Vorteilen der VPC-Freigabe gehört, dass Sie nicht so viele VPCs verwalten müssen, und es kann Ihnen helfen, Ihr Netzwerk zu vereinfachen. Der Vorteil für Amazon-Redshift-Administratoren und -Benutzer besteht speziell darin, dass Redshift-Ressourcen in der freigegebenen VPC produktiv arbeiten können. Weitere Informationen zur VPC-Freigabe finden Sie unter Freigeben Ihrer VPC für andere Konten. Darin wird näher auf die Vorteile der VPC-Freigabe und dessen Funktionsweise eingegangen.

So verwenden Sie Data-Warehouse-Ressourcen von Amazon Redshift in einer freigegebenen VPC

Zunächst gilt es zu verstehen, dass ein Amazon-Redshift-Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe für Teilnehmer in einem freigegebenen Subnetz nicht sichtbar gemacht werden kann. Dies hindert die Teilnehmer jedoch nicht daran, mit der Datenbank des Besitzers in einer freigegebenen VPC zu arbeiten. Dies wird in den folgenden Schritten ausführlicher beschrieben.

Bevor Sie einen bereitgestellten Amazon-Redshift-Cluster in einer freigegebenen VPC erstellen, müssen Sie eine Subnetzgruppe erstellen, die Sie für Amazon Redshift verwenden möchten. Dies sollte die Subnetze der freigegebenen VPC einschließen, die Sie verwenden möchten. Wenn Sie Ihren Amazon-Redshift-Cluster erstellen, müssen Sie dieses Subnetz auswählen und auch die Sicherheitsgruppe der freigegebenen VPC angeben. Ebenso müssen Sie die freigegebenen Subnetze und die Sicherheitsgruppe angeben, die Sie in der freigegebenen VPC erstellt haben, wenn Sie die Amazon-Redshift-Serverless-Arbeitsgruppe und -Datenbank erstellen. Nachdem Sie Ihre Subnetze eingerichtet haben, führen Sie die folgenden Schritte aus, um Redshift-Ressourcen in der freigegebenen Umgebung einzurichten:

1. Der VPC-Besitzer erstellt einen Amazon-Redshift-Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe unter Verwendung eines Subnetzes in der freigegebenen VPC.
2. Der VPC-Besitzer stellt den Cluster oder die Arbeitsgruppe in einem VPC-übergreifenden Szenario zur Verfügung. Die Schritte für einen provisionierten Cluster werden in Arbeiten mit von Redshift verwalteten VPC-Endpunkten in Amazon Redshift und die für Amazon Redshift Serverless werden in Herstellen einer Verbindung mit Amazon Redshift Serverless von einem von Amazon Redshift verwalteten VPC-Endpunkt aus beschrieben. Durch die Aktivierung der VPC-übergreifenden Verfügbarkeit können sie die Datenbank Benutzern in demselben AWS-Konto oder in anderen Konten zur Verfügung stellen.

3. Umgekehrt kann ein Besitzer mithilfe der VPC-Freigabe ein Subnetz mit einem Teilnehmer teilen, und der Teilnehmer kann einen Amazon-Redshift-Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe im Subnetz erstellen. In diesem Fall kann der Besitzer jedoch keine Amazon-Redshift-Ressource anzeigen, die von einem Teilnehmer erstellt wurde. Der Cluster oder die Arbeitsgruppe muss zugänglich gemacht werden, indem die VPC-übergreifende Verfügbarkeit auf dieselbe Weise aktiviert wird, wie im vorherigen Schritt beschrieben.

Nutzungshinweise für die Verwendung von Amazon-Redshift-Ressourcen in einer freigegebenen VPC

Beachten Sie die folgenden Verhaltensweisen bei der Verwendung von Amazon Redshift in einem freigegebenen Subnetz:

- Wie im vorherigen Abschnitt beschrieben, kann der VPC-Besitzer einen Amazon-Redshift-Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe nicht über VPC-Freigabe mit einem Teilnehmer teilen. Der Teilnehmer kann jedoch einen Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe im Subnetz des Besitzers erstellen. In diesem Fall ist Amazon Redshift durch VPC-Freigabe für den Besitzer nicht sichtbar.
- Der VPC-Besitzer kann einen von Amazon Redshift bereitgestellten Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe, die der Teilnehmer im freigegebenen Subnetz erstellt, nicht anzeigen, aktualisieren oder löschen.
- Es sind keine Berechtigungen dafür verfügbar, damit ein anderes AWS-Konto auf Amazon-Redshift-Ressourcen zugreifen kann, die Sie in der freigegebenen VPC erstellen.

Amazon-Redshift-Cluster-Subnetzgruppen

Übersicht

Sie erstellen eine Cluster-Subnetzgruppe, wenn Sie Ihren Cluster in Ihrer Virtual Private Cloud (VPC) bereitstellen. Weitere Informationen zur VPC finden Sie auf der Produktdetailseite für Amazon VPC.

Ihre VPC kann ein oder mehrere Subnetze enthalten, d. h. eine Teilmenge der IP-Adressen in Ihrer VPC, mit deren Hilfe Sie Ihre Ressourcen auf der Grundlage Ihrer Sicherheits- und Betriebsanforderungen gruppieren können. Eine Cluster-Subnetzgruppe ermöglicht Ihnen die Angabe von Subnetzen in Ihrer VPC. Wenn Sie einen Cluster bereitstellen, geben Sie die Subnetzgruppe an und Amazon Redshift erstellt den Cluster in einem der Subnetze in der Gruppe.

Weitere Informationen zum Erstellen einer VPC finden Sie im Amazon-VPC-Benutzerhandbuch.

Nach dem Erstellen einer Subnetzgruppe können Sie zuvor hinzugefügte Subnetze entfernen oder weitere Subnetze hinzufügen. Amazon Redshift stellt API-Vorgänge bereit, mit denen Sie Cluster-Subnetzgruppen erstellen, ändern oder löschen können. Sie können diese Operationen auch in der Konsole durchführen.

Verwalten von Cluster-Subnetzgruppen über die Konsole

Sie können Ihre Cluster-Subnetzgruppen über die Amazon-Redshift-Konsole verwalten. Sie können eine Cluster-Subnetzgruppe erstellen, eine vorhandene Cluster-Subnetzgruppe verwalten oder eine vorhandene Cluster-Subnetzgruppe löschen. All diese Aufgaben beginnen in der Liste der Cluster-Subnetzgruppen. Sie müssen eine Cluster-Subnetzgruppe auswählen, um sie zu verwalten.

Sie können einen Cluster in einem der Subnetze bereitstellen, die Sie in der Subnetzgruppe bereitstellen. Eine Cluster-Subnetzgruppe ermöglicht Ihnen die Angabe einer Reihe von Subnetzen in Ihrer Virtual Private Cloud (VPC).

Erstellen einer Cluster-Subnetzgruppe

Sie müssen mindestens eine Cluster-Subnetzgruppe definieren, um in einer VPC ein Cluster bereitstellen zu können.

So erstellen Sie eine Cluster-Subnetzgruppe

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Configurations (Konfigurationen) und dann Subnet groups (Subnetzgruppen) aus. Die Liste der Subnetzgruppen wird angezeigt.
3. Wählen Sie Create cluster subnet group (Cluster-Subnetzgruppe erstellen) aus, um die Erstellungsseite anzuzeigen.
4. Geben Sie Informationen für die Subnetzgruppe ein, einschließlich der Subnetze, die hinzugefügt werden sollen.
5. Wählen Sie Create cluster subnet group (Cluster-Subnetzgruppe erstellen) aus, um die Gruppe mit den von Ihnen gewählten Subnetzen zu erstellen.

Ändern einer Cluster-Subnetzgruppe

So ändern Sie eine Cluster-Subnetzgruppe

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Configurations (Konfigurationen) und dann Subnet groups (Subnetzgruppen) aus. Die Liste der Subnetzgruppen wird angezeigt.
3. Wählen Sie die zu ändernde Subnetzgruppe aus.
4. Wählen Sie für Actions (Aktionen) Modify (Ändern) aus, um die Details der Subnetzgruppe anzuzeigen.
5. Aktualisieren Sie Informationen für die Subnetzgruppe.
6. Wählen Sie Save (Speichern) aus, um die Gruppe zu ändern.

Wenn Sie Subnetze ändern oder entfernen möchten, sind in einigen Fällen zusätzliche Schritte erforderlich. Zum Beispiel dieser AWS Knowledge Center-Artikel, Wie verschiebe ich meinen bereitgestellten Amazon Redshift Redshift-Cluster in ein anderes Subnetz? , beschreibt einen Anwendungsfall, der das Verschieben eines Clusters behandelt.

Löschen einer Cluster-Subnetzgruppe

Sie können eine Cluster-Subnetzgruppe, die von einem Cluster verwendet wird, nicht löschen.

So löschen Sie eine Cluster-Subnetzgruppe

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Configurations (Konfigurationen) und dann Subnet groups (Subnetzgruppen) aus. Die Liste der Subnetzgruppen wird angezeigt.
3. Wählen Sie die zu löschende Subnetzgruppe und dann Delete (Löschen) aus.

Cluster-Subnetzgruppen mithilfe der AWS CLI und der Amazon Redshift Redshift-API verwalten

Sie können zur Verwaltung von Cluster-Subnetzgruppen die folgenden Amazon-Redshift-CLI-Vorgänge verwenden.

- create-cluster-subnet-group
- delete-cluster-subnet-group
- describe-cluster-subnet-groups
- modify-cluster-subnet-group

Sie können zur Verwaltung von Cluster-Subnetzgruppen die folgenden Amazon-Redshift-API-Vorgänge verwenden.

- CreateClusterSubnetGroup
- DeleteClusterSubnetGroup
- DescribeClusterSubnetGroups
- ModifyClusterSubnetGroup

Cluster-Versionsverlauf

Amazon Redshift veröffentlicht regelmäßig neue Cluster-Versionen, die zum Aktualisieren des Clusters verwendet werden.

> **Important**
>
> Aktuelle Informationen zu den verfügbaren Amazon–Redshift-Cluster-Versionen und deren Funktionen, Verbesserungen und Fehlerbehebungen finden Sie unter Cluster-Versionen für Amazon Redshift.

Arbeiten mit Null-ETL-Integrationen

Dies ist eine Vorabdokumentation für Null-ETL-Integrationen von Aurora PostgreSQL und RDS für MySQL mit Amazon Redshift, die sich in der Vorschauversion befinden. Dokumentation und Features unterliegen Änderungen. Wir empfehlen, Null-ETL-Integrationen von RDS für MySQL und Aurora PostgreSQL nur in Testumgebungen und nicht in Produktionsumgebungen zu verwenden. Weitere Informationen zu den Bedingungen für Vorschauversionen finden Sie unter Betas und Vorversionen in den AWS -Servicebedingungen.

Null-ETL-Integration ist eine vollständig verwaltete Lösung, die Transaktions- oder operative Daten beinahe in Echtzeit in Amazon Redshift verfügbar macht. Mit dieser Lösung können Sie eine Integration aus Ihrer Quelle mit einem Amazon Redshift Data Warehouse konfigurieren. Sie müssen keine Pipeline für Extract, Transform, Load (ETL) verwalten. Wir übernehmen die ETL-Operationen für Sie, indem wir die Erstellung und Verwaltung der Datenreplikation aus der Datenquelle zum Amazon-Redshift-Cluster oder Redshift-Serverless-Namespace automatisieren. Sie können Ihre Quelldaten weiter aktualisieren und abfragen und gleichzeitig Amazon Redshift für Analyse-Workloads wie Berichte und Dashboards verwenden.

Die folgenden Quellen werden derzeit für Null-ETL-Integrationen unterstützt:

- Aurora MySQL-Compatible Edition
- Aurora PostgreSQL-Compatible Edition (Vorschau)
- RDS für MySQL (Vorschau)

Um eine Null-ETL-Integration zu erstellen, geben Sie eine Integrationsquelle und ein Amazon Redshift Data Warehouse als Ziel an. Die Integration repliziert Daten aus der Quelle zum gewünschten Data-Warehouse. Die Daten sind innerhalb von Sekunden in Amazon Redshift verfügbar. Die Integration überwacht den Zustand der Datenpipeline und behebt nach Möglichkeit Probleme. Sie können Integrationen aus Quellen desselben Typs zu einem einzigen Amazon Redshift Data Warehouse erstellen, um ganzheitliche Einblicke über mehrere Anwendungen hinweg zu erhalten.

Mit den Daten in Amazon Redshift können Sie die von Amazon Redshift bereitgestellten Analysen nutzen. Zum Beispiel: integriertes Machine Learning (ML), materialisierte Ansichten, Datenfreigaben und der direkte Zugriff auf mehrere Datenspeicher und Data Lakes Eine Null-ETL-Integration

isoliert die Rechenressourcen von den Datenressourcen, um möglichst effiziente Tools für die Datenverarbeitung zu verwenden. Dateningenieuren bietet die Null-ETL-Integration Zugriff auf zeitkritische Daten, die andernfalls durch zeitweilige Fehler in komplexen Datenpipelines verzögert werden könnten. Sie können analytische Abfragen und ML-Modelle für Transaktionsdaten ausführen, um beinahe in Echtzeit Einblicke in zeitkritische Ereignisse und Geschäftsentscheidungen zu gewinnen.

Sie können Amazon-Redshift-Ereignisbenachrichtigungen abonnieren, um beim Auftreten eines Ereignisses für eine bestimmte Null-ETL-Integration benachrichtigt zu werden. Die Liste der integrationsbezogenen Ereignisbenachrichtigungen finden Sie unter Ereignisbenachrichtigungen zur Null-ETL-Integration mit Amazon EventBridge. Am einfachsten lässt sich ein Abonnement mit der Amazon-SNS-Konsole erstellen. Informationen zum Erstellen und Abonnieren eines Amazon-SNS-Themas finden Sie unter Erste Schritte mit Amazon SNS im Amazon-Simple-Notification-Service-Entwicklerhandbuch.

Wenn Sie mit Null-ETL-Integrationen beginnen, sollten Sie die folgenden Konzepte berücksichtigen:

- Die Quelldatenbank ist die Datenbank, aus der Daten zu Amazon Redshift repliziert werden.
- Das Ziel-Data-Warehouse ist der von Amazon Redshift bereitgestellte Cluster oder die Redshift-Serverless-Arbeitsgruppe, zu dem/der die Daten repliziert werden.
- Die Zieldatenbank ist die Datenbank, die Sie aus einer Null-ETL-Integration im Ziel-Data-Warehouse erstellen.

Sie können Ihre Null-ETL-Integrationen überwachen, indem Sie die folgenden Systemansichten in Amazon Redshift abfragen.

- SVV_INTEGRATION stellt Informationen zu Konfigurationsdetails von Null-ETL-Integrationen bereit.
- SYS_INTEGRATION_ACTIVITY stellt Informationen zu abgeschlossenen Null-ETL-Integrationen bereit.
- SVV_INTEGRATION_TABLE_STATE stellt Informationen zum Integrationsstatus bereit.
- SYS_INTEGRATION_TABLE_STATE_CHANGE stellt Informationen zum Änderungsprotokoll für Tabellenstatus für Integrationen bereit.

Preisinformationen für Null-ETL-Integrationen finden Sie auf der entsprechenden Preisseite:

- Amazon-Redshift-Preise

- Amazon-Aurora-Preise
- Amazon-RDS-Preise

Weitere Informationen zu den Quellen für Null-ETL-Integrationen finden Sie in den folgenden Themen:

- Informationen zu Aurora-Null-ETL-Integrationen finden Sie unter Vorteile, Die wichtigsten Konzepte, Einschränkungen, Kontingente und Unterstützte Regionen für Null-ETL-Integrationen im Amazon-Aurora-Benutzerhandbuch.
- Informationen zu RDS-Null-ETL-Integrationen finden Sie unter Vorteile, Die wichtigsten Konzepte, Einschränkungen, Kontingente und Unterstützte Regionen für Null-ETL-Integrationen im Amazon-RDS-Benutzerhandbuch.

Themen

- Überlegungen bei der Verwendung von Null-ETL-Integrationen mit Amazon Redshift
- Erste Schritte mit Null-ETL-Integrationen
- Erstellen von Zieldatenbanken in Amazon Redshift
- Abfragen und Erstellen von materialisierten Ansichten mit replizierten Daten
- Verwalten von Null-ETL-Integrationen
- Metriken für Null-ETL-Integrationen
- Fehlerbehebung bei Null-ETL-Integrationen

Überlegungen bei der Verwendung von Null-ETL-Integrationen mit Amazon Redshift

Die folgenden Überlegungen gelten für Null-ETL-Integrationen mit Amazon Redshift.

- Ihr Ziel-Data-Warehouse von Amazon Redshift muss die folgenden Voraussetzungen erfüllen:
  - Es muss ein Amazon-Redshift-Serverless- oder RA3-Knotentyp (ra3.16xlarge, ra3.4xlarge und ra3.xlplus) ausgeführt werden.
  - Es muss verschlüsselt sein (bei Verwendung eines bereitgestellten Clusters).
  - Die Unterscheidung zwischen Groß- und Kleinschreibung muss aktiviert sein.

- Sie können die erweiterte VPC-Unterstützung nicht für Data Warehouses mit konfigurierten Integrationen aktivieren.
- Wenn Sie eine autorisierte Integrationsquelle für ein Amazon Redshift Data Warehouse löschen, wechseln alle zugehörigen Integrationen in den Status `FAILED`.
- Sie können Data Warehouses von Amazon Redshift mit vorhandenen Null-ETL-Integrationen nicht löschen. Sie müssen zuerst alle zugehörigen Integrationen löschen.
- Sie müssen zuerst alle mit einer Zieldatenbank verknüpften Integrationen löschen, bevor Sie diese Zieldatenbank löschen können.
- Die Zieldatenbank ist schreibgeschützt. Sie können in der Zieldatenbank keine Tabellen, Ansichten oder materialisierten Ansichten erstellen. Sie können jedoch materialisierte Ansichten für andere Tabellen im Ziel-Data-Warehouse verwenden.
- Materialisierte Ansichten werden in datenbankübergreifenden Abfragen unterstützt. Das Aktualisieren materialisierter Ansichten mit Daten, die aus Null-ETL-Integrationen repliziert wurden, führt zu einer vollständigen Aktualisierung der Ansicht. Die inkrementelle Aktualisierung, die automatische Umschreibung von Abfragen, die automatische Aktualisierung und automatisierte materialisierte Ansichten werden nicht unterstützt. Informationen zum Erstellen von materialisierten Ansichten mit Daten, die über Null-ETL-Integrationen repliziert wurden, finden Sie unter Erstellen von materialisierten Ansichten mit replizierten Daten.
- Sie können im Ziel-Data-Warehouse nur Tabellen mit dem Status `Synced` abfragen. Weitere Informationen finden Sie unter Metriken für Null-ETL-Integrationen.
- Null-ETL-Integrationen werden in Ziel-Data-Warehouses, die für eine Multi-AZ-Bereitstellung konfiguriert sind, nicht unterstützt.
- Die klassische Größenänderung wird für bereitgestellte Cluster mit Null-ETL-Integrationen nicht unterstützt. Diese Operation führt dazu, dass die Integration in den Status `FAILED` wechselt.
- Amazon Redshift akzeptiert nur UTF-8-Zeichen und berücksichtigt daher möglicherweise nicht die in der Quelle definierte Sortierung. Die Sortier- und Vergleichsregeln können unterschiedlich sein, was sich letztendlich auf die Abfrageergebnisse auswirken kann.
- Tabellen in der Integrationsquelle müssen einen Primärschlüssel haben. Andernfalls können Ihre Tabellen nicht in das Ziel-Data Warehouse in Amazon Redshift repliziert werden.
- Für Null-ETL-Integrationen von Aurora PostgreSQL und RDS für MySQL mit Amazon Redshift erstellen Sie Ihr Ziel-Data-Warehouse in Vorschau. Weitere Informationen finden Sie unter Erstellen und Konfigurieren eines Ziel-Data-Warehouse in Amazon Redshift.

Informationen zu Überlegungen, die auch für die Integrationsquelle gelten, finden Sie in den folgenden Themen:

- Informationen zu Aurora-Quellen finden Sie unter Einschränkungen im Amazon-Aurora-Benutzerhandbuch.
- Informationen zu Amazon-RDS-Quellen finden Sie unter Einschränkungen im Amazon-RDS-Benutzerhandbuch.

Erste Schritte mit Null-ETL-Integrationen

Bevor Sie Ihre Null-ETL-Integration für Amazon Redshift konfigurieren, müssen Sie die Integrationsquelle konfigurieren und mit den erforderlichen Parametern und Berechtigungen einrichten. Fahren Sie dann von der Amazon Redshift Redshift-Konsole aus mit der restlichen Ersteinrichtung fort und AWS CLI.

Erstellen einer Aurora-Null-ETL-Integration mit Amazon Redshift

So erstellen Sie eine Aurora-Null-ETL-Integration mit Amazon Redshift:

1. Erstellen Sie in der Amazon-RDS-Konsole eine benutzerdefinierte DB-Cluster-Parametergruppe wie im Amazon-Aurora-Benutzerhandbuch beschrieben.
2. Erstellen Sie in der Amazon-RDS-Konsole einen Amazon-Aurora-DB-Quell-Cluster wie im Amazon-Aurora-Benutzerhandbuch beschrieben.
3. Über die Amazon-Redshift-Konsole: Erstellen und Konfigurieren eines Ziel-Data-Warehouse in Amazon Redshift.
   - Von der AWS CLI oder der Amazon Redshift Redshift-Konsole aus:Aktivieren der Unterscheidung zwischen Groß- und Kleinschreibung für Ihr Data Warehouse.
   - Über die Amazon-Redshift-Konsole: Konfigurieren der Autorisierung für Ihr Amazon Redshift Data Warehouse.
4. Erstellen Sie in der Amazon-RDS-Konsole eine Null-ETL-Integration wie im Amazon-Aurora-Benutzerhandbuch beschrieben.
5. Erstellen Sie in der Amazon-Redshift-Konsole oder im Query Editor v2 eine Amazon-Redshift-Datenbank aus der Integration.

   Anschließend müssen Sie materialisierte Ansichten mit replizierten Daten abfragen und erstellen.

Erstellen einer RDS-Null-ETL-Integration mit Amazon Redshift

So erstellen Sie eine RDS-Null-ETL-Integration mit Amazon Redshift:

1. Erstellen Sie in der Amazon-RDS-Konsole eine benutzerdefinierte DB-Cluster-Parametergruppe wie im Amazon-RDS-Benutzerhandbuch beschrieben.
2. Erstellen Sie in der Amazon-RDS-Konsole eine Amazon-RDS-Quell-Instance wie im Amazon-RDS-Benutzerhandbuch beschrieben.
3. Über die Amazon-Redshift-Konsole: Erstellen und Konfigurieren eines Ziel-Data-Warehouse in Amazon Redshift.
   - Von der AWS CLI oder der Amazon Redshift Redshift-Konsole aus:Aktivieren der Unterscheidung zwischen Groß- und Kleinschreibung für Ihr Data Warehouse.
   - Über die Amazon-Redshift-Konsole: Konfigurieren der Autorisierung für Ihr Amazon Redshift Data Warehouse.
4. Erstellen Sie in der Amazon-RDS-Konsole eine Null-ETL-Integration, wie im Amazon-RDS-Benutzerhandbuch beschrieben.
5. Erstellen Sie in der Amazon-Redshift-Konsole oder im Query Editor v2 eine Amazon-Redshift-Datenbank aus der Integration.

   Anschließend müssen Sie materialisierte Ansichten mit replizierten Daten abfragen und erstellen.

Die Amazon RDS-Konsole bietet einen Ablauf zur step-by-step Integrationserstellung, in dem Sie die Quelldatenbank und das Amazon Redshift Redshift-Ziel-Data Warehouse angeben. Auftretende Probleme können Sie von Amazon RDS beheben lassen, anstatt sie manuell in der Amazon-RDS- oder der Amazon-Redshift-Konsole zu beheben.

Erstellen und Konfigurieren eines Ziel-Data-Warehouse in Amazon Redshift

Erstellen Sie vor diesem Schritt Ihre Integrationsquelle und konfigurieren Sie die für den Quelltyp erforderlichen Parameter für Null-ETL-Integrationen.

In diesem Schritt erstellen und konfigurieren Sie ein Ziel-Data-Warehouse in Amazon Redshift, z. B. eine Redshift-Serverless-Arbeitsgruppe oder einen bereitgestellten Cluster.

Ihr Ziel-Data Warehouse muss die folgenden Eigenschaften aufweisen:

- Es muss Amazon Redshift Serverless oder einen bereitgestellten Cluster vom Instance-Typ ra3.16xlarge, ra3.4xlarge oder ra3.xlplus ausführen.

- Die Unterscheidung zwischen Groß- und Kleinschreibung (`enable_case_sensitive_identifier`) muss aktiviert sein. Weitere Informationen finden Sie unter Aktivieren der Unterscheidung zwischen Groß- und Kleinschreibung für Ihr Data Warehouse.
- Wenn Ihr Ziel-Data-Warehouse ein in Amazon Redshift bereitgestellter Cluster ist, muss es verschlüsselt sein. Weitere Informationen finden Sie unter Verschlüsselung von Amazon-Redshift-Datenbanken.
- In derselben AWS Region wie die Integrationsquelle erstellt.

> **Note**
>
> Beachten Sie für Null-ETL-Integrationen von Aurora PostgreSQL und RDS für MySQL mit Amazon Redshift zudem Folgendes für Ihr Ziel-Data-Warehouse:
>
> - Sie müssen Ihr Data Warehouse in der Vorschau auf Track `preview_2023` erstellen. Sie können keine Vorschau-Features in der Produktion verwenden und Ihr Vorschau-Data-Warehouse auch nicht in eine Produktionsbereitstellung verschieben.
> - Wenn Sie einen von Amazon Redshift bereitgestellten Cluster erstellen, muss dieser Cluster mindestens zwei Knoten umfassen.
> - Für Aurora PostgreSQL-Quellen müssen Sie Ihr Ziel-Data Warehouse in der Region USA Ost (Ohio) AWS erstellen. Beachten Sie, dass Sie Ihre Quelldatenbank für Null-ETL-Integrationen von Aurora PostgreSQL in der Datenbank-Vorschauumgebung in Amazon RDS erstellen müssen.
>
>   Für RDS for MySQL-Quellen müssen Sie Ihr Ziel-Data Warehouse in einer unterstützten AWS Region erstellen. Eine Liste der AWS -Regionen, in denen Null-ETL-Integrationen von RDS für MySQL verfügbar sind, finden Sie unter Unterstützte Regionen für Null-ETL-Integrationen mit Amazon Redshift im Amazon-RDS-Benutzerhandbuch.
>
> Informationen zum Erstellen Ihres Ziel-Data-Warehouse in der Vorschau für Ihre Null-ETL-Integrationen von Aurora PostgreSQL und RDS für MySQL finden Sie je nach Bereitstellungstyp in einem der folgenden Themen:
>
> - Informationen zum Erstellen eines von Amazon Redshift bereitgestellten Vorschau-Clusters finden Sie unter Erstellen eines Vorschau-Clusters. Stellen Sie sicher, dass Sie den Track `preview_2023` auswählen, um Null-ETL-Integrationen verwenden zu können.

- Informationen zum Erstellen einer Amazon-Redshift-Serverless-Vorschau-Arbeitsgruppe finden Sie unter Erstellen einer Vorschau-Arbeitsgruppe.

Informationen zum Erstellen Ihres Ziel-Data-Warehouse für Ihre Null-ETL-Integrationen von Aurora MySQL finden Sie je nach Bereitstellungstyp in einem der folgenden Themen:

- Informationen zum Erstellen eines von Amazon Redshift bereitgestellten Clusters finden Sie unter Erstellen eines Clusters.
- Informationen zum Erstellen einer Amazon-Redshift-Serverless-Arbeitsgruppe mit einem Namespace finden Sie unter Erstellen einer Arbeitsgruppe mit einem Namespace.

Wenn Sie einen bereitgestellten Cluster erstellen, erstellt Amazon Redshift auch eine Standardparametergruppe. Die Standard-Parametergruppe kann nicht bearbeitet werden. Sie können jedoch vor Erstellung eines neuen Clusters eine benutzerdefinierte Parametergruppe erstellen und diese dann dem Cluster zuordnen. Sie können auch die Parametergruppe bearbeiten, die dem erstellten Cluster zugeordnet wird. Wenn Sie die benutzerdefinierte Parametergruppe erstellen oder eine aktuelle Parametergruppe bearbeiten, müssen Sie für die Parametergruppe auch die Unterscheidung zwischen Groß- und Kleinschreibung aktivieren, um Null-ETL-Integrationen verwenden zu können.

Sie können eine benutzerdefinierte Parametergruppe entweder mit der Amazon Redshift Redshift-Konsole oder AWS CLI wie folgt erstellen:

- Über die Amazon-Redshift-Konsole – Verwaltung von Parametergruppen mit der Konsole
- Mit dem AWS CLI — Verwalten von Parametergruppen mit der AWS CLI und der Amazon Redshift API

Aktivieren der Unterscheidung zwischen Groß- und Kleinschreibung für Ihr Data Warehouse

Sie können eine Parametergruppe anfügen und die Berücksichtigung von Groß- und Kleinschreibung für einen bereitgestellten Cluster bei der Erstellung aktivieren. Sie können eine Serverless-Arbeitsgruppe jedoch erst über die AWS Command Line Interface (AWS CLI) aktualisieren, nachdem sie erstellt wurde. Dies ist notwendig, damit die Unterscheidung zwischen Groß- und Kleinschreibung für MySQL und PostgreSQL unterstützt wird. `enable_case_sensitive_identifier` ist

ein Konfigurationswert, der bestimmt, ob Namensbezeichner von Datenbanken, Tabellen und Spalten die Groß- und Kleinschreibung beachten. Dieser Parameter muss aktiviert sein, um Null-ETL-Integrationen im Data Warehouse zu erstellen. Weitere Informationen finden Sie unter enable_case_sensitive_identifier.

Bei Amazon Redshift Serverless – Aktivieren Sie die Berücksichtigung von Groß- und Kleinschreibung für Amazon Redshift Serverless mithilfe der AWS CLI. Beachten Sie, dass Sie die Unterscheidung zwischen Groß- und Kleinschreibung für Amazon Redshift Serverless nur über die AWS CLI aktivieren können.

Beachten Sie bei von Amazon Redshift bereitgestellten Clustern die Informationen in folgenden Themen, um die Groß- und Kleinschreibung für Ihren Ziel-Cluster zu aktivieren:

- Aktivieren der Unterscheidung zwischen Groß- und Kleinschreibung für in Amazon Redshift bereitgestellte Cluster über die Amazon-Redshift-Konsole
- Aktivieren Sie die Berücksichtigung von Groß- und Kleinschreibung für von Amazon Redshift bereitgestellte Cluster mithilfe der AWS CLI

Aktivieren Sie die Berücksichtigung von Groß- und Kleinschreibung für Amazon Redshift Serverless mithilfe der AWS CLI

Führen Sie den folgenden AWS CLI Befehl aus, um die Groß- und Kleinschreibung für Ihre Arbeitsgruppe zu aktivieren.

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

Warten Sie, bis der Status der Arbeitsgruppe `Active` lautet, bevor Sie mit dem nächsten Schritt fortfahren.

Aktivieren der Unterscheidung zwischen Groß- und Kleinschreibung für in Amazon Redshift bereitgestellte Cluster über die Amazon-Redshift-Konsole

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im linken Navigationsbereich die Option Dashboard für bereitgestellte Cluster aus.

3. Wählen Sie den bereitgestellten Cluster aus, in den Sie Daten replizieren möchten.
4. Wählen Sie im linken Navigationsbereich Konfigurationen > Workload-Management aus.
5. Wählen Sie auf der Seite „Workload-Management“ die Parametergruppe aus.
6. Wählen Sie die Registerkarte Parameters aus.
7. Wählen Sie Parameter bearbeiten aus und ändern Sie dann enable_case_sensitive_identifier in true.
8. Wählen Sie dann Save (Speichern) aus.

Aktivieren Sie die Berücksichtigung von Groß- und Kleinschreibung für von Amazon Redshift bereitgestellte Cluster mithilfe der AWS CLI

1. Da Sie die Standardparametergruppe nicht bearbeiten können, führen Sie in Ihrem Terminalprogramm den folgenden AWS CLI Befehl aus, um eine benutzerdefinierte Parametergruppe zu erstellen. Später werden Sie diese dem bereitgestellten Cluster zuordnen.

```
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. Führen Sie den folgenden AWS CLI Befehl aus, um die Berücksichtigung von Groß- und Kleinschreibung für die Parametergruppe zu aktivieren.

```
aws redshift modify-cluster-parameter-group \
    --parameter-group-name zero-etl-params \
    --parameters ParameterName=enable_case_sensitive_identifier,ParameterValue=true
```

3. Führen Sie den folgenden Befehl aus, um die Parametergruppe dem Cluster zuzuordnen.

```
aws redshift modify-cluster \
    --cluster-identifier target-cluster \
    --cluster-parameter-group-name zero-etl-params
```

4. Warten Sie, bis der bereitgestellte Cluster verfügbar ist. Sie können den Status des Clusters mithilfe des Befehls `describe-cluster` überprüfen. Führen Sie anschließend den folgenden Befehl aus, um den Cluster zu erstellen.

```
aws redshift reboot-cluster \
```

```
    --cluster-identifier target-cluster
```

Konfigurieren der Autorisierung für Ihr Amazon Redshift Data Warehouse

Um Daten aus Ihrer Integrationsquelle in Ihr Amazon Redshift Data Warehouse zu replizieren, müssen Sie zunächst die folgenden zwei Entitäten hinzufügen:

- Autorisierter Prinzipal: Identifiziert den Benutzer oder die Rolle, der/die Null-ETL-Integrationen für das Data Warehouse erstellen kann.
- Autorisierte Integrationsquelle: Identifiziert die Quelldatenbank, die das Data Warehouse aktualisieren kann.

Sie können autorisierte Prinzipale und autorisierte Integrationsquellen auf der Registerkarte Ressourcenrichtlinie in der Amazon-Redshift-Konsole oder unter Verwendung der Amazon-Redshift-API-Operation `PutResourcePolicy` konfigurieren.

Autorisierte Prinzipale hinzufügen

Um eine Null-ETL-Integration für Ihre Redshift Serverless Workgroup oder Ihren bereitgestellten Cluster zu erstellen, autorisieren Sie den Zugriff auf den zugehörigen Namespace oder den bereitgestellten Cluster.

Sie können diesen Schritt überspringen, wenn die beiden folgenden Bedingungen zutreffen:

- Derjenige AWS-Konto , der die Redshift Serverless Workgroup oder den bereitgestellten Cluster besitzt, besitzt auch die Quelldatenbank.
- Dieser Prinzipal ist mit einer identitätsbasierten IAM-Richtlinie verknüpft, die berechtigt ist, Null-ETL-Integrationen für diesen Redshift Serverless-Namespace oder bereitgestellten Cluster zu erstellen.

Autorisierte Prinzipale zu einem Amazon Redshift Serverless-Namespace hinzufügen

1. Wählen Sie in der Amazon-Redshift-Konsole im linken Navigationsbereich Redshift Serverless aus.
2. Wählen Sie Namespace-Konfiguration und dann Ihren Namespace aus und wechseln Sie zur Registerkarte Ressourcenrichtlinie.

3. Wählen Sie Add authorized principals aus.
4. Geben Sie für jeden autorisierten Prinzipal, den Sie hinzufügen möchten, entweder den ARN des Benutzers oder der Rolle oder die ID des AWS Benutzers oder der Rolle in den Namespace ein, dem Sie Zugriff gewähren möchten AWS-Konto , um Zero-ETL-Integrationen zu erstellen. Eine Konto-ID wird als ARN gespeichert.
5. Wählen Sie Änderungen speichern aus.

Autorisierte Prinzipale zu einem in Amazon Redshift bereitgestellten Cluster hinzufügen

1. Wählen Sie in der Amazon-Redshift-Konsole im linken Navigationsbereich Dashboard für bereitgestellte Cluster aus.
2. Wählen Sie Cluster und dann den gewünschten Cluster aus und wechseln Sie zur Registerkarte Ressourcenrichtlinie.
3. Wählen Sie Add authorized principals aus.
4. Geben Sie für jeden autorisierten Prinzipal, den Sie hinzufügen möchten, entweder den ARN des AWS Benutzers oder der Rolle in den Cluster ein, oder die ID desjenigen, dem Sie Zugriff gewähren möchten AWS-Konto , um Zero-ETL-Integrationen zu erstellen. Eine Konto-ID wird als ARN gespeichert.
5. Wählen Sie Änderungen speichern aus.

Autorisierte Integrationsquellen hinzufügen

Damit Ihre Quelle Ihr Amazon Redshift Data Warehouse aktualisieren kann, müssen Sie sie als autorisierte Integrationsquelle zum Namespace hinzufügen.

Eine autorisierte Integrationsquelle zu einem Amazon Redshift Serverless-Namespace hinzufügen

1. Gehen Sie in der Amazon-Redshift-Konsole zum Serverless-Dashboard.
2. Wählen Sie den Namen des Namespace aus.
3. Wechseln Sie zur Registerkarte Ressourcenrichtlinie.
4. Wählen Sie Add authorized integration source aus.
5. Geben Sie den ARN der Quelle für die Null-ETL-Integration an.

> **Note**
>
> Wenn eine autorisierte Integrationsquelle entfernt wird, werden keine Daten mehr in den Namespace repliziert. Diese Aktion deaktiviert alle Null-ETL-Integrationen aus dieser Quelle in diesen Namespace.

Eine autorisierte Integrationsquelle zu einem in Amazon Redshift bereitgestellten Cluster hinzufügen

1. Gehen Sie in der Amazon-Redshift-Konsole zu Provisioned clusters dashboard.
2. Wählen Sie den Namen des bereitgestellten Clusters aus.
3. Wechseln Sie zur Registerkarte Ressourcenrichtlinie.
4. Wählen Sie Add authorized integration source aus.
5. Geben Sie den ARN der Quelle an, die die Datenquelle für die Null-ETL-Integration bildet.

> **Note**
>
> Wenn eine autorisierte Integrationsquelle entfernt wird, werden keine Daten mehr in den bereitgestellten Cluster repliziert. Diese Aktion deaktiviert alle Null-ETL-Integrationen aus dieser Quelle in diesen in Amazon Redshift bereitgestellten Cluster.

Konfigurieren einer Autorisierung unter Verwendung der Amazon-Redshift-API

Sie können mithilfe von Amazon-Redshift-API-Operationen Ressourcenrichtlinien konfigurieren, die mit Null-ETL-Integrationen verwendet werden können.

Erstellen Sie zum Steuern der Quelle, die eine eingehende Integration in den Namespace erstellen kann, eine Ressourcenrichtlinie und fügen Sie diese an den Namespace an. Mit der Ressourcenrichtlinie können Sie die Quelle angeben, die Zugriff auf die Integration hat. Die Ressourcenrichtlinie ist an den Namespace Ihres Ziel-Data-Warehouse angefügt, damit die Quelle eine eingehende Integration erstellen kann, um Live-Daten aus der Quelle in Amazon Redshift zu replizieren.

Im Folgenden finden Sie ein Beispiel für eine Ressourcenrichtlinie.

```
{
```

```
  "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"
    }
  ]
}
```

Im Folgenden sind die anwendbaren Amazon-Redshift-API-Operationen für die Konfiguration von Ressourcenrichtlinien für Integrationen zusammengefasst:

- Verwenden Sie den PutResourcePolicyAPI-Vorgang, um die Ressourcenrichtlinie beizubehalten. Wenn Sie eine andere Ressourcenrichtlinie angeben, wird die vorherige Ressourcenrichtlinie für die Ressource ersetzt. Verwenden Sie die Ressourcenrichtlinie aus dem vorherigen Beispiel, die Berechtigungen für folgenden Aktionen gewährt:
  - `CreateInboundIntegration`: Ermöglicht es dem Quellprinzipal, eine eingehende Integration für Daten zu erstellen, die von der Quelle in das Ziel-Data-Warehouse repliziert werden sollen.
  - `AuthorizeInboundIntegration`: Ermöglicht es Amazon Redshift, kontinuierlich zu überprüfen, ob das Ziel-Data-Warehouse vom Quell-ARN replizierte Daten empfangen kann.
- Verwenden Sie den GetResourcePolicyAPI-Vorgang, um vorhandene Ressourcenrichtlinien anzuzeigen.
- Verwenden Sie den DeleteResourcePolicyAPI-Vorgang, um eine Ressourcenrichtlinie aus der Ressource zu entfernen.

Um eine Ressourcenrichtlinie zu aktualisieren, können Sie auch den put-resource-policy AWS CLI Befehl verwenden.

Nächste Schritte

Da Sie nun die Autorisierung für Ihr Amazon-Redshift-Ziel-Data Warehouse konfiguriert haben, können Sie eine Null-ETL-Integration erstellen und mit der Datenreplikation beginnen.

Führen Sie je nach Quelle einen der folgenden Schritte durch:

- Beachten Sie zum Erstellen von Aurora-Null-ETL-Integrationen die Informationen unter Erstellen von Null-ETL-Integrationen von Aurora mit Amazon Redshift im Amazon-Aurora-Benutzerhandbuch.
- Beachten Sie zum Erstellen von RDS-Null-ETL-Integrationen die Informationen unter Erstellen von Null-ETL-Integrationen von Amazon RDS mit Amazon Redshift im Amazon-RDS-Benutzerhandbuch.

Erstellen von Zieldatenbanken in Amazon Redshift

Zum Replizieren von Daten aus Ihrer Quelle in Amazon Redshift müssen Sie eine Datenbank aus Ihrer Integration in Amazon Redshift erstellen.

Stellen Sie eine Verbindung zu Ihrer Redshift-Serverless-Zielarbeitsgruppe oder Ihrem bereitgestellten Ziel-Cluster her und erstellen Sie eine Datenbank mit einem Verweis auf Ihre Integrations-ID. Diese ID ist der Wert, der für `integration_id` zurückgegeben wird, wenn Sie die Ansicht SVV_INTEGRATION abfragen.

> **Important**
>
> Bevor Sie eine Datenbank aus Ihrer Integration erstellen, muss Ihre Null-ETL-Integration erstellt sein und sich in der Amazon-RDS- oder Amazon-Redshift-Konsole im Status `Active` befinden.

Erstellen einer Zieldatenbank in Amazon Redshift

Bevor Sie mit dem Replizieren von Daten aus Ihrer Quelle in Amazon Redshift beginnen können, erstellen Sie eine Datenbank aus der Integration in Amazon Redshift. Sie können die Datenbank entweder über die Amazon-Redshift-Konsole oder mit Query Editor v2 erstellen.

Erstellen einer Zieldatenbank über die Amazon-Redshift-Konsole

1. Wählen Sie im linken Navigationsbereich Zero-ETL-Integrationen aus.
2. Wählen Sie aus der Integrationsliste eine Integration aus.
3. Wenn Sie einen bereitgestellten Cluster verwenden, müssen Sie zuerst eine Verbindung zur Datenbank herstellen. Wählen Sie Connect to database (Verbindung zur Datenbank herstellen). Sie können dazu eine bestehende Verbindung nutzen oder eine neue erstellen.
4. Um eine Datenbank aus der Integration heraus zu erstellen, wählen Sie Create database from integration aus.
5. Geben Sie einen Database name (Datenbanknamen) ein. Die Integrations-ID und der Data Warehouse-Name sind bereits ausgefüllt.

   Geben Sie für Aurora-PostgreSQL-Quellen auch die benannte Datenbank ein, die Sie beim Erstellen Ihrer Null-ETL-Integration angegeben haben.
6. Wählen Sie Datenbank erstellen aus.

Erstellen einer Zieldatenbank mit Query Editor v2

1. Navigieren Sie zur Amazon-Redshift-Konsole und wählen Sie die Option Query Editor v2 aus.
2. Wählen Sie im linken Bereich Ihre Amazon-Redshift-Serverless-Arbeitsgruppe oder Ihren von Amazon Redshift bereitgestellten Cluster aus und stellen Sie eine Verbindung her.
3. Um die Integrations-ID abzurufen, navigieren Sie zur Integrationsliste auf der Amazon-Redshift-Konsole.

   Führen Sie alternativ den folgenden Befehl aus, um den Wert für `integration_id` abzurufen:

   ```
   SELECT integration_id FROM SVV_INTEGRATION;
   ```
4. Führen Sie dann den folgenden Befehl aus, um die Datenbank zu erstellen. Durch die Angabe der Integrations-ID stellen Sie eine Verbindung zwischen der Datenbank und Ihrer Quelle her.

Ersetzen Sie `integration_id` durch den vom vorherigen Befehl zurückgegebenen Wert.

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

Für Aurora-PostgreSQL-Quellen müssen Sie auch einen Verweis auf die benannte Datenbank innerhalb des Clusters hinzufügen, die Sie beim Erstellen der Integration angegeben haben. Beispielsweise:

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

> **Note**
>
> Daten in der Datenbank, die Sie anhand Ihrer Integration erstellen, können nur von Ihrer Integrationsquelle aktualisiert werden. Um das Schema einer Tabelle zu ändern, führen Sie DDL- oder DML-Befehle für Tabellen in der Quelle aus. Sie können DDL- und DML-Befehle für Tabellen in der Quelle ausführen, in der Zieldatenbank können Sie jedoch nur DDL-Befehle und schreibgeschützte Abfragen ausführen.

Weitere Informationen zum Anzeigen des Status einer Zieldatenbank finden Sie unterVerwalten von Null-ETL-Integrationen.

Hinzufügen von Daten zu Ihrer Quelle

Nachdem Sie eine Zieldatenbank erstellt haben, können Sie Daten zu Ihrer Quelle hinzufügen. Informationen zum Hinzufügen von Daten zu Ihrer Quelle finden Sie in den folgenden Themen:

- Für Aurora-Quellen beachten Sie die Informationen unter Hinzufügen von Daten zum Quell-DB-Cluster im Amazon-Aurora-Benutzerhandbuch.
- Für Amazon-RDS-Quellen beachten Sie die Informationen unter Hinzufügen von Daten zur Quell-DB-Instance im Amazon-RDS-Benutzerhandbuch.

Abfragen und Erstellen von materialisierten Ansichten mit replizierten Daten

Abfragen von replizierten Daten in Amazon Redshift

Nachdem Sie Ihrer Quelle Daten hinzugefügt haben, werden diese nahezu in Echtzeit in das Amazon Redshift Data Warehouse repliziert und können nun abgefragt werden. Hinweise zu Integrationsmetriken und Tabellenstatistiken finden Sie unter Metriken für Null-ETL-Integrationen.

> **Note**
>
> Da eine Datenbank wie ein Schema in MySQL ist, wird die MySQL-Datenbankebene der Amazon-Redshift-Schemaebene zugeordnet. Beachten Sie diesen Unterschied bei der Zuordnung, wenn Sie Daten abfragen, die aus Aurora MySQL oder RDS für MySQL repliziert wurden.

So fragen Sie die replizierten Daten ab

1. Navigieren Sie zur Amazon-Redshift-Konsole und wählen Sie die Option Query Editor v2 aus.
2. Stellen Sie eine Verbindung zu Ihrer Amazon-Redshift-Serverless-Arbeitsgruppe oder Ihrem von Amazon Redshift bereitgestellten Cluster her und wählen Sie Ihre Datenbank aus der Dropdown-Liste aus.
3. Verwenden Sie eine SELECT-Anweisung, um alle replizierten Daten aus dem Schema und der Tabelle auszuwählen, die Sie in der Quelle erstellt haben. Um zwischen Groß- und Kleinschreibung zu unterscheiden, verwenden Sie doppelte Anführungszeichen (" ") für Schema-, Tabellen- und Spaltennamen. Beispielsweise:

   ```
   SELECT * FROM "schema_name"."table_name";
   ```

   Sie können die Daten auch mithilfe der Amazon-Redshift-CLI abfragen.

Erstellen von materialisierten Ansichten mit replizierten Daten

Sie können materialisierte Ansichten in Ihrer lokalen Amazon-Redshift-Datenbank erstellen, um Daten zu transformieren, die über Null-ETL-Integrationen repliziert wurden. Stellen Sie eine

Verbindung zu Ihrer lokalen Datenbank her und verwenden Sie datenbankübergreifende Abfragen, um auf die Zieldatenbanken zuzugreifen. Sie können entweder vollqualifizierte Objektnamen mit der dreiteiligen Notation (destination-database-name.schema-name.table-name) verwenden oder ein externes Schema erstellen, das auf das Zieldatenbank-Schemapaar verweist, und die zweiteilige Notation (.table-name) verwenden. external-schema-name Weitere Informationen zu datenbankübergreifenden Abfragen finden Sie unter Datenbankübergreifendes Abfragen von Daten.

Verwenden Sie das folgende Beispiel, um Beispieldaten zu erstellen und aus der Quelle *tickit_zetl* in die Tabellen *sales_zetl* und *event_zetl* einzufügen. Die Tabellen werden in die Amazon-Redshift-Datenbank *zetl_int_db* repliziert.

```
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");
```

Sie können eine materialisierte Ansicht mithilfe der dreiteiligen Notation erstellen, um den Gesamtumsatz pro Veranstaltung zu ermitteln:

```
--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.tickit_zetl.sales_zetl S, zetl_int_db.tickit_zetl.event_zetl E
WHERE S.eventid = E.eventid
GROUP BY 1);
```

Sie können eine materialisierte Ansicht mithilfe der zweiteiligen Notation erstellen, um den Gesamtumsatz pro Veranstaltung zu ermitteln:

```
--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
);
```

Verwenden Sie das folgende Beispiel, um die von Ihnen erstellten materialisierten Ansichten anzuzeigen.

```
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        |
+-----------+-------------+
```

Verwalten von Null-ETL-Integrationen

Sie können die Details einer Null-ETL-Integration anzeigen, um ihre Konfigurationsinformationen und ihren Status in der Amazon-Redshift-Konsole anzusehen.

So zeigen Sie die Details einer Null-ETL-Integration an

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im linken Navigationsbereich entweder das Serverless- oder das Provisioned clusters-Dashboard aus. Wählen Sie dann Zero-ETL integrations aus.
3. Wählen Sie die Null-ETL-Integration aus, die Sie anzeigen möchten. Für jede Integration werden die folgenden Informationen angegeben:

   - Die Integrations-ID ist der Bezeichner, der beim Erstellen der Integration zurückgegeben wird.
   - Der Status kann wie folgt lauten:
     - `Active`— Die Zero-ETL-Integration sendet Transaktionsdaten an das Amazon Redshift Redshift-Ziel-Data Warehouse.
     - `Syncing`— Bei der Zero-ETL-Integration ist ein behebbarer Fehler aufgetreten und die Daten werden erneut eingespeist. Betroffene Tabellen sind erst für Abfragen in Amazon Redshift verfügbar, wenn die Neusynchronisierung abgeschlossen ist.
     - `Failed`— Bei der Zero-ETL-Integration ist ein nicht behebbares Ereignis oder ein Fehler aufgetreten, der nicht behoben werden kann. Sie müssen die Zero-ETL-Integration löschen und neu erstellen.
     - `Creating`— Die Zero-ETL-Integration wird erstellt.
     - `Deleting`— Die Zero-ETL-Integration wird gelöscht.
     - `Needs attention`— Bei der Zero-ETL-Integration ist ein Ereignis oder ein Fehler aufgetreten, für dessen Behebung ein manuelles Eingreifen erforderlich ist. Befolgen Sie die Anweisungen in der Fehlermeldung, um das Problem zu beheben.
   - Quell-ARN ist der ARN der Quelldaten.
   - Ziel ist der ARN des Ziel-Data-Warehouse-Namespace.
   - Für Datenbank sind folgende Angaben möglich:
     - `No database` – Es gibt keine Zieldatenbank für die Integration.
     - `Creating` – Amazon Redshift erstellt gerade die Zieldatenbank für die Integration.
     - `Active` – Daten werden derzeit aus der Integrationsquelle auf Amazon Redshift repliziert.
     - `Error` – Bei der Integration ist ein Fehler aufgetreten.
     - `Recovering` – Die Integration wird wiederhergestellt, nachdem das Data Warehouse neu gestartet wurde.

  - `Resyncing` – Amazon Redshift synchronisiert die Tabellen in der Integration neu.
- Zieltyp ist der Typ des Amazon Redshift Data Warehouse.
- Erstellungsdatum ist das Datum und die Uhrzeit (UTC) der Erstellung der Integration.

> **Note**
>
> Um Integrationsdetails für ein Data Warehouse anzuzeigen, wählen Sie die Detailseite für Ihren bereitgestellten Cluster oder Serverless-Namespace und dann die Registerkarte Null-ETL-Integrationen aus.

In der Liste Null-ETL-Integrationen können Sie Abfragen von Daten auswählen, um zu Amazon Redshift Query Editor v2 zu wechseln. In der Amazon-Redshift-Zieldatenbank ist der Parameter enable_case_sensitive_identifier aktiviert. Beim Schreiben von SQL müssen Sie Schemas, Tabellen und Spaltennamen möglicherweise in doppelte Anführungszeichen setzen ("<Name>"). Weitere Informationen zum Abfragen von Daten in Ihrem Amazon Redshift Data Warehouse finden Sie unter Abfragen für Datenbanken mit dem Amazon-Redshift-Abfrage-Editor v2.

In der Liste Null-ETL-Integrationen können Sie Daten teilen auswählen, um ein Datashare zu erstellen. Um ein Datashare für die Amazon-Redshift-Datenbank zu erstellen, folgen Sie den Anweisungen auf der Seite Datenfreigabe erstellen. Bevor Sie Daten in Ihrer Amazon-Redshift-Datenbank freigeben können, müssen Sie eine Zieldatenbank erstellen. Weitere Informationen zur Datenfreigabe finden Sie unter Konzepte für Datenfreigabe mit Amazon Redshift.

Zum Aktualisieren Ihrer Integration können Sie den Befehl ALTER DATABASE verwenden. Dadurch werden alle Daten aus Ihrer Integrationsquelle in Ihre Zieldatenbank repliziert. Im folgenden Beispiel werden alle synchronisierten und fehlgeschlagenen Tabellen in Ihrer Null-ETL-Integration aktualisiert.

```
ALTER DATABASE sample_integration_db INTEGRATION REFRESH ALL tables;
```

Freigeben Ihrer Daten in Amazon Redshift

Nachdem Sie Daten zur Quelle hinzugefügt haben, werden diese sofort in Amazon Redshift repliziert und können durch die Erstellung von Datashares gemeinsam genutzt werden.

Um Daten freigeben zu können, müssen Sie zunächst eine Zieldatenbank erstellen.

Important

Um Daten aus einem Amazon-Redshift-Vorschau-Data-Warehouse für ein Konsumenten-Data-Warehouse von Amazon Redshift freizugeben, muss sich Ihr Konsumenten-Data-Warehouse auf Track `preview_2023` befinden. Weitere Informationen über Datashares finden Sie unter Was ist ein Datashare? im Datenbankentwicklerhandbuch zu Amazon Redshift.
Informationen zum Erstellen eines Ziel-Data Warehouse in der Vorschauversion finden Sie je nach Bereitstellungstyp in einem der folgenden Themen:

- Von Amazon Redshift bereitgestellter Cluster – Erstellen eines Vorschau-Clusters
- Redshift-Serverless-Arbeitsgruppe – Erstellen einer Vorschau-Arbeitsgruppe

Freigeben von Daten in Amazon Redshift Serverless über die Amazon-Redshift-Konsole

1. Wählen Sie im linken Navigationsbereich der Amazon-Redshift-Konsole Amazon Redshift Serverless > Serverless-Dashboard aus.
2. Wählen Sie im linken Navigationsbereich Null-ETL-Integrationen aus.
3. Wählen Sie Share data (Daten freigeben).
4. Folgen Sie auf der Seite zum Erstellen von Datashares den Schritten unter Erstellen von Datashares.

Freigeben von Daten in von Amazon Redshift bereitgestellten Clustern über die Amazon-Redshift-Konsole

1. Wählen Sie in der Amazon-Redshift-Konsole im linken Navigationsbereich Dashboard für bereitgestellte Cluster aus.
2. Wählen Sie im linken Navigationsbereich Null-ETL-Integrationen aus.
3. Wählen Sie aus der Integrationsliste eine Integration aus.
4. Wählen Sie auf der Seite mit den Integrationsdetails die Option Verbindung zur Datenbank herstellen aus.

5. Auf der Seite für die Verbindung zur Datenbank können Sie entweder eine neue Verbindung erstellen oder eine kürzlich verwendete Verbindung nutzen. Stellen Sie sicher, dass die Verbindung zur Zieldatenbank hergestellt wird.
6. Wenn Sie eine neue Verbindung erstellen, geben Sie im Feld Database name einen Namen für die Datenbank ein. Klicken Sie dann auf Connect.
7. Wählen Sie auf der Seite mit den Integrationsdetails die Option Daten teilen aus.
8. Folgen Sie auf der Seite zum Erstellen von Datashares den Schritten unter Erstellen von Datashares.

Metriken für Null-ETL-Integrationen

Sie können die Metriken in der Amazon Redshift Redshift-Konsole und in Amazon verwenden CloudWatch , um mehr über den Zustand und die Leistung Ihrer Zero-ETL-Integrationen zu erfahren. Sie können die Metriken anpassen, um Daten für kürzere oder längere Dauer anzuzeigen, oder wählen, ob Metriken in angezeigt werden sollen. CloudWatch Um die Metriken für Ihre Integration in der Amazon-Redshift-Konsole anzuzeigen, wählen Sie Null-ETL-Integrationen im linken Navigationsbereich und anschließend Ihre Integrations-ID aus.

Für Null-ETL-Integrationen von Aurora und Amazon RDS bietet Amazon Redshift zwei Arten von Metriken auf der Seite mit den Integrationsdetails für eine Integration. Die Metrikarten lauten wie folgt:

- Auf der Registerkarte Integrationsmetriken sind die folgenden Diagramme verfügbar:

Metrik	Beschreibung
`Lag`	Die Verzögerung zwischen der Übertragung der Daten an Ihre Quelle und dem Zeitpunkt, zu dem die Daten für Abfragen in Amazon Redshift verfügbar sind. Einheiten: Sekunden Maße: `IntegrationLag`
`Tables replicated`	Die Anzahl der Tabellen, die von Ihrer Quelldatenbank nach Amazon Redshift repliziert wurden. Einheiten: Anzahl

Metrik	Beschreibung
	Maße: `IntegrationNumTablesReplicated`
`Tables failed`	Die Anzahl der Tabellen, bei denen die Replikation fehlgesch lagen ist. Einheiten: Anzahl Maße: `IntegrationNumTablesFailedReplication`

- Auf der Registerkarte Tabellenstatistiken können Sie die Liste der Tabellen ansehen, die derzeit aktiv sind oder Fehler aufweisen. Die Statistiken auf dieser Registerkarte lauten wie folgt:
  - Schemaname: Der Name des Schemas, in dem sich die Tabelle befindet.
  - Tabellenname: Der Name der Tabelle in der Quelldatenbank.
  - Status: Der Status der Tabelle. Mögliche Werte sind `Synced`, `Failed`, `Deleted`, `Resync Required` und `Resync Initiated`.
  - Datenbank: Die Amazon-Redshift-Datenbank, in der sich die Tabelle befindet.
  - Letzte Aktualisierung: Datum und Uhrzeit (UTC) der letzten Aktualisierung der Tabelle.

Fehlerbehebung bei Null-ETL-Integrationen

Fehlerbehebung bei Null-ETL-Integrationen mit Aurora MySQL

Verwenden Sie die folgenden Informationen, um häufig auftretende Fehler bei Null-ETL-Integrationen mit Aurora MySQL zu beheben.

Themen

- Die Erstellung der Integration ist fehlgeschlagen
- Tabellen haben keine Primärschlüssel
- Nicht unterstützte Datentypen in Tabellen
- Befehle der Datenbearbeitungssprache (DML) sind fehlgeschlagen
- Nachverfolgte Änderungen zwischen Datenquellen stimmen nicht überein
- Autorisierung fehlgeschlagen

- Die Anzahl der Tabellen beträgt mehr als 100.000 oder die Anzahl der Schemata beträgt mehr als 4950
- Amazon Redshift kann keine Daten laden
- Die Einstellungen der Arbeitsgruppenparameter sind falsch
- Die Datenbank zur Aktivierung einer Null-ETL-Integration wurde nicht erstellt
- Die Tabelle befindet sich im Status Resynchronisierung erforderlich oder Resynchronisierung eingeleitet

Die Erstellung der Integration ist fehlgeschlagen

Wenn die Erstellung der Null-ETL-Integration fehlgeschlagen ist, lautet der Status der Integration `Inactive`. Stellen Sie sicher, dass Folgendes für Ihren Aurora-DB-Quell-Cluster zutrifft:

- Sie haben Ihren Cluster in der Amazon RDS-Konsole erstellt.
- Auf Ihrem Aurora-Quell-DB-Cluster wird MySQL Version 3.05 oder höher ausgeführt. Um dies zu überprüfen, wechseln Sie zur Registerkarte Konfiguration für den Cluster und überprüfen Sie die Engine-Version.
- Sie haben die Binlog-Parametereinstellungen für Ihren Cluster korrekt konfiguriert. Wenn Ihre Aurora MySQL-Binlog-Parameter falsch eingestellt sind oder nicht mit dem Aurora-DB-Quell-Cluster verknüpft sind, schlägt die Erstellung fehl. Siehe Konfiguration von DB-Cluster-Parametern.

Stellen Sie außerdem sicher, dass Folgendes für Ihr Amazon Redshift Data Warehouse zutrifft:

- Die Unterscheidung zwischen Groß- und Kleinschreibung ist aktiviert. Siehe Aktivieren der Unterscheidung zwischen Groß- und Kleinschreibung für Ihr Data Warehouse.
- Sie haben den richtigen autorisierten Prinzipal und die richtige Integrationsquelle für Ihren Namespace hinzugefügt. Siehe Konfigurieren der Autorisierung für Ihr Amazon Redshift Data Warehouse.

Tabellen haben keine Primärschlüssel

In der Zieldatenbank haben eine oder mehrere Tabellen keinen Primärschlüssel und können nicht synchronisiert werden.

Um dieses Problem zu beheben, wechseln Sie zur Registerkarte Tabellenstatistiken auf der Seite der Integrationsdetails oder verwenden Sie SVV_INTEGRATION_TABLE_STATE, um die

fehlgeschlagenen Tabellen anzuzeigen. Sie können Primärschlüssel zu den Tabellen hinzufügen und Amazon Redshift synchronisiert die Tabellen erneut. Alternativ können Sie diese Tabellen in Aurora löschen und Tabellen mit einem Primärschlüssel erstellen. Dies wird jedoch nicht empfohlen. Weitere Informationen finden Sie unter Bewährte Methoden für die Gestaltung von Tabellen mit Amazon Redshift.

Nicht unterstützte Datentypen in Tabellen

In der Datenbank, die Sie aus der Integration in Amazon Redshift erstellt haben und in der Daten aus dem Aurora-DB-Cluster repliziert werden, weist mindestens eine Tabelle nicht unterstützte Datentypen auf und kann nicht synchronisiert werden.

Um dieses Problem zu beheben, wechseln Sie zur Registerkarte Tabellenstatistiken auf der Seite der Integrationsdetails oder verwenden Sie SVV_INTEGRATION_TABLE_STATE, um die fehlgeschlagenen Tabellen anzuzeigen. Entfernen Sie diese Tabellen anschließend und erstellen Sie neue Tabellen auf Amazon RDS. Weitere Informationen zu nicht unterstützten Datentypen finden Sie unter Datentypunterschiede zwischen Aurora- und Amazon-Redshift-Datenbanken im Amazon-Aurora-Benutzerhandbuch.

Befehle der Datenbearbeitungssprache (DML) sind fehlgeschlagen

Amazon Redshift konnte keine DML-Befehle in den Redshift-Tabellen ausführen. Um dieses Problem zu beheben, verwenden Sie SVV_INTEGRATION_TABLE_STATE, um die fehlgeschlagenen Tabellen anzuzeigen. Amazon Redshift synchronisiert die Tabellen automatisch neu, um diesen Fehler zu beheben.

Nachverfolgte Änderungen zwischen Datenquellen stimmen nicht überein

Dieser Fehler tritt auf, wenn die Änderungen zwischen Amazon Aurora und Amazon Redshift nicht übereinstimmen, was dazu führt, dass die Integration in den Status `Failed` wechselt.

Um dieses Problem zu beheben, löschen Sie die Null-ETL-Integration und erstellen Sie sie in Amazon RDS neu. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen und Löschen von Null-ETL-Integrationen.

Autorisierung fehlgeschlagen

Die Autorisierung ist fehlgeschlagen, weil der Aurora-DB-Quell-Cluster als autorisierte Integrationsquelle für das Amazon Redshift Data Warehouse entfernt wurde.

Um dieses Problem zu beheben, löschen Sie die Null-ETL-Integration und erstellen Sie sie in Amazon RDS neu. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen und Löschen von Null-ETL-Integrationen.

Die Anzahl der Tabellen beträgt mehr als 100.000 oder die Anzahl der Schemata beträgt mehr als 4950

Für ein Ziel-Data-Warehouse beträgt die Anzahl der Tabellen mehr als 100.000 oder die Anzahl der Schemas mehr als 4950. Amazon Aurora kann keine Daten an Amazon Redshift senden. Die Anzahl der Tabellen und Schemas überschreitet den festgelegten Grenzwert. Um dieses Problem zu beheben, entfernen Sie alle unnötigen Schemata oder Tabellen aus der Quelldatenbank.

Amazon Redshift kann keine Daten laden

Amazon Redshift kann keine Daten in die Null-ETL-Integration laden.

Um dieses Problem zu beheben, löschen Sie die Null-ETL-Integration auf Amazon RDS und erstellen Sie sie neu. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen und Löschen von Null-ETL-Integrationen.

Die Einstellungen der Arbeitsgruppenparameter sind falsch

In Ihrer Arbeitsgruppe ist die Unterscheidung zwischen Groß- und Kleinschreibung nicht aktiviert.

Um dieses Problem zu beheben, wechseln Sie zur Registerkarte Eigenschaften, wählen Sie die Parametergruppe aus und aktivieren Sie auf der Registerkarte Eigenschaften die ID zur Unterscheidung zwischen Groß- und Kleinschreibung. Wenn Sie keine bestehende Parametergruppe haben, erstellen Sie eine, bei der die Unterscheidung zwischen Groß- und Kleinschreibung aktiviert ist. Erstellen Sie dann eine neue Null-ETL-Integration in Amazon RDS. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen.

Die Datenbank zur Aktivierung einer Null-ETL-Integration wurde nicht erstellt

Es wurde keine Datenbank erstellt, um die Null-ETL-Integration zu aktivieren.

Um dieses Problem zu beheben, erstellen Sie eine Datenbank für die Integration. Weitere Informationen finden Sie unter Erstellen einer Zieldatenbank in Amazon Redshift.

Die Tabelle befindet sich im Status Resynchronisierung erforderlich oder Resynchronisierung eingeleitet

Ihre Tabelle befindet sich im Status Resynchronisierung erforderlich oder Resynchronisierung eingeleitet.

Um ausführlichere Fehlerinformationen darüber zu sammeln, warum sich Ihre Tabelle in diesem Status befindet, verwenden Sie die Systemansicht SYS_LOAD_ERROR_DETAIL.

Fehlerbehebung bei Null-ETL-Integrationen mit Aurora PostgreSQL

Verwenden Sie die folgenden Informationen, um häufig auftretende Fehler bei Null-ETL-Integrationen mit Aurora PostgreSQL zu beheben.

Themen

- Die Erstellung der Integration ist fehlgeschlagen
- Tabellen haben keine Primärschlüssel
- Nicht unterstützte Datentypen in Tabellen
- Befehle der Datenbearbeitungssprache (DML) sind fehlgeschlagen
- Nachverfolgte Änderungen zwischen Datenquellen stimmen nicht überein
- Autorisierung fehlgeschlagen
- Die Anzahl der Tabellen beträgt mehr als 100.000 oder die Anzahl der Schemata beträgt mehr als 4950
- Amazon Redshift kann keine Daten laden
- Die Einstellungen der Arbeitsgruppenparameter sind falsch
- Die Datenbank zur Aktivierung einer Null-ETL-Integration wurde nicht erstellt
- Die Tabelle befindet sich im Status Resynchronisierung erforderlich oder Resynchronisierung eingeleitet

Die Erstellung der Integration ist fehlgeschlagen

Wenn die Erstellung der Null-ETL-Integration fehlgeschlagen ist, lautet der Status der Integration `Inactive`. Stellen Sie sicher, dass Folgendes für Ihren Aurora-DB-Quell-Cluster zutrifft:

- Sie haben Ihren Cluster in der Amazon RDS-Konsole erstellt.
- Auf Ihrem Aurora-DB-Quell-Cluster wird Aurora PostgreSQL Version 15.4.99 oder höher ausgeführt. Um dies zu überprüfen, wechseln Sie zur Registerkarte Konfiguration für den Cluster und überprüfen Sie die Engine-Version.
- Sie haben die Binlog-Parametereinstellungen für Ihren Cluster korrekt konfiguriert. Wenn Ihre Aurora-PostgreSQL-Binlog-Parameter falsch eingestellt oder nicht mit dem Aurora-DB-Quell-Cluster verknüpft sind, schlägt die Erstellung fehl. Siehe Konfiguration von DB-Cluster-Parametern.

Stellen Sie außerdem sicher, dass Folgendes für Ihr Amazon Redshift Data Warehouse zutrifft:

- Die Unterscheidung zwischen Groß- und Kleinschreibung ist aktiviert. Siehe Aktivieren der Unterscheidung zwischen Groß- und Kleinschreibung für Ihr Data Warehouse.
- Sie haben den richtigen autorisierten Prinzipal und die richtige Integrationsquelle für Ihren Namespace hinzugefügt. Siehe Konfigurieren der Autorisierung für Ihr Amazon Redshift Data Warehouse.

Tabellen haben keine Primärschlüssel

In der Zieldatenbank haben eine oder mehrere Tabellen keinen Primärschlüssel und können nicht synchronisiert werden.

Um dieses Problem zu beheben, wechseln Sie zur Registerkarte Tabellenstatistiken auf der Seite der Integrationsdetails oder verwenden Sie SVV_INTEGRATION_TABLE_STATE, um die fehlgeschlagenen Tabellen anzuzeigen. Sie können Primärschlüssel zu den Tabellen hinzufügen und Amazon Redshift synchronisiert die Tabellen erneut. Alternativ können Sie diese Tabellen in Aurora löschen und Tabellen mit einem Primärschlüssel erstellen. Dies wird jedoch nicht empfohlen. Weitere Informationen finden Sie unter Bewährte Methoden für die Gestaltung von Tabellen mit Amazon Redshift.

Nicht unterstützte Datentypen in Tabellen

In der Datenbank, die Sie aus der Integration in Amazon Redshift erstellt haben und in der Daten aus dem Aurora-DB-Cluster repliziert werden, weist mindestens eine Tabelle nicht unterstützte Datentypen auf und kann nicht synchronisiert werden.

Um dieses Problem zu beheben, wechseln Sie zur Registerkarte Tabellenstatistiken auf der Seite der Integrationsdetails oder verwenden Sie SVV_INTEGRATION_TABLE_STATE, um die fehlgeschlagenen Tabellen anzuzeigen. Entfernen Sie diese Tabellen anschließend und erstellen Sie neue Tabellen auf Amazon RDS. Weitere Informationen zu nicht unterstützten Datentypen finden Sie unter Datentypunterschiede zwischen Aurora- und Amazon-Redshift-Datenbanken im Amazon-Aurora-Benutzerhandbuch.

Befehle der Datenbearbeitungssprache (DML) sind fehlgeschlagen

Amazon Redshift konnte keine DML-Befehle in den Redshift-Tabellen ausführen. Um dieses Problem zu beheben, verwenden Sie SVV_INTEGRATION_TABLE_STATE, um die fehlgeschlagenen Tabellen anzuzeigen. Amazon Redshift synchronisiert die Tabellen automatisch neu, um diesen Fehler zu beheben.

Nachverfolgte Änderungen zwischen Datenquellen stimmen nicht überein

Dieser Fehler tritt auf, wenn die Änderungen zwischen Amazon Aurora und Amazon Redshift nicht übereinstimmen, was dazu führt, dass die Integration in den Status `Failed` wechselt.

Um dieses Problem zu beheben, löschen Sie die Null-ETL-Integration und erstellen Sie sie in Amazon RDS neu. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen und Löschen von Null-ETL-Integrationen.

Autorisierung fehlgeschlagen

Die Autorisierung ist fehlgeschlagen, weil der Aurora-DB-Quell-Cluster als autorisierte Integrationsquelle für das Amazon Redshift Data Warehouse entfernt wurde.

Um dieses Problem zu beheben, löschen Sie die Null-ETL-Integration und erstellen Sie sie in Amazon RDS neu. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen und Löschen von Null-ETL-Integrationen.

Die Anzahl der Tabellen beträgt mehr als 100.000 oder die Anzahl der Schemata beträgt mehr als 4950

Für ein Ziel-Data-Warehouse beträgt die Anzahl der Tabellen mehr als 100.000 oder die Anzahl der Schemas mehr als 4950. Amazon Aurora kann keine Daten an Amazon Redshift senden. Die Anzahl der Tabellen und Schemas überschreitet den festgelegten Grenzwert. Um dieses Problem zu beheben, entfernen Sie alle unnötigen Schemata oder Tabellen aus der Quelldatenbank.

Amazon Redshift kann keine Daten laden

Amazon Redshift kann keine Daten in die Null-ETL-Integration laden.

Um dieses Problem zu beheben, löschen Sie die Null-ETL-Integration auf Amazon RDS und erstellen Sie sie neu. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen und Löschen von Null-ETL-Integrationen.

Die Einstellungen der Arbeitsgruppenparameter sind falsch

In Ihrer Arbeitsgruppe ist die Unterscheidung zwischen Groß- und Kleinschreibung nicht aktiviert.

Um dieses Problem zu beheben, wechseln Sie zur Registerkarte Eigenschaften, wählen Sie die Parametergruppe aus und aktivieren Sie auf der Registerkarte Eigenschaften die ID zur Unterscheidung zwischen Groß- und Kleinschreibung. Wenn Sie keine bestehende Parametergruppe

haben, erstellen Sie eine, bei der die Unterscheidung zwischen Groß- und Kleinschreibung aktiviert ist. Erstellen Sie dann eine neue Null-ETL-Integration in Amazon RDS. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen.

Die Datenbank zur Aktivierung einer Null-ETL-Integration wurde nicht erstellt

Es wurde keine Datenbank erstellt, um die Null-ETL-Integration zu aktivieren.

Um dieses Problem zu beheben, erstellen Sie eine Datenbank für die Integration. Weitere Informationen finden Sie unter Erstellen einer Zieldatenbank in Amazon Redshift.

Die Tabelle befindet sich im Status Resynchronisierung erforderlich oder Resynchronisierung eingeleitet

Ihre Tabelle befindet sich im Status Resynchronisierung erforderlich oder Resynchronisierung eingeleitet.

Um ausführlichere Fehlerinformationen darüber zu sammeln, warum sich Ihre Tabelle in diesem Status befindet, verwenden Sie die Systemansicht SYS_LOAD_ERROR_DETAIL.

Fehlerbehebung bei Null-ETL-Integrationen mit RDS für MySQL

Verwenden Sie die folgenden Informationen, um häufig auftretende Fehler bei Null-ETL-Integrationen mit RDS für MySQL zu beheben.

Themen

- Die Erstellung der Integration ist fehlgeschlagen
- Tabellen haben keine Primärschlüssel
- Nicht unterstützte Datentypen in Tabellen
- Befehle der Datenbearbeitungssprache (DML) sind fehlgeschlagen
- Nachverfolgte Änderungen zwischen Datenquellen stimmen nicht überein
- Autorisierung fehlgeschlagen
- Die Anzahl der Tabellen beträgt mehr als 100.000 oder die Anzahl der Schemata beträgt mehr als 4950
- Amazon Redshift kann keine Daten laden
- Die Einstellungen der Arbeitsgruppenparameter sind falsch
- Die Datenbank zur Aktivierung einer Null-ETL-Integration wurde nicht erstellt

- Die Tabelle befindet sich im Status Resynchronisierung erforderlich oder Resynchronisierung eingeleitet

Die Erstellung der Integration ist fehlgeschlagen

Wenn die Erstellung der Null-ETL-Integration fehlgeschlagen ist, lautet der Status der Integration `Inactive`. Stellen Sie sicher, dass Folgendes für Ihre RDS-DB-Quell-Instance zutrifft:

- Sie haben Ihre Instance in der Amazon-RDS-Konsole erstellt.
- Auf Ihrer RDS-DB-Instance wird RDS für MySQL Version 8.0.28 oder höher ausgeführt. Um dies zu überprüfen, wechseln Sie zur Registerkarte Konfiguration für die Instance und prüfen Sie die Engine-Version.
- Sie haben die Binlog-Parametereinstellungen für Ihre Instance korrekt konfiguriert. Wenn die Binlog-Parameter von RDS für MySQL falsch eingestellt oder nicht mit der RDS-DB-Quell-Instance verknüpft sind, schlägt die Erstellung fehl. Siehe Konfigurieren von DB-Instance-Parametern.

Stellen Sie außerdem sicher, dass Folgendes für Ihr Amazon Redshift Data Warehouse zutrifft:

- Die Unterscheidung zwischen Groß- und Kleinschreibung ist aktiviert. Siehe Aktivieren der Unterscheidung zwischen Groß- und Kleinschreibung für Ihr Data Warehouse.
- Sie haben den richtigen autorisierten Prinzipal und die richtige Integrationsquelle für Ihren Namespace hinzugefügt. Siehe Konfigurieren der Autorisierung für Ihr Amazon Redshift Data Warehouse.

Tabellen haben keine Primärschlüssel

In der Zieldatenbank haben eine oder mehrere Tabellen keinen Primärschlüssel und können nicht synchronisiert werden.

Um dieses Problem zu beheben, wechseln Sie zur Registerkarte Tabellenstatistiken auf der Seite der Integrationsdetails oder verwenden Sie SVV_INTEGRATION_TABLE_STATE, um die fehlgeschlagenen Tabellen anzuzeigen. Sie können Primärschlüssel zu den Tabellen hinzufügen und Amazon Redshift synchronisiert die Tabellen erneut. Alternativ können Sie diese Tabellen in RDS löschen und Tabellen mit einem Primärschlüssel erstellen. Dies wird jedoch nicht empfohlen. Weitere Informationen finden Sie unter Bewährte Methoden für die Gestaltung von Tabellen mit Amazon Redshift.

Nicht unterstützte Datentypen in Tabellen

In der Datenbank, die Sie aus der Integration in Amazon Redshift erstellt haben und in der Daten aus der RDS-DB-Instance repliziert werden, weist mindestens eine Tabelle nicht unterstützte Datentypen auf und kann nicht synchronisiert werden.

Um dieses Problem zu beheben, wechseln Sie zur Registerkarte Tabellenstatistiken auf der Seite der Integrationsdetails oder verwenden Sie SVV_INTEGRATION_TABLE_STATE, um die fehlgeschlagenen Tabellen anzuzeigen. Entfernen Sie diese Tabellen anschließend und erstellen Sie neue Tabellen auf Amazon RDS. Weitere Informationen zu nicht unterstützten Datentypen finden Sie unter Datentypunterschiede zwischen RDS- und Amazon-Redshift-Datenbanken im Amazon-RDS-Benutzerhandbuch.

Befehle der Datenbearbeitungssprache (DML) sind fehlgeschlagen

Amazon Redshift konnte keine DML-Befehle in den Redshift-Tabellen ausführen. Um dieses Problem zu beheben, verwenden Sie SVV_INTEGRATION_TABLE_STATE, um die fehlgeschlagenen Tabellen anzuzeigen. Amazon Redshift synchronisiert die Tabellen automatisch neu, um diesen Fehler zu beheben.

Nachverfolgte Änderungen zwischen Datenquellen stimmen nicht überein

Dieser Fehler tritt auf, wenn die Änderungen zwischen Amazon Aurora und Amazon Redshift nicht übereinstimmen, was dazu führt, dass die Integration in den Status `Failed` wechselt.

Um dieses Problem zu beheben, löschen Sie die Null-ETL-Integration und erstellen Sie sie in Amazon RDS neu. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen und Löschen von Null-ETL-Integrationen.

Autorisierung fehlgeschlagen

Die Autorisierung ist fehlgeschlagen, da die RDS-DB-Quell-Instance als autorisierte Integrationsquelle für das Amazon Redshift Data Warehouse entfernt wurde.

Um dieses Problem zu beheben, löschen Sie die Null-ETL-Integration und erstellen Sie sie in Amazon RDS neu. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen und Löschen von Null-ETL-Integrationen.

Die Anzahl der Tabellen beträgt mehr als 100.000 oder die Anzahl der Schemata beträgt mehr als 4950

Für ein Ziel-Data-Warehouse beträgt die Anzahl der Tabellen mehr als 100.000 oder die Anzahl der Schemas mehr als 4950. Amazon Aurora kann keine Daten an Amazon Redshift senden. Die Anzahl der Tabellen und Schemas überschreitet den festgelegten Grenzwert. Um dieses Problem zu beheben, entfernen Sie alle unnötigen Schemata oder Tabellen aus der Quelldatenbank.

Amazon Redshift kann keine Daten laden

Amazon Redshift kann keine Daten in die Null-ETL-Integration laden.

Um dieses Problem zu beheben, löschen Sie die Null-ETL-Integration auf Amazon RDS und erstellen Sie sie neu. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen und Löschen von Null-ETL-Integrationen.

Die Einstellungen der Arbeitsgruppenparameter sind falsch

In Ihrer Arbeitsgruppe ist die Unterscheidung zwischen Groß- und Kleinschreibung nicht aktiviert.

Um dieses Problem zu beheben, wechseln Sie zur Registerkarte Eigenschaften, wählen Sie die Parametergruppe aus und aktivieren Sie auf der Registerkarte Eigenschaften die ID zur Unterscheidung zwischen Groß- und Kleinschreibung. Wenn Sie keine bestehende Parametergruppe haben, erstellen Sie eine, bei der die Unterscheidung zwischen Groß- und Kleinschreibung aktiviert ist. Erstellen Sie dann eine neue Null-ETL-Integration in Amazon RDS. Weitere Informationen finden Sie unter Erstellen von Null-ETL-Integrationen.

Die Datenbank zur Aktivierung einer Null-ETL-Integration wurde nicht erstellt

Es wurde keine Datenbank erstellt, um die Null-ETL-Integration zu aktivieren.

Um dieses Problem zu beheben, erstellen Sie eine Datenbank für die Integration. Weitere Informationen finden Sie unter Erstellen einer Zieldatenbank in Amazon Redshift.

Die Tabelle befindet sich im Status Resynchronisierung erforderlich oder Resynchronisierung eingeleitet

Ihre Tabelle befindet sich im Status Resynchronisierung erforderlich oder Resynchronisierung eingeleitet.

Um ausführlichere Fehlerinformationen darüber zu sammeln, warum sich Ihre Tabelle in diesem Status befindet, verwenden Sie die Systemansicht SYS_LOAD_ERROR_DETAIL.

Abfragen einer Datenbank

Sie haben zwei Möglichkeiten, von Ihrem Amazon-Redshift-Cluster gehostete Datenbanken abzufragen:

- Connect zu Ihrem Cluster her und führen Sie Abfragen auf dem AWS Management Console mit dem Abfrage-Editor aus.

  Wenn Sie den Abfrage-Editor in der Amazon-Redshift-Konsole verwenden, müssen Sie keine SQL-Clientanwendung herunterladen und einrichten.
- Verwenden Sie ein SQL-Client-Tool (z. B. SQL Workbench/J), um eine Verbindung zu Ihrem Cluster herzustellen.

  Amazon Redshift unterstützt SQL-Client-Tools, die über Java Database Connectivity (JDBC) und Open Database Connectivity (ODBC) Verbindungen herstellen. Amazon Redshift stellt keine SQL-Client-Tools oder Bibliotheken bereit oder installiert sie. Daher müssen Sie diese auf Ihrem Clientcomputer oder Ihrer Amazon-EC2-Instance installieren. Sie können die meisten SQL-Client-Tools verwenden, die JDBC- oder ODBC-Treiber unterstützen.

> **Note**
>
> Wenn Sie gespeicherte Prozeduren schreiben, empfehlen wir eine bewährte Methode zum Sichern sensibler Werte:
> Nehmen Sie keine Hardkodierung für sensible Informationen in der gespeicherten Prozedurlogik vor. Weisen Sie beispielsweise kein Benutzerkennwort in einer CREATE USER-Anweisung im Text einer gespeicherten Prozedur zu. Dies stellt ein Sicherheitsrisiko dar, da hartkodierte Werte als Schema-Metadaten in Katalogtabellen aufgezeichnet werden können. Übergeben Sie stattdessen mithilfe von Parametern sensible Werte wie Passwörter als Argumente an die gespeicherte Prozedur.
> Weitere Informationen über gespeicherte Prozeduren finden Sie unter CREATE PROCEDURE und Erstellen von gespeicherten Prozeduren in Amazon Redshift. Weitere Informationen über die Katalogtabellen finden Sie unter Systemkatalogtabellen.

Themen

- Abfragen für Datenbanken mit dem Amazon-Redshift-Abfrage-Editor v2

- Abfragen für Datenbanken mit dem Abfrage-Editor
- Herstellen einer Verbindung zu einem Amazon Redshift Data Warehouse mithilfe von SQL-Client-Tools
- Verwenden der Amazon Redshift Data API

Abfragen für Datenbanken mit dem Amazon-Redshift-Abfrage-Editor v2

Der Abfrage-Editor v2 ist eine separate webbasierte SQL-Clientanwendung, mit der Sie Abfragen in Ihrem Amazon Redshift Data Warehouse erstellen und ausführen können. Sie können Ihre Ergebnisse in Diagrammen darstellen und Abfragen mit anderen im Team teilen. Der Abfrage-Editor v2 ersetzt den vorherigen Abfrage-Editor.

> **Note**
>
> Der Abfrage-Editor v2 ist kommerziell erhältlich AWS-Regionen. Eine Liste, AWS-Regionen wo der Abfrage-Editor v2 verfügbar ist, finden Sie in den Endpunkten, die für den Redshift-Abfrage-Editor v2 aufgeführt sind. Allgemeine Amazon Web Services-Referenz

Eine Demo zum Abfrage-Editor v2 finden Sie im folgenden Video. Abfrage-Editor V2 von Amazon Redshift.

Eine Demo zur Datenanalyse finden Sie im folgenden Video. Datenanalyse mit dem Abfrage-Editor v2 von Amazon Redshift.

Eine Demo zur Verwendung des Abfrage-Editors v2 für die Ausführung mehrerer Abfragen mit einer isolierten oder einer gemeinsam genutzten Verbindung finden Sie im folgenden Video. Gleichzeitige Abfrageausführung mit Abfrage-Editor v2.

Der Abfrage-Editor v2 verfügt über eine Vielzahl von Funktionen zum Verwalten und Ausführen Ihrer SQL-Anweisungen. Die Themen in den folgenden Abschnitten erleichtern Ihnen den Einstieg in viele dieser Funktionen. Erkunden Sie den Abfrage-Editor v2 selbst, um sich mit seinen Funktionen vertraut zu machen.

Themen

- Konfiguration Ihres AWS-Konto

- Arbeiten mit dem Abfrage-Editor v2
- Interaktion mit generativem SQL in Query Editor v2 (Vorschau)
- Laden von Daten in eine Datenbank
- Erstellen und Ausführen von Abfragen
- Erstellen und Ausführen von Notebooks
- Abfragen der AWS Glue Data Catalog
- Abfragen eines Data Lake
- Arbeiten mit Datashares
- Planung einer Abfrage mit dem Query Editor v2
- Visualisieren von Abfrageergebnissen
- Zusammenarbeiten und Teilen im Team

Konfiguration Ihres AWS-Konto

Wenn Sie den Abfrage-Editor v2 über die Amazon-Redshift-Konsole auswählen, öffnet sich eine neue Registerkarte in Ihrem Browser, auf der die Schnittstelle des Abfrage-Editors v2 zu sehen ist. Mit den entsprechenden Berechtigungen können Sie auf Daten in einem Amazon Redshift Redshift-Cluster oder einer Arbeitsgruppe zugreifen, deren Eigentümer Sie sind und AWS-Konto die sich in der aktuellen Version befinden. AWS-Region

Wenn ein Administrator den Query Editor v2 zum ersten Mal für Sie konfiguriert, wählt er den aus AWS-Konto, der zum Verschlüsseln der AWS KMS key Query Editor v2-Ressourcen verwendet wird. Standardmäßig wird ein AWS eigener Schlüssel zum Verschlüsseln von Ressourcen verwendet. Ein Administrator kann auch einen vom Kunden verwalteten Schlüssel verwenden, indem er den Amazon-Ressourcennamen (ARN) als Schlüssel auf der Konfigurationsseite auswählt. Nach der Konfiguration eines Kontos können die AWS KMS Verschlüsselungseinstellungen nicht geändert werden. Weitere Informationen zum Erstellen und Verwenden eines vom Kunden verwalteten Schlüssels mit dem Abfrage-Editor v2 finden Sie unter Einen vom AWS KMS Kunden verwalteten Schlüssel zur Verwendung mit dem Abfrage-Editor v2 erstellen. Der Administrator kann optional auch einen S3-Bucket und Pfad auswählen, der für einige Funktionen wie z. B. das Laden von Daten aus einer Datei verwendet wird. Weitere Informationen finden Sie unter Laden von Daten aus einer lokalen Datei – Einrichtung und Workflow.

Der Amazon-Redshift-Abfrage-Editor v2 unterstützt Authentifizierung, Verschlüsselung, Isolation und Compliance, um Data-at-Rest zu wahren und Daten während der Übertragung zu schützen. Weitere Informationen zu Datensicherheit im Abfrage-Editor v2 finden Sie hier:

- Verschlüsselung im Ruhezustand
- Verschlüsselung während der Übertragung
- Konfigurations- und Schwachstellenanalyse in Amazon Redshift

AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden, AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen zur Ausführung des Abfrage-Editors v2 in AWS CloudTrail finden Sie unter Protokollieren mit CloudTrail. Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

Der Abfrage-Editor v2 verfügt für einige seiner Ressourcen über einstellbare Kontingente. Weitere Informationen finden Sie unter Kontingente für Amazon-Redshift-Objekte.

Mit dem Abfrage-Editor v2 erstellte Ressourcen

Im Abfrage-Editor v2 können Sie Ressourcen wie gespeicherte Abfragen und Diagramme erstellen. Alle Ressourcen im Abfrage-Editor v2 sind einer IAM-Rolle oder einem Benutzer zugeordnet. Wir empfehlen, Richtlinien an eine IAM-Rolle anzufügen und die Rolle einem Benutzer zuzuweisen.

Im Abfrage-Editor v2 können Sie Tags für gespeicherte Abfragen und Diagramme hinzufügen und entfernen. Sie können diese Tags verwenden, wenn Sie benutzerdefinierte IAM-Richtlinien einrichten oder nach Ressourcen suchen. Sie können Tags auch mithilfe des AWS Resource Groups Tag-Editors verwalten.

Sie können IAM-Rollen mit IAM-Richtlinien einrichten, um Abfragen mit anderen in Ihrem eigenen Bereich zu teilen. AWS-Konto AWS-Region

Einen vom AWS KMS Kunden verwalteten Schlüssel zur Verwendung mit dem Abfrage-Editor v2 erstellen

So erstellen Sie einen kundenverwalteten Schlüssel mit symmetrischer Verschlüsselung:

Sie können einen vom Kunden verwalteten symmetrischen Verschlüsselungsschlüssel erstellen, um die Ressourcen des Abfrageeditors v2 mithilfe der AWS KMS Konsole oder AWS KMS API-Operationen zu verschlüsseln. Anweisungen zum Erstellen eines Schlüssels finden Sie unter Erstellen eines symmetrischen AWS KMS Verschlüsselungsschlüssels im AWS Key Management Service Entwicklerhandbuch.

Schlüsselrichtlinie

Schlüsselrichtlinien steuern den Zugriff auf den vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die aussagt, wer den Schlüssel wie verwenden kann. Wenn Sie Ihren vom Kunden verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie im AWS Key Management Service Entwicklerhandbuch unter Verwaltung des Zugriffs auf AWS KMS Schlüssel.

Um Ihren vom Kunden verwalteten Schlüssel mit dem Amazon-Redshift-Abfrage-Editor v2 verwenden zu können, müssen die folgenden API-Operationen per Schlüsselrichtlinie zulässig sein:

- `kms:GenerateDataKey` – Erzeugt einen eindeutigen symmetrischen Datenschlüssel zur Verschlüsselung Ihrer Daten.
- `kms:Decrypt` – Entschlüsselt Daten, die mit dem vom Kunden verwalteten Schlüssel verschlüsselt wurden.
- `kms:DescribeKey` – Stellt die vom Kunden verwalteten Schlüsseldetails bereit, damit der Service den Schlüssel validieren kann.

Im Folgenden finden Sie ein Beispiel für eine AWS KMS Richtlinie für AWS-Konto `111122223333`. Im ersten Abschnitt wird schränkt der `kms:ViaService` die Verwendung des Schlüssels auf den Service (Abfrage-Editor v2) ein (in der Richtlinie `sqlworkbench.`*`region`*`.amazonaws.com` genannt). Die AWS-Konto Verwendung des Schlüssels muss erfolgen`111122223333`. Im zweiten Abschnitt AWS-Konto `111122223333` können der Root-Benutzer und die Schlüsseladministratoren von auf den Schlüssel zugreifen.

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer

anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

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

In den folgenden Ressourcen finden Sie weitere Informationen zu AWS KMS Schlüsseln:

- Weitere Informationen zu AWS KMS Richtlinien finden Sie im AWS Key Management Service Entwicklerhandbuch unter Angeben von Berechtigungen in einer Richtlinie.
- Informationen zur Fehlerbehebung bei AWS KMS Richtlinien finden Sie unter Problembehandlung beim Schlüsselzugriff im AWS Key Management Service Entwicklerhandbuch.
- Weitere Informationen über Schlüssel finden Sie unter AWS -KMS-Schlüssel im AWS Key Management Service -Entwicklerhandbuch.

Zugreifen auf den Abfrage-Editor v2

Um den Abfrage-Editor v2 aufzurufen, benötigen Sie eine Berechtigung. Ein Administrator kann der Rolle eine der folgenden AWS verwalteten Richtlinien hinzufügen, um Berechtigungen zu erteilen. (Wir empfehlen, Richtlinien an eine IAM-Rolle anzufügen und die Rolle einem Benutzer zuzuweisen.) Diese AWS verwalteten Richtlinien verfügen über verschiedene Optionen, mit denen gesteuert wird, wie das Markieren von Ressourcen die gemeinsame Nutzung von Abfragen ermöglicht. Sie können zum Zuweisen von IAM-Richtlinien die IAM-Konsole (https://console.aws.amazon.com/iam/) verwenden.

- AmazonRedshiftQueryEditorV2 FullAccess — Gewährt vollen Zugriff auf die Vorgänge und Ressourcen des Amazon Redshift Query Editor v2. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste.
- AmazonRedshiftQueryEditorV2 NoSharing — Ermöglicht die Arbeit mit dem Amazon Redshift Query Editor v2, ohne Ressourcen gemeinsam zu nutzen. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste.
- AmazonRedshiftQueryEditorV2 ReadSharing — Ermöglicht die Arbeit mit dem Amazon Redshift Query Editor v2 mit begrenzter gemeinsamer Nutzung von Ressourcen. Der Prinzipal mit der entsprechenden Berechtigung kann die mit seinem Team geteilten Ressourcen lesen, kann sie jedoch nicht ändern. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste.
- AmazonRedshiftQueryEditorV2 ReadWriteSharing — Ermöglicht die Arbeit mit dem Amazon Redshift Query Editor v2 mit gemeinsamer Nutzung von Ressourcen. Der Prinzipal mit den entsprechenden Berechtigungen kann die mit seinem Team geteilten Ressourcen lesen und bearbeiten. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste.

Sie können auch Ihre eigene Richtlinie erstellen, basierend auf den zulässigen und verweigerten Berechtigungen in den bereitgestellten verwalteten Richtlinien. Wenn Sie den IAM-Konsolenrichtlinien-Editor verwenden, um Ihre eigene Richtlinie zu erstellen, wählen Sie SQL

Workbench als Service aus, für den Sie die Richtlinie im visuellen Editor erstellen. Der Abfrage-Editor v2 verwendet den Dienstnamen AWS SQL Workbench im visuellen Editor und im IAM-Richtliniensimulator.

Damit ein Prinzipal (ein Benutzer mit einer zugewiesenen IAM-Rolle) eine Verbindung mit einem Amazon-Redshift-Cluster herstellen kann, benötigt er die Berechtigungen in einer der verwalteten Richtlinien des Abfrage-Editors v2. Sie brauchen auch die Berechtigung `redshift:GetClusterCredentials` für den Cluster. Um diese Berechtigung zu erhalten, kann jemand mit Administratorberechtigung eine Richtlinie an die IAM-Rollen anfügen, mit denen mithilfe temporärer Anmeldeinformationen eine Verbindung zum Cluster hergestellt wird. Sie können die Richtlinie auf bestimmte Cluster eingrenzen oder sie allgemeiner formulieren. Weitere Informationen zur Berechtigung zur Verwendung temporärer Anmeldeinformationen finden Sie unter Erstellen einer IAM-Rolle oder eines IAM-Benutzers mit Anrufberechtigungen. GetClusterCredentials

Damit ein Prinzipal (in der Regel ein Benutzer mit einer zugewiesenen IAM-Rolle) auf der Seite Kontoeinstellungen die Funktion Ergebnissatz exportieren für andere im Konto aktivieren kann, benötigt er die Berechtigung `sqlworkbench:UpdateAcountExportSettings`, die der Rolle angefügt ist. Diese Berechtigung ist in der `AmazonRedshiftQueryEditorV2FullAccess` AWS verwalteten Richtlinie enthalten.

Wenn dem Abfrage-Editor v2 neue Funktionen hinzugefügt werden, werden die AWS verwalteten Richtlinien nach Bedarf aktualisiert. Wenn Sie basierend auf den zulässigen und verweigerten Berechtigungen in den bereitgestellten verwalteten Richtlinien Ihre eigene Richtlinie erstellen, bearbeiten Sie Ihre Richtlinien, sodass sie den Änderungen an den verwalteten Richtlinien entsprechen. Weitere Informationen zu verwalteten Richtlinien für Amazon Redshift finden Sie unter AWS verwaltete Richtlinien für Amazon Redshift.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.

- IAM-Benutzer:

- Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
- (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

> **Note**
>
> Wenn ein AWS IAM Identity Center -Administrator alle Berechtigungssatzzuordnungen für einen bestimmten Berechtigungssatz im gesamten Konto entfernt, ist der Zugriff auf alle Query-Editor-Ressourcen, die ursprünglich dem entfernten Berechtigungssatz zugeordnet waren, nicht mehr möglich. Wenn dieselben Berechtigungen später erneut erstellt werden, wird eine neue interne Kennung erstellt. Da sich die interne Kennung geändert hat, kann auf Query-Editor-Ressourcen, die zuvor einem Benutzer gehört haben, nicht zugegriffen werden. Bevor Administratoren einen Berechtigungssatz löschen, empfehlen wir, dass Benutzer des betreffenden Berechtigungssatzes Query-Editor-Ressourcen wie Notebooks und Abfragen als Backup exportieren.

Einrichten von Prinzipal-Tags für die Verbindung eines Clusters oder einer Arbeitsgruppe von Query Editor v2 aus

Wenn Sie mithilfe der Verbundbenutzeroption eine Verbindung zu Ihrem Cluster oder Ihrer Arbeitsgruppe herstellen möchten, richten Sie entweder Ihre IAM-Rolle oder einen Benutzer mit Prinzipal-Tags ein. Sie können auch Ihren Identitätsanbieter (IDP) für die Weitergabe in `RedshiftDbUser` und (optional) `RedshiftDbGroups` einrichten. Weitere Informationen zur Verwendung von IAM zum Verwalten von Tags finden Sie unter Übergeben von Sitzungs-Tags in AWS Security Token Service im IAM-Benutzerhandbuch. Um den Zugriff einzurichten AWS Identity and Access Management, kann ein Administrator mithilfe der IAM-Konsole (https://console.aws.amazon.com/iam/) Tags hinzufügen.

So fügen Sie einer IAM-Rolle Prinzipal-Tags hinzu

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles (Rollen) aus.

3. Wählen Sie die Rolle aus, die Zugriff auf den Abfrage-Editor v2 unter Verwendung eines Verbundbenutzers benötigt.
4. Wählen Sie die Registerkarte Tags aus.
5. Wählen Sie Manage tags (Tags verwalten) aus.
6. Klicken Sie auf Add tag (Tag hinzufügen) und geben Sie für den Wert Key (Schlüssel) `RedshiftDbUser` und unter Value (Wert) den Namen des Verbundbenutzers ein.
7. Wählen Sie optional Add tag (Tag hinzufügen) aus und geben Sie für den Wert Key (Schlüssel) `RedshiftDbGroups` und unter Value (Wert) den Gruppennamen ein, der dem Benutzer zugeordnet werden soll.
8. Klicken Sie auf Save changes (Änderungen speichern), um die Liste der Tags anzuzeigen, die mit Ihrer ausgewählten IAM-Rolle verknüpft sind. Das Weitergeben von Änderungen kann mehrere Sekunden dauern.
9. Um den Verbundbenutzer zu verwenden, aktualisieren Sie die Seite des Abfrage-Editors v2, nachdem die Änderungen weitergegeben wurden.

Einrichten Ihres Identitätsanbieters (IDP) zur Weitergabe von Prinzipal-Tags

Die Vorgehensweise zum Einrichten von Tags mithilfe eines Identitätsanbieters (IDP) variiert je nach IDP. Anweisungen zum Übergeben von Benutzer- und Gruppeninformationen an SAML-Attribute finden Sie in der IDP-Dokumentation. Bei korrekter Konfiguration erscheinen die folgenden Attribute in Ihrer SAML-Antwort, die von verwendet wird, AWS Security Token Service um die wichtigsten Tags für und auszufüllen. `RedshiftDbUser` `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>
```

Der optionale Wert *db_groups* muss eine durch Doppelpunkt getrennte Liste sein, z. B. `group1:group2:group3`.

Darüber hinaus können Sie das Attribut `TransitiveTagKeys` festlegen, um die Tags während der Rollenverkettung beizubehalten.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
```

```
  <AttributeValue>RedshiftDbUser</AttributeValue>
  <AttributeValue>RedshiftDbGroups</AttributeValue>
</Attribute>
```

Weitere Informationen zum Einrichten des Abfrage-Editors v2 finden Sie unter Für die Verwendung des Abfrage-Editors v2 erforderliche Berechtigungen .

> **Note**
>
> Wenn Sie mithilfe der Verbindungsoption Verbundbenutzer von Query Editor v2 eine Verbindung zu Ihrem Cluster oder Ihrer Arbeitsgruppe herstellen, kann der Identitätsanbieter (IDP) benutzerdefinierte Prinzipal-Tags für `RedshiftDbUser` und `RedshiftDbGroups` bereitstellen. Unterstützt derzeit nicht AWS IAM Identity Center die direkte Übergabe von benutzerdefinierten Prinzipal-Tags an den Abfrage-Editor v2.

Arbeiten mit dem Abfrage-Editor v2

Der Abfrage-Editor v2 dient hauptsächlich dazu, Abfragen zu bearbeiten und auszuführen, Ergebnisse zu visualisieren und Ihre Arbeit mit Ihrem Team zu teilen. Mit dem Abfrage-Editor v2 können Sie Datenbanken, Schemata, Tabellen und benutzerdefinierte Funktionen (user-defined functions, UDFs) erstellen. Im Strukturansichtsbereich können Sie für jede Ihrer Datenbanken ihre Schemata anzeigen. Von den einzelnen Schemata können Sie Tabellen, Ansichten, UDFs und gespeicherte Prozeduren anzeigen.

Themen

- Öffnen des Abfrage-Editors v2
- Herstellen einer Verbindung mit einer Amazon-Redshift-Datenbank
- Durchsuchen einer Amazon-Redshift-Datenbank
- Erstellen von Datenbankobjekten
- Abfrage- und Registerkarten-Verlauf anzeigen
- Überlegungen zur Arbeit mit dem Abfrage-Editor v2
- Ändern von Kontoeinstellungen

Öffnen des Abfrage-Editors v2

Den Abfrage-Editor v2 öffnen

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigator-Menü Editor und dann Query editor v2 (Abfrage-Editor v2) aus. Der Abfrage-Editor v2 wird in einer neuen Registerkarte geöffnet.

Die Abfrage-Editor-Seite enthält ein Navigationsmenü, in dem Sie eine Ansicht wie folgt auswählen können:

Editor

Sie verwalten und fragen Ihre Daten ab, die als Tabellen organisiert und in einer Datenbank enthalten sind. Die Datenbank kann gespeicherte Daten oder einen Verweis auf Daten enthalten, die an anderer Stelle, z. B. in Amazon S3, gespeichert sind. Sie stellen eine Verbindung zu einer Datenbank her, die entweder in einem Cluster oder einer Serverless-Arbeitsgruppe enthalten ist.

In der Ansicht Editor haben Sie die folgenden Steuerelemente:

- Im Feld Cluster oder Workgroup (Arbeitsgruppe) wird der Name des Objekts angezeigt, mit dem Sie gerade verbunden sind. Das Feld Database (Datenbank) zeigt die Datenbanken innerhalb des Clusters oder der Arbeitsgruppe an. Aktionen in der Ansicht Database (Datenbank) wirken sich standardmäßig auf die ausgewählte Datenbank aus.
- Eine hierarchische Strukturansicht Ihrer Cluster oder Arbeitsgruppen, Datenbanken und Schemata. Unter den Schemata können Sie mit Ihren Tabellen, Ansichten, Funktionen und gespeicherten Prozeduren arbeiten. Jedes Objekt in der Baumansicht bietet ein Kontextmenü zum Ausführen verknüpfter Aktionen für das Objekt, etwa Refresh (Aktualisieren) oder Drop (Entfernen).
- Die Aktion

  Create (Erstellen) zum Erstellen von Datenbanken, Schemata, Tabellen und Funktionen.

- Die

  -
  Aktion Daten laden, um Daten aus Amazon S3 oder aus einer lokalen Datei in Ihrer Datenbank zu laden.
- Das Symbol

  Save (Speichern) zum Speichern Ihrer Abfrage.
- Das Symbol

  Shortcuts zum Anzeigen der Tastenkombinationen für den Editor.
- Ein

  Mehr-Symbol, um mehr Aktionen im Editor anzuzeigen. Wie beispielsweise:
  - Für mein Team freigeben zum Freigeben einer Abfrage oder eines Notebooks für Ihr Team. Weitere Informationen finden Sie unter Zusammenarbeiten und Teilen im Team.
  - Das Symbol Shortcuts zum Anzeigen der Tastenkombinationen für den Editor.
  - Tab-Verlauf, um den Verlauf einer Registerkarte im Editor anzuzeigen.
  - Aktualisieren der automatischen Vervollständigung, um die angezeigten Vorschläge beim Verfassen von SQL zu aktualisieren.
- Den

  Editor-Bereich, in dem Sie Ihre Abfrage eingeben und ausführen können.

  Nachdem Sie eine Abfrage ausgeführt haben, erscheint die Registerkarte Result mit den Ergebnissen. Hier können Sie Chart (Diagramm) aktivieren und sich die Ergebnisse visuell darstellen lassen. Sie können mit der Option Export (Exportieren) einen Export Ihrer Ergebnisse durchführen.
- Ein

  Notebook-Bereich, in dem Sie Abschnitte hinzufügen können, um SQL einzugeben und auszuführen oder Markdown hinzuzufügen.

Nachdem Sie eine Abfrage ausgeführt haben, erscheint die Registerkarte Result mit den Ergebnissen. In diesem Bereich können Sie mit Export (Exportieren) einen Export Ihrer Ergebnisse durchführen.

Abfragen

Eine Abfrage enthält die SQL-Befehle zum Verwalten und Abfragen Ihrer Daten in einer Datenbank. Wenn Sie den Abfrage-Editor v2 verwenden, um Beispieldaten zu laden, werden auch Beispielabfragen für Sie erstellt und gespeichert.

Wenn Sie eine gespeicherte Abfrage auswählen, können Sie diese über das Kontextmenü (Rechtsklickmenü) öffnen, umbenennen und löschen. Sie können Attribute wie den Abfrage-ARN einer gespeicherten Abfrage anzeigen, indem Sie Abfragedetails auswählen. Sie können auch den Versionsverlauf einsehen, an die Abfrage angehängte Tags bearbeiten und die Abfrage mit Ihrem Team teilen.

Notebooks

Ein SQL-Notebook enthält SQL- und Markdown-Zellen. Sie können mit Notebooks mehrere SQL-Befehle in einem einzigen Dokument organisieren, kommentieren und freigeben.

Wenn Sie ein gespeichertes Notebook auswählen, können Sie dieses über das Kontextmenü (Rechtsklickmenü) öffnen, umbenennen, duplizieren und löschen. Sie können Attribute wie den Notebook-ARN eines gespeicherten Notebooks anzeigen, indem Sie Notebook-Details auswählen. Sie können auch den Versionsverlauf einsehen, an das Notebook angehängte Tags bearbeiten, das Notebook exportieren und mit Ihrem Team teilen. Weitere Informationen finden Sie unter Erstellen und Ausführen von Notebooks.

Diagramme

Ein Diagramm ist eine visuelle Darstellung Ihrer Daten. Der Abfrage-Editor v2 bietet Werkzeuge, um verschiedene Diagramme zu erstellen und zu speichern.

Wenn Sie ein gespeichertes Diagramm auswählen, können Sie dieses über das Kontextmenü (Rechtsklickmenü) öffnen, umbenennen und löschen. Sie können Attribute wie den Diagramm-ARN eines gespeicherten Diagramms anzeigen, indem Sie Diagrammdetails auswählen. Sie

können auch an das Diagramm angehängte Tags bearbeiten und das Diagramm exportieren. Weitere Informationen finden Sie unter Visualisieren von Abfrageergebnissen.

Verlauf

Der Abfrage-Verlauf ist eine Liste von Abfragen, die Sie mit dem Amazon-Redshift-Abfrage-Editor v2 ausgeführt haben. Diese Abfragen wurden entweder als einzelne Abfragen oder als Teil eines SQL-Notebooks ausgeführt. Weitere Informationen finden Sie unter Abfrage- und Registerkarten-Verlauf anzeigen.

Geplante Abfragen

Eine geplante Abfrage ist eine Abfrage, deren Ausführung für bestimmte Zeitpunkte geplant ist.

Alle Ansichten des Abfrage-Editors v2 haben die folgenden Symbole:

- Ein Symbol

  Visual mode (Visualisierungsmodus) zum Umschalten zwischen Hell- und Dunkelmodus.
- Ein Symbol

  Settings (Einstellungen), um ein Menü mit den verschiedenen Einstellungsbildschirmen anzuzeigen.
  - Ein Symbol

    Editor preferences (Editor-Einstellungen) zum Bearbeiten Ihrer Einstellungen, wenn Sie den Abfrage-Editor v2 verwenden. Hier können Sie die Workspace-Einstellungen bearbeiten, um die Schriftgröße, die Tabulatorgröße und andere Anzeigeneinstellungen zu ändern. Sie können die automatische Vervollständigung auch aktivieren (oder deaktivieren), um Vorschläge bei der Eingabe Ihrer SQL-Anweisung anzuzeigen.
  - Ein Symbol

Connections (Verbindungen), um die von Ihren Editor-Registerkarten verwendeten Verbindungen anzuzeigen.

Eine Verbindung wird zum Abrufen von Daten aus einer Datenbank verwendet. Eine Verbindung wird für eine bestimmte Datenbank erstellt. Bei einer isolierten Verbindung sind die Ergebnisse eines SQL-Befehls, der die Datenbank ändert, z. B. das Erstellen einer temporären Tabelle, auf einer anderen Editor-Registerkarte nicht sichtbar. Wenn Sie eine Editor-Registerkarte im Abfrage-Editor v2 öffnen, ist die Standardeinstellung eine isolierte Verbindung. Wenn Sie eine gemeinsam genutzte Verbindung erstellen, d. h. Sie deaktivieren den Schalter Isolated session (Isolierte Sitzung), dann sind die Ergebnisse in anderen gemeinsam genutzten Verbindungen mit der gleichen Datenbank untereinander sichtbar. Editor-Registerkarten, die eine gemeinsame Verbindung mit einer Datenbank verwenden, werden jedoch nicht parallel ausgeführt. Abfragen, die dieselbe Verbindung verwenden, müssen warten, bis die Verbindung verfügbar ist. Eine Verbindung mit einer Datenbank kann nicht mit einer anderen Datenbank gemeinsam genutzt werden, sodass SQL-Ergebnisse nicht über verschiedene Datenbankverbindungen hinweg sichtbar sind.

Die Anzahl der Verbindungen, die im Konto eines Benutzers aktiv sein können, wird von einem Administrator des Abfrage-Editors v2 gesteuert.

- Ein Symbol

  Account settings (Kontoeinstellungen), das von einem Administrator verwendet wird, um bestimmte Einstellungen aller Benutzer im Konto zu ändern. Weitere Informationen finden Sie unter Ändern von Kontoeinstellungen.

Herstellen einer Verbindung mit einer Amazon-Redshift-Datenbank

Um eine Verbindung zu einer Datenbank herzustellen, wählen Sie den Namen des Clusters oder der Arbeitsgruppe im Strukturansichtsbereich aus. Geben Sie bei Aufforderung die Verbindungsparameter ein.

Wenn Sie eine Verbindung zu einem Cluster oder einer Arbeitsgruppe und ihren Datenbanken herstellen, geben Sie in der Regel einen Namen für Database (Datenbank) an. Sie stellen außerdem Parameter bereit, die für eine der folgenden Authentifizierungsmethoden erforderlich sind:

IAM Identity Center

Stellen Sie mit dieser Methode mit Ihren Single-Sign-On-Anmeldeinformationen von Ihrem Identitätsanbieter (IDP) eine Verbindung zu Ihrem Amazon Redshift Data Warehouse her. Ihr Cluster oder Ihre Arbeitsgruppe muss in der Amazon-Redshift-Konsole für IAM Identity Center aktiviert sein.

Verbundbenutzer

Bei dieser Methode müssen die Prinzipal-Tags Ihrer IAM-Rolle oder Ihres Benutzers die Verbindungsdetails angeben. Sie konfigurieren diese Tags in AWS Identity and Access Management oder Ihrem Identity Provider (IdP). Der Abfrage-Editor v2 basiert auf den folgenden Tags.

- `RedshiftDbUser` – Dieses Tag definiert den Datenbankbenutzer, der vom Abfrage-Editor v2 verwendet wird. Dieses Tag ist erforderlich.
- `RedshiftDbGroups` – Dieses Tag definiert die Datenbankgruppen, die beim Herstellen einer Verbindung mit dem Abfrage-Editor v2 verbunden werden. Dieses Tag ist optional und sein Wert muss eine durch Doppelpunkte getrennte Liste sein, z. B. `group1:group2:group3`. Leere Werte werden ignoriert, d. h. `group1::::group2` wird als `group1:group2` interpretiert.

Diese Tags werden an die API `redshift:GetClusterCredentials` weitergeleitet, um Anmeldeinformationen für Ihren Cluster abzurufen. Weitere Informationen finden Sie unter Einrichten von Prinzipal-Tags für die Verbindung eines Clusters oder einer Arbeitsgruppe von Query Editor v2 aus.

Temporäre Anmeldeinformationen unter Verwendung eines Datenbankbenutzernamens

Diese Option ist nur dann verfügbar, wenn Sie eine Verbindung mit einem Cluster herstellen. Bei dieser Methode, Abfrage-Editor v2, geben Sie einen User name (Benutzername) für die Datenbank an. Query Editor v2 generiert ein temporäres Passwort, um eine Verbindung zu der Datenbank mit Ihrem Datenbankbenutzernamen herzustellen. Ein Benutzer, der diese Methode verwendet, um eine Verbindung herzustellen, muss über die IAM-Berechtigung `redshift:GetClusterCredentials` verfügen. Wenn Sie verhindern möchten, dass Benutzer diese Methode verwenden, ändern Sie ihren IAM-Benutzer oder ihre -Rolle, um diese Berechtigung zu verweigern.

Temporäre Anmeldeinformationen unter Verwendung Ihrer IAM-Identität

Diese Option ist nur dann verfügbar, wenn Sie eine Verbindung mit einem Cluster herstellen. Bei dieser Methode ordnet Query Editor v2 Ihrer IAM-Identität einen Benutzernamen zu und generiert

ein temporäres Passwort zum Herstellen einer Verbindung zu der Datenbank mit Ihrer IAM-Identität. Ein Benutzer, der diese Methode verwendet, um eine Verbindung herzustellen, muss über die IAM-Berechtigung `redshift:GetClusterCredentialsWithIAM` verfügen. Wenn Sie verhindern möchten, dass Benutzer diese Methode verwenden, ändern Sie ihren IAM-Benutzer oder ihre -Rolle, um diese Berechtigung zu verweigern.

Datenbank-Benutzername und -Passwort

Geben Sie bei dieser Methode auch einen User name (Benutzername) und ein Password (Passwort) für die Datenbank an, mit der Sie eine Verbindung herstellen. Der Abfrage-Editor v2 erstellt in Ihrem Namen ein Secret, das in AWS Secrets Manager gesichert wird. Dieses Secret enthält Anmeldeinformationen zum Verbinden mit Ihrer Datenbank.

AWS Secrets Manager

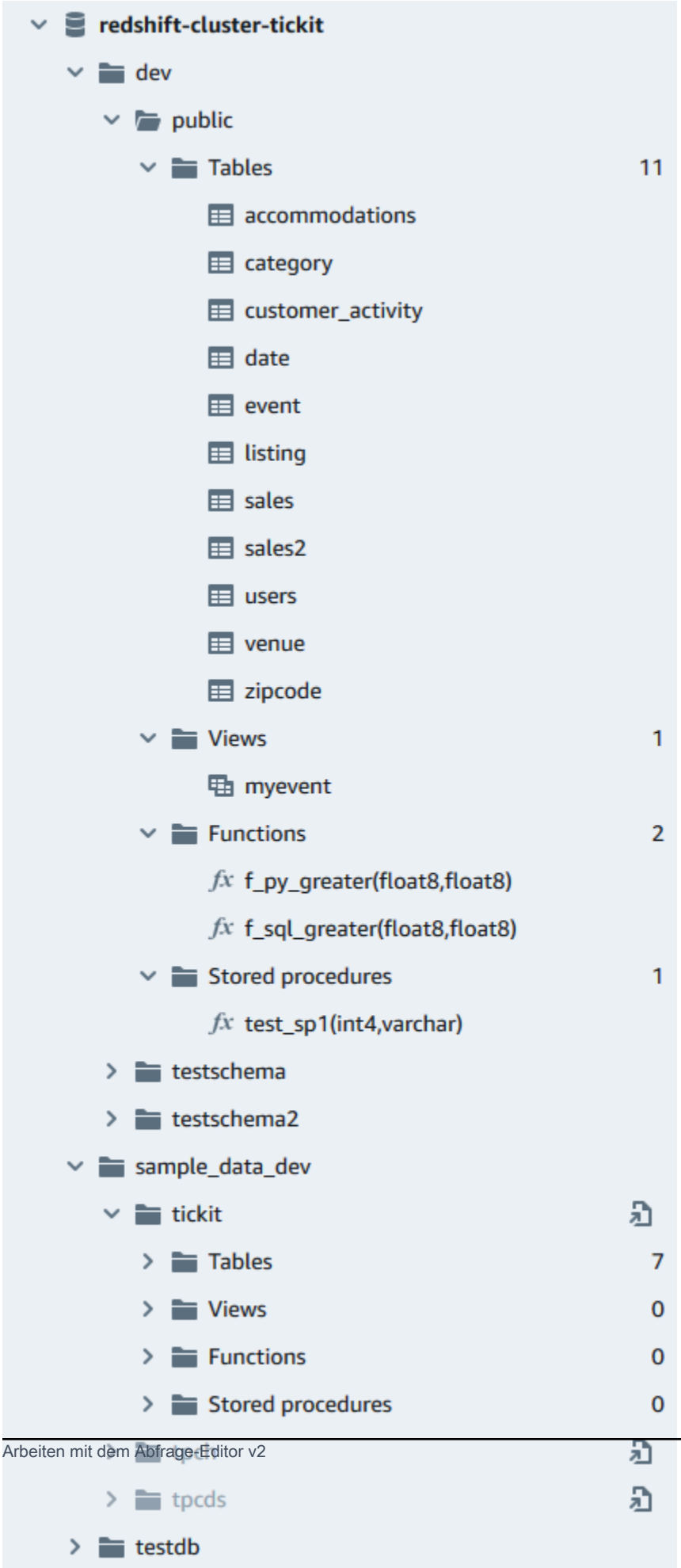
Bei dieser Methode geben Sie anstelle eines Datenbanknamens ein in Secrets Manager gespeichertes Secret an, das Ihre Datenbank und Ihre Anmeldeinformationen enthält. Hinweise zum Erstellen eines Geheimnisses finden Sie unterEin Geheimnis für Datenbankverbindungsdaten erstellen.

Wenn Sie mit dem Abfrage-Editor v2 einen Cluster oder eine Arbeitsgruppe auswählen, können Sie je nach Kontext Verbindungen über das Kontextmenü (Rechtsklick) erstellen, bearbeiten und löschen. Sie können Attribute wie den Verbindungs-ARN der Verbindung anzeigen, indem Sie Verbindungsdetails auswählen. Sie können auch an die Verbindung angehängte Tags bearbeiten.

Durchsuchen einer Amazon-Redshift-Datenbank

In einer Datenbank können Sie Schemata, Tabellen, Ansichten, Funktionen und gespeicherte Prozeduren im Baumansichtsbereich verwalten. Jedem Objekt in der Ansicht sind Aktionen in einem Kontextmenü (rechte Maustaste) zugeordnet.

In der hierarchischen Strukturansicht werden Datenbankobjekte angezeigt. Wenn Sie das Strukturansichtsfenster aktualisieren und Datenbankobjekte anzeigen möchten, die möglicherweise erstellt wurden, nachdem die Strukturansicht zuletzt angezeigt wurde, wählen Sie das -Symbol aus. Beim Öffnen des Kontextmenüs (rechte Maustaste) erscheint ein Objekt, das anzeigt, welche Aktionen Sie ausführen können.


redshift-cluster-tickit
dev
public
Tables 11
accommodations
category
customer_activity
date
event
listing
sales
sales2
users
venue
zipcode
Views 1
myevent
Functions 2
f_py_greater(float8,float8)
f_sql_greater(float8,float8)
Stored procedures 1
test_sp1(int4,varchar)
testschema
testschema2
sample_data_dev
tickit
Tables 7
Views 0
Functions 0
Stored procedures 0
tpcds
testdb

Nachdem Sie eine Tabelle ausgewählt haben, haben Sie folgende Optionen:

- Um eine Abfrage im Editor mit einer SELECT-Anweisung zu starten, die alle Spalten in der Tabelle abfragt, verwenden Sie die Option Select table (Tabelle wählen).
- Um die Attribute oder eine Tabelle anzuzeigen, verwenden Sie die Option Show table definition (Tabellendefinition anzeigen). Hiermit können Sie Spaltennamen, Spaltentypen, Kodierung, Verteilungsschlüssel, Sortierschlüssel sehen und ob eine Spalte Nullwerte enthalten kann. Weitere Informationen über Tabellenattribute finden Sie unter CREATE TABLE im Datenbankentwicklerhandbuch zu Amazon Redshift.
- Um eine Tabelle zu löschen, verwenden Sie Delete (Löschen). Sie können entweder mit Truncate table (Tabelle abschneiden) alle Zeilen aus der Tabelle löschen oder mit Drop table (Tabelle entfernen) die Tabelle aus der Datenbank entfernen. Weitere Informationen finden Sie unter TRUNCATE und DROP TABLE im Datenbankentwicklerhandbuch zu Amazon Redshift.

Wählen Sie bei einem Schema Refresh (Aktualisieren) oder Drop Schema (Schema entfernen) aus.

Wählen Sie bei einer Ansicht Show view definition (Ansichtsdefinition anzeigen) oder Drop view (Ansicht entfernen) aus.

Wählen Sie bei einer Funktion Show function definition (Funktionsdefinition anzeigen) oder Drop function (Funktion entfernen) aus.

Wählen Sie bei einer gespeicherten Prozedur Show procedure definition (Prozedurdefinition anzeigen) oder Drop procedure (Prozedur entfernen) aus.

Erstellen von Datenbankobjekten

Sie können Datenbankobjekte erstellen, etwa Datenbanken, Schemata, Tabellen und benutzerdefinierte Funktionen (UDFs). Sie müssen mit einem Cluster oder einer Arbeitsgruppe und einer Datenbank verbunden sein, um Datenbankobjekte zu erstellen.

Erstellen von Datenbanken

Sie können den Abfrage-Editor v2 verwenden, um Datenbanken in Ihrem Cluster oder Ihrer Arbeitsgruppe zu erstellen.

Eine Datenbank erstellen

Weitere Informationen über Datenbanken finden Sie unter CREATE DATABASE im Datenbankentwicklerhandbuch zu Amazon Redshift.

1. Wählen Sie

   Create (Erstellen) aus und danach Database (Datenbank).
2. Geben Sie einen Database name (Datenbanknamen) ein.
3. (Optional) Wählen Sie Users and groups (Benutzer und Gruppen) und dort einen Database user (Datenbankbenutzer) aus.
4. (Optional) Sie können die Datenbank aus einem Datashare oder AWS Glue Data Catalog erstellen. Weitere Informationen zu AWS Glue finden Sie unter Was ist AWS Glue? im AWS Glue Entwicklerhandbuch.
   - (Optional) Wählen Sie Mit einem Datashare erstellen aus und klicken Sie auf Einen Datashare auswählen. Die Liste enthält Producer-Datashares, mit denen ein Consumer-Datashare im aktuellen Cluster oder in der aktuellen Arbeitsgruppe erstellt werden kann.
   - (Optional) Wählen Sie Erstellen mit AWS Glue Data Catalog und wählen Sie eine AWS Glue-Datenbank aus. Geben Sie im Datenkatalogschema den Namen ein, der für das Schema verwendet wird, wenn auf die Daten in einem dreiteiligen Namen (database.schema.table) verwiesen wird.
5. Wählen Sie Datenbank erstellen aus.

   Die neue Datenbank wird in der Baumansicht angezeigt.

   Wenn Sie den optionalen Schritt zum Abfragen einer Datenbank auswählen, die aus einem Datashare erstellt wurde, stellen Sie eine Verbindung mit einer Amazon-Redshift-Datenbank im Cluster oder in der Arbeitsgruppe her (z. B. die Standarddatenbank `dev`). Verwenden Sie dabei die dreiteilige Notation (database.schema.table), die auf den Datenbanknamen verweist, den Sie beim Auswählen der Option Mit einem Datashare erstellen erstellt haben. Die Datashare-Datenbank ist auf der Editor-Registerkarte des Abfrage-Editors v2 aufgeführt, jedoch nicht für eine direkte Verbindung aktiviert.

   Wenn Sie den optionalen Schritt zur Abfrage einer Datenbank wählen, die aus einer erstellt wurde AWS Glue Data Catalog, stellen Sie eine Verbindung zu Ihrer Amazon Redshift Redshift-Datenbank im Cluster oder in der Arbeitsgruppe her (z. B. die Standarddatenbank`dev`) und verwenden Sie die dreiteilige Notation (database.schema.table), die auf den Datenbanknamen verweist, den Sie erstellt haben, als Sie Create using ausgewählt haben, auf das Schema AWS Glue Data Catalog, das Sie in Data catalog schema benannt haben, und auf die Tabelle in. AWS Glue Data CatalogÄhnlich wie:

```
SELECT * FROM glue-database.glue-schema.glue-table
```

> **Note**
>
> Vergewissern Sie sich, dass Sie mithilfe der Verbindungsmethode Temporäre Anmeldeinformationen mit Ihrer IAM-Identität mit der Standarddatenbank verbunden sind und dass Ihren IAM-Anmeldeinformationen Nutzungsrechte für die AWS Glue Datenbank gewährt wurden.
>
> ```
> GRANT USAGE ON DATABASE glue-database to "IAM:MyIAMUser"
> ```

Die AWS Glue Datenbank ist auf der Registerkarte des Abfrage-Editors v2 aufgeführt, sie ist jedoch nicht für eine direkte Verbindung aktiviert.

Weitere Informationen zum Abfragen von finden Sie unter Arbeiten mit von Lake Formation verwalteten Datenfreigaben als Verbraucher und Arbeiten mit von Lake Formation verwalteten Datenfreigaben als Produzent im Amazon Redshift Database Developer Guide. AWS Glue Data Catalog

Beispiel für das Erstellen einer Datenbank als Datashare-Consumer

Das folgende Beispiel beschreibt ein bestimmtes Szenario, das verwendet wurde, um mithilfe des Abfrage-Editors v2 eine Datenbank aus einem Datashare zu erstellen. Sehen Sie sich dieses Szenario an, um zu erfahren, wie Sie aus einem Datashare in Ihrer Umgebung eine Datenbank erstellen können. Dieses Szenario verwendet zwei Cluster, `cluster-base` (der Producer-Cluster) und `cluster-view` (der Consumer-Cluster).

1. Verwenden Sie die Amazon-Redshift-Konsole, um einen Datashare für die Tabelle `category2` im Cluster `cluster-base` zu erstellen. Der Producer-Datashare heißt `datashare_base`.

   Weitere Informationen zum Erstellen von Datashares finden Sie unter Freigeben von Daten über Cluster in Amazon Redshift im Datenbankentwicklerhandbuch zu Amazon Redshift.
2. Verwenden Sie die Amazon-Redshift-Konsole, um einen Datashare `datashare_base` als Consumer für die Tabelle `category2` im Cluster `cluster-view` zu erstellen.

3. Sehen Sie sich das Strukturansichtsfenster im Abfrage-Editor v2 an, das die Hierarchie von `cluster-base` anzeigt als:

   - Cluster: `cluster-base`
     - Datenbank: `dev`
       - Schema: `public`
         - Tabellen: `category2`

4. Wählen Sie Create (Erstellen) aus und danach Database (Datenbank).

5. Geben Sie `see_datashare_base` als Datenbankname ein.

6. Wählen Sie Mit einem Datashare erstellen aus und klicken Sie auf Einen Datashare auswählen. Wählen Sie `datashare_base` als Quelle der Datenbank aus, die Sie erstellen.

   Das Strukturansichtsfenster im Abfrage-Editor v2 zeigt die Hierarchie von `cluster-view` an als:

   - Cluster: `cluster-view`
     - Datenbank: `see_datashare_base`
       - Schema: `public`
         - Tabellen: `category2`

7. Wenn Sie die Daten abfragen, stellen Sie eine Verbindung mit der Standarddatenbank des Clusters `cluster-view` (in der Regel `dev`) her, aber verweisen Sie auf die Datashare-Datenbank `see_datashare_base` in Ihrem SQL-Code.

   > **Note**
   >
   > In der Editoransicht des Abfrage-Editors v2 ist der ausgewählte Cluster `cluster-view`. Die ausgewählte Datenbank ist `dev`. Die `see_datashare_base`-Datenbank ist aufgeführt, jedoch nicht für eine direkte Verbindung aktiviert. Sie wählen die `dev`-Datenbank aus und verweisen auf `see_datashare_base` in dem SQL-Code, den Sie ausführen.

```
SELECT * FROM "see_datashare_base"."public"."category2";
```

Die Abfrage ruft Daten aus dem Datashare `datashare_base` im Cluster `cluster_base` ab.

Beispiel für das Erstellen einer Datenbank aus einem AWS Glue Data Catalog

Das folgende Beispiel beschreibt ein bestimmtes Szenario, das verwendet wurde, um eine Datenbank AWS Glue Data Catalog mithilfe eines Abfrage-Editors v2 zu erstellen. Sehen Sie sich dieses Szenario an, um zu erfahren, wie Sie eine Datenbank aus einer AWS Glue Data Catalog in Ihrer Umgebung erstellen können. Dieses Szenario verwendet einen Cluster `cluster-view`, der die von Ihnen erstellte Datenbank enthalten soll.

1. Wählen Sie Create (Erstellen) aus und danach Database (Datenbank).
2. Geben Sie `data_catalog_database` als Datenbankname ein.
3. Wählen Sie Create using a AWS Glue Data Catalog und wählen Sie Choose an AWS Glue database aus. Wählen Sie `glue_db` als Quelle der Datenbank aus, die Sie erstellen.

   Wählen Sie Datenkatalogschema aus und geben Sie `myschema` als Schemaname ein, der in dreiteiliger Notation verwendet werden soll.

   Das Strukturansichtsfenster im Abfrage-Editor v2 zeigt die Hierarchie von `cluster-view` an als:

   - Cluster: `cluster-view`
     - Datenbank: `data_catalog_database`
       - Schema: `myschema`
         - Tabellen: `category3`
4. Wenn Sie die Daten abfragen, stellen Sie eine Verbindung mit der Standarddatenbank des Clusters `cluster-view` (in der Regel `dev`) her, aber verweisen Sie auf die Datenbank `data_catalog_database` in Ihrem SQL-Code.

> **Note**
>
> In der Editoransicht des Abfrage-Editors v2 ist der ausgewählte Cluster `cluster-view`. Die ausgewählte Datenbank ist `dev`. Die `data_catalog_database`-Datenbank ist aufgeführt, jedoch nicht für eine direkte Verbindung aktiviert. Sie wählen die `dev`-Datenbank aus und verweisen auf `data_catalog_database` in dem SQL-Code, den Sie ausführen.

```
SELECT * FROM "data_catalog_database"."myschema"."category3";
```

Die Abfrage ruft Daten ab, die von AWS Glue Data Catalog katalogisiert sind.

Erstellen von Schemata

Sie können den Abfrage-Editor v2 verwenden, um Schemata in Ihrem Cluster oder Ihrer Arbeitsgruppe zu erstellen.

Ein Schema erstellen

Weitere Informationen über Schemata finden Sie unter Schemata im Datenbankentwicklerhandbuch zu Amazon Redshift.

1. Wählen Sie

   Create (Erstellen) aus und danach Schema.
2. Geben Sie einen Schema name (Schemennamen) ein.
3. Wählen Sie entweder Local (Lokal) oder External (Extern) für Schema type (Schematyp) aus.

   Weitere Informationen über lokale Schemata finden Sie unter CREATE SCHEMA im Datenbankentwicklerhandbuch zu Amazon Redshift. Weitere Informationen über externe Schemata finden Sie unter CREATE EXTERNAL SCHEMA im Datenbankentwicklerhandbuch zu Amazon Redshift.
4. Wenn Sie External (Extern) auswählen, stehen Ihnen folgende Optionen für ein externes Schema zur Verfügung.

- Glue Data Catalog (Glue-Datenkatalog) – zum Erstellen eines externen Schemas in Amazon Redshift, das auf Tabellen in AWS Glue verweist. Wählen Sie neben der AWS Glue Datenbank auch die dem Cluster zugeordnete IAM-Rolle und die dem Datenkatalog zugeordnete IAM-Rolle aus.
- PostgreSQL – zum Erstellen eines externen Schemas in Amazon Redshift, das auf eine Datenbank verweist, die mit Amazon RDS für PostgreSQL oder mit einer Edition von Amazon Aurora PostgreSQL kompatibel ist. Geben Sie die Verbindungsinformationen für die Datenbank an. Weitere Informationen über Verbundabfragen finden Sie unter Abfragen von Daten mit Verbundabfragen im Datenbankentwicklerhandbuch zu Amazon Redshift.
- MySQL – zum Erstellen eines externen Schemas in Amazon Redshift, das auf eine Datenbank verweist, die mit Amazon RDS für MySQL oder mit einer Edition von Amazon Aurora MySQL kompatibel ist. Geben Sie die Verbindungsinformationen für die Datenbank an. Weitere Informationen über Verbundabfragen finden Sie unter Abfragen von Daten mit Verbundabfragen im Datenbankentwicklerhandbuch zu Amazon Redshift.

5. Wählen Sie Create schema (Schema erstellen) aus.

   Das neue Schema wird in der Baumansicht angezeigt.

Erstellen von Tabellen

Sie können den Abfrage-Editor v2 verwenden, um Tabellen in Ihrem Cluster oder Ihrer Arbeitsgruppe zu erstellen.

Eine Tabelle erstellen

Sie können eine Tabelle basierend auf einer CSV-Datei erstellen, in der Sie jede Spalte der Tabelle angeben bzw. definieren. Weitere Informationen über Tabellen finden Sie unter Gestalten von Tabellen und CREATE TABLE im Datenbankentwicklerhandbuch zu Amazon Redshift.

Wählen Sie Open query in editor (Abfrage im Editor öffnen) aus, um die Anweisung CREATE TABLE anzuzeigen und zu bearbeiten, bevor Sie die Abfrage zum Erstellen der Tabelle ausführen.

1. Klicken Sie auf

   Create (Erstellen) und wählen Sie Table (Tabelle) aus.
2. Wählen Sie ein Schema aus.

3. Geben Sie einen Tabellennamen ein.
4. Wählen Sie

   Add field (Feld hinzufügen), um eine Spalte hinzuzufügen.
5. Verwenden Sie eine CSV-Datei als Vorlage für die Tabellendefinition:

   a. Wählen Sie Load from CSV (Laden aus CSV) aus.

   b. Gehen Sie zum Speicherort der Datei.

      Wenn Sie eine CSV-Datei verwenden, muss die erste Zeile der Datei die Spaltenüberschriften enthalten.

   c. Wählen Sie die Datei und dann Open (Öffnen). Bestätigen Sie, dass die Spaltennamen und Datentypen korrekt sind.
6. Wählen Sie die einzelnen Spalten und die gewünschten Optionen aus:

   - Wählen Sie einen Wert für Encoding (Codierung) aus.
   - Wählen Sie einen Default value (Standardwert) aus.
   - Aktivieren Sie Automatically increment (Automatisch inkrementieren), wenn die Spaltenwerte inkrementiert werden sollen. Geben Sie dann einen Wert für Auto increment seed (Seed automatisch inkrementieren) und Auto increment step (Schritt automatisch inkrementieren) ein.
   - Aktivieren Sie Not NULL (Nicht NULL), wenn die Spalte immer einen Wert enthalten soll.
   - Geben Sie einen Wert für Size (Größe) für die Spalte ein.
   - Aktivieren Sie Primary key (Primärschlüssel), wenn Sie möchten, dass die Spalte ein Primärschlüssel sein soll.
   - Aktivieren Sie Unique key (Einmaliger Schlüssel), wenn Sie möchten, dass die Spalte ein einmaliger Schlüssel sein soll.
7. (Optional) Wählen Sie Table details (Tabellendetails) und dann eine der folgenden Optionen aus:

   - Spalte des Verteilungsschlüssels und deren Stil.
   - Spalte des Sortierschlüssels und deren Stil.
   - Aktivieren Sie Backup, um die Tabelle in Snapshots aufzunehmen.
   - Aktivieren Sie Temporary table (Temporäre Tabelle), um die Tabelle als temporäre Tabelle zu erstellen.

8. Wählen Sie Open query in editor (Abfrage im Editor öffnen) aus, um noch mehr Einstellungen zum Definieren der Tabelle zu treffen, bzw. Create table (Tabelle erstellen), um die Tabelle zu erstellen.

Erstellung von Funktionen

Sie können den Abfrage-Editor v2 verwenden, um Funktionen in Ihrem Cluster oder Ihrer Arbeitsgruppe zu erstellen.

Eine Funktion erstellen

1. Wählen Sie

   Create (Erstellen) aus und dann Function (Funktion).
2. Wählen Sie bei Type entweder SQL oder Python als Typ aus.
3. Wählen Sie einen Wert für Schema aus.
4. Geben Sie bei Name einen Namen für die Funktion ein.
5. Geben Sie bei Volatility den Wert der Volatilität der Funktion ein.
6. Wählen Sie Parameters nach ihren Datentypen in der Reihenfolge der Eingabeparameter.
7. Wählen Sie bei Returns (Rückgabewerte) einen Datentyp aus.
8. Geben Sie den SQL-Programmcode oder den Python-Programmcode für die Funktion ein.
9. Wählen Sie Create (Erstellen) aus.

Weitere Informationen über benutzerdefinierte Funktionen (UDFs) finden Sie unter Erstellen von benutzerdefinierten Funktionen im Datenbankentwicklerhandbuch zu Amazon Redshift.

Abfrage- und Registerkarten-Verlauf anzeigen

Sie können den Abfrage-Verlauf mit dem Abfrage-Editor v2 anzeigen. Im Abfrageverlauf werden nur Abfragen angezeigt, die Sie mit dem Abfrage-Editor v2 ausgeführt haben. Es werden Abfragen angezeigt, die über eine Editor- oder Notebook-Registerkarte ausgeführt wurden. Sie können die angezeigte Liste nach einem Zeitraum filtern, z. B. `This week`, in dem eine Woche als Montag–Sonntag definiert ist. Die Liste der Abfragen ruft gleichzeitig 25 Zeilen mit Abfragen ab, die Ihrem Filter entsprechen. Wählen Sie Load more (Mehr laden) aus, um den nächsten Satz anzuzeigen. Wählen Sie eine Abfrage aus dem Menü Actions (Aktionen) aus. Die verfügbaren Aktionen hängen

davon ab, ob die ausgewählte Abfrage gespeichert wurde. Sie können die folgenden Operationen auswählen:

- View query details (Abfragedetails anzeigen) – zeigt eine Abfragedetailseite mit weiteren Informationen zu der ausgeführten Abfrage an.
- Open query in a new tab (Abfrage in einer neuen Registerkarte öffnen) – öffnet eine neue Editor-Registerkarte und bereitet sie mit der ausgewählten Abfrage vor. Wenn die Verbindung noch besteht, werden der Cluster oder die Arbeitsgruppe und die Datenbank automatisch ausgewählt. Stellen Sie zum Durchführen der Abfrage zunächst sicher, dass der richtige Cluster oder die richtige Arbeitsgruppe und die richtige Datenbank ausgewählt wurden.
- Open source tab (Open-Source-Registerkarte) – wenn die Registerkarte noch geöffnet ist, wird zu der Editor- oder Notebook-Registerkarte navigiert, die die Abfrage bei ihrer Ausführung enthielt. Der Inhalt des Editors oder Notebooks hat sich möglicherweise geändert, nachdem die Abfrage ausgeführt wurde.
- Open saved query (Gespeicherte Abfrage öffnen) – navigiert zur Editor- oder Notebook-Registerkarte und öffnet die Abfrage.

Sie können auch den Verlauf der Abfragen anzeigen, die auf einer Editor-Registerkarte ausgeführt wurden, oder den Verlauf der Abfragen, die auf einer Notebook-Registerkarte ausgeführt wurden. Wenn Sie den Verlauf der Abfragen auf einer Registerkarte anzeigen möchten, wählen Sie Tab history (Registerkartenverlauf) aus. Im Registerkartenverlauf können Sie Folgendes tun:

- Copy query (Abfrage kopieren) – kopiert den SQL-Inhalt der Abfrageversion in die Zwischenablage.
- Open query in a new tab (Abfrage in einer neuen Registerkarte öffnen) – öffnet eine neue Editor-Registerkarte und bereitet sie mit der ausgewählten Abfrage vor. Wenn Sie die Abfrage ausführen möchten, müssen Sie den Cluster oder die Arbeitsgruppe und die Datenbank auswählen.
- View query details (Abfragedetails anzeigen) – zeigt eine Abfragedetailseite mit weiteren Informationen zu der ausgeführten Abfrage an.

Überlegungen zur Arbeit mit dem Abfrage-Editor v2

Beachten Sie Folgendes, wenn Sie mit dem Abfrage-Editor v2 arbeiten.

- Das Abfrageergebnis darf höchstens 5 MB bzw. 100 000 Zeilen groß sein.
- Sie können Abfragen mit bis zu 300 000 Zeichen ausführen.
- Sie können Abfragen mit bis zu 30 000 Zeichen speichern.

- Standardmäßig führt der Abfrage-Editor v2 automatisch einen Commit für jeden einzelnen SQL-Befehl aus, der ausgeführt wird. Wenn eine BEGIN-Anweisung bereitgestellt wird, werden Anweisungen innerhalb des BEGIN-COMMIT- oder BEGIN-ROLLBACK-Blocks als einzelne Transaktion ausgeführt. Weitere Informationen zu Transaktionen finden Sie unter BEGIN im Datenbankentwicklerhandbuch zu Amazon Redshift.
- Die maximale Anzahl von Warnungen, die der Abfrage-Editor v2 während der Ausführung einer SQL-Anweisung anzeigt, beträgt `10`. Wenn beispielsweise eine gespeicherte Prozedur ausgeführt wird, werden maximal 10 RAISE-Anweisungen angezeigt.
- Der Abfrage-Editor v2 unterstützt kein IAM`RoleSessionName`, das Kommas (,) enthält. Möglicherweise wird ein Fehler ähnlich dem folgenden angezeigt: Fehlermeldung: „'aroa123456789example:MyText, yourtext' is not a valid value for TagValue - it contains unzulässige Zeichen“ Dieses Problem tritt auf, wenn Sie ein IAM definieren, das ein Komma enthält, und dann den Abfrage-Editor v2 mit dieser IAM-Rolle verwenden`RoleSessionName`.

  Weitere Informationen zu einem IAM finden Sie unter SAML-Attribut im IAM-Benutzerhandbuch. *`RoleSessionName`* RoleSessionName

Ändern von Kontoeinstellungen

Ein Benutzer mit den richtigen IAM-Berechtigungen kann Account settings (Kontoeinstellungen) für andere Benutzer im selben AWS-Konto anzeigen und ändern. Dieser Administrator kann Folgendes anzeigen oder festlegen:

- Die maximale Anzahl gleichzeitiger Datenbankverbindungen pro Benutzer im Konto. Dazu gehören Verbindungen für Isolated sessions (Isolierte Sitzungen). Wenn Sie diesen Wert ändern, kann es 10 Minuten dauern, bis die Änderung wirksam wird.
- Erlauben Sie Benutzern im Konto, einen gesamten Ergebnissatz aus einem SQL-Befehl in eine Datei zu exportieren.
- Laden und zeigen Sie Beispieldatenbanken mit einigen zugehörigen gespeicherten Abfragen an.
- Geben Sie einen Amazon-S3-Pfad an, der von Kontobenutzern verwendet wird, um Daten aus einer lokalen Datei zu laden.
- Zeigen Sie den ARN des KMS-Schlüssels an, der zum Verschlüsseln von Ressourcen des Abfrage-Editors v2 verwendet wird.

Interaktion mit generativem SQL in Query Editor v2 (Vorschau)

Dies ist die Vorabdokumentation für generatives SQL in Query Editor v2, das sich in der Vorversio n befindet. Sowohl die Dokumentation als auch die Funktion können sich ändern. Wir empfehlen, diese Funktion nur in Test- und nicht in Produktionsumgebungen zu verwenden. Die Bedingungen für Vorversionen finden Sie unter Beta-Service-Teilnahme in den AWS-Servicebedingungen.

Note

Derzeit ist Unterstützung für generatives SQL nur in folgenden AWS-Regionen verfügbar:

- Region USA Ost (Nord-Virginia) (us-east-1)
- Region USA West (Oregon) (us-west-2)

Sie können in Amazon Redshift Query Editor v2 mit der Funktion für generatives SQL von Amazon Q interagieren. Es handelt sich hier um einen Programmierassistenten, der SQL-Anweisungen basierend auf Ihren Aufforderungen und Ihrem Datenbankschema generiert. Dieser Programmierassistent ist verfügbar, während Sie ein Notebook in Query Editor v2 erstellen.

Stellen Sie bei der Interaktion mit generativem SQL spezifische Fragen, iterieren Sie bei komplexen Anforderungen und überprüfen Sie die Richtigkeit der Antworten.

Seien Sie bei Analyseanforderungen in natürlicher Sprache so spezifisch wie möglich, damit der Programmierassistent genau versteht, was Sie benötigen. Anstatt nur nach den Veranstaltungsorten zu fragen, die die meisten Tickets verkauft haben, sollten Sie weitere Details nennen, also beispielsweise nach den Namen/IDs der drei Veranstaltungsorte fragen, die 2008 die meisten Tickets verkauft haben. Verwenden Sie einheitliche Namen für Objekte in Ihrer Datenbank, also beispielsweise die in Ihrer Datenbank definierten Schema-, Tabellen- und Spaltennamen, anstatt auf unterschiedliche Weise auf dasselbe Objekt zu verweisen, da dies den Assistenten verwirren kann.

Unterteilen Sie komplexe Anforderungen in mehrere einfache Anweisungen, die für den Assistenten leichter zu interpretieren sind. Stellen Sie immer wieder Folgefragen, um eine detailliertere Analyse von dem Assistenten zu erhalten. Fragen Sie zum Beispiel zuerst, in welchem Bundesstaat es die meisten Veranstaltungsorte gibt. Fragen Sie dann unter Berücksichtigung der Antwort nach dem beliebtesten Veranstaltungsort in diesem Bundesstaat.

Überprüfen Sie das generierte SQL vor der Ausführung, um die Richtigkeit sicherzustellen. Wenn die generierte SQL-Abfrage Fehler enthält oder nicht Ihrer Absicht entspricht, geben Sie dem Assistenten Anweisungen zur Korrektur, anstatt die gesamte Anforderung neu zu formulieren. Wenn in der Abfrage beispielsweise eine Prädikatklausel für das Jahr fehlt, fordern Sie den Assistenten auf, die Veranstaltungsorte aus dem Jahr 2008 anzugeben.

Überlegungen bei der Interaktion mit generativem SQL

Beachten Sie bei der Arbeit im Chat-Bereich Folgendes:

- Der Administrator von Query Editor v2 für Ihr Konto muss die Chat-Funktion auf der Seite Einstellungen für generatives SQL aktiviert haben.
- Um generatives SQL in Query Editor v2 verwenden zu können, benötigen Sie zusätzlich zu den anderen Berechtigungen, die in der AWS-verwalteten Richtlinie für Query Editor v2 angegeben sind, die Berechtigung `sqlworkbench:GetQSqlRecommendations` in Ihrer IAM-Richtlinie. Weitere Informationen über von AWS verwaltete Richtlinien finden Sie unter Zugreifen auf den Abfrage-Editor v2.
- Ihre Fragen müssen auf Englisch verfasst werden.
- Ihre Fragen müssen sich auf die verbundene Datenbank in Ihrem Cluster oder Ihrer Arbeitsgruppe beziehen. Um Fehler wegen eines leeren Zustands zu vermeiden, sollte die Datenbank mindestens eine Tabelle und einige Daten enthalten.
- Ihre Fragen müssen sich auf Daten beziehen, die in der verbundenen Datenbank gespeichert sind. Sie können nicht auf ein externes Schema verweisen. Weitere Informationen zu den unterstützten Schemas finden Sie unter Erstellen eines Schemas im Datenbankentwicklerhandbuch zu Amazon Redshift.
- Bei allen Fragen, die bewirken, dass SQL die verbundene Datenbank ändert, kann es zu einer Warnung kommen.
- Generative KI-Technologie ist neu und die Antworten können Fehler enthalten, die manchmal als Halluzinationen bezeichnet werden. Testen und überprüfen Sie den gesamten Code auf Fehler und Schwachstellen, bevor Sie ihn in Ihrer Umgebung oder Ihrem Workload verwenden.
- Sie können die Empfehlungen verbessern, indem Sie die von anderen Benutzern in Ihrem Konto ausgeführten SQL-Abfragen gemeinsam nutzen. Ihr Kontoadministrator kann die folgenden SQL-Befehle ausführen, um Zugriff auf den Abfrageverlauf des Kontos zu gewähren.

```
GRANT ROLE SYS:MONITOR to "IAMR:role-name";
GRANT ROLE SYS:MONITOR to "IAM:user-name";
```

```
GRANT ROLE SYS:MONITOR to "database-username";
```

Weitere Informationen zu `SYS:MONITOR` finden Sie unter Systemdefinierte Amazon-Redshift-Rollen im Datenbankentwicklerhandbuch zu Amazon Redshift.

- Ihre Daten sind sicher und privat. Ihre Daten werden nicht kontoübergreifend gemeinsam genutzt. Ihre Abfragen, Daten und Datenbankschemas werden nicht zum Trainieren eines Basismodells (FM) für generative KI verwendet. Ihre Eingaben werden als kontextbezogene Aufforderungen an das FM nur zur Beantwortung Ihrer Fragen verwendet.

Verwendung von generativem SQL

Nach Konfiguration der richtigen Berechtigungen können Sie bei der Arbeit mit einem Notebook in Query Editor v2 ein Symbol auswählen, um eine Konversation zu starten.

So interagieren Sie mit dem generativen SQL-Chat in Query Editor v2, um SQL zu generieren

1. Öffnen Sie auf der Registerkarte Editor von Query Editor v2 ein Notebook.
2. Wählen Sie das Symbol für generatives SQL

   aus und folgen Sie dann den Anweisungen, um Ihre Fragen an das generative SQL von Amazon Redshift Query Editor v2 im Chat-Bereich zu stellen.

   Sie stellen Fragen in einem Eingabeaufforderungsfeld und Query Editor v2 antwortet mit SQL-Vorschlägen. Alle aufgetretenen Fehler werden Ihnen im Chat-Bereich zurückgemeldet.
3. Wählen Sie Zu Notebook hinzufügen aus, um Ihrem Notebook eine Markdown-Zelle mit Ihrer Aufforderung und eine SQL-Zelle mit dem vorgeschlagenen SQL hinzuzufügen.
4. (Optional) Wählen Sie SQL neu generieren aus, um eine andere Antwort für dieselbe Aufforderung zu generieren. Sie können SQL neu generieren einmal für die aktuelle Aufforderung auswählen.
5. (Optional) Wählen Sie im generativen SQL-Chatbereich das Symbol für Mehr

   und anschließend Datenbank aktualisieren aus, um die Metadaten zu aktualisieren, die Ihre verbundene Datenbank beschreiben. Diese Metadaten umfassen die Definitionen von Schemas, Tabellen und Spalten in Ihrer Datenbank.

Aktualisieren der Einstellungen für generatives SQL als Administrator

Ein Benutzer mit den richtigen IAM-Berechtigungen kann die Einstellungen für generatives SQL für andere Benutzer in demselben AWS-Konto anzeigen und ändern. Dieser Administrator muss zusätzlich zu anderen in der AWS-verwalteten Richtlinie für Query Editor v2 angegebenen Berechtigungen über die Berechtigung `sqlworkbench:UpdateAccountQSqlSettings` in seiner IAM-Richtlinie verfügen. Weitere Informationen über verwaltete Richtlinien finden Sie unter Für die Verwendung des Abfrage-Editors v2 erforderliche Berechtigungen .

So kann ein Administrator den generativen SQL-Chat für alle Benutzer in dem Konto aktivieren

1. Wählen Sie das Symbol für Einstellungen

   aus, um ein Menü mit den verschiedenen Einstellungsbildschirmen anzuzeigen.
2. Wählen Sie dann das Symbol für Einstellungen für generatives SQL

   aus, um die Seite mit den Einstellungen für generatives SQL anzuzeigen.
3. Wählen Sie Generatives SQL aus, um die Funktion für generatives SQL für Benutzer in dem Konto zu aktivieren.

Beispiel für die Verwendung der Amazon-Q-Funktion für generatives SQL mit den TICKIT-Daten

Um effiziente Aufforderungen zum Generieren von SQL zu erstellen, müssen Sie sich mit Ihrem Datenbankschema und Ihren Daten vertraut machen. Die TICKIT-Daten umfassen sieben Tabellen, zwei Faktentabellen und fünf Dimensionen. Die Beispieldaten enthalten Aufzeichnungen über Verkäufe an Besucher von Unterhaltungsveranstaltungen, die im Jahr 2008 stattfanden. Weitere Informationen über das TICKIT-Datenschema finden Sie unter Beispieldatenbank im Datenbankentwicklerhandbuch zu Amazon Redshift. Sie können die TICKIT-Daten mit verschiedenen Methoden in der Amazon Redshift-Konsole und in Query Editor v2 in eine Datenbank laden. Query Editor v2 bietet eine Methode zum Laden von TICKIT-Daten in die Datenbank `sample_data_dev`. Weitere Informationen finden Sie unter Laden von Beispieldaten. Query Editor v2 bietet auch Beispielaufforderungen für die TICKIT-Daten. Das folgende Szenario beschreibt eine Konversation mit generativem SQL zum Generieren von SQL zu den TICKIT-Beispieldaten. In diesem Szenario

sind die TICKIT-Beispieldaten bereits in einer Datenbank `dev` in einem Amazon-Redshift-Cluster erstellt.

> **Note**
>
> Dieses Beispiel dient der Veranschaulichung einer Konversation. Es kann sein, dass die Antworten des generativen SQL nicht mit den Ergebnissen übereinstimmen, die Sie bei Verwendung derselben Aufforderungen erhalten.

Beispiel für eine Konversation mit generativem SQL in Query Editor v2

1. Stellen Sie im Editor eine Verbindung zu einem Cluster oder einer Arbeitsgruppe her, die die TICKIT-Beispieldaten enthält.
2. Erstellen Sie ein leeres Notebook und wählen Sie das Symbol für generatives SQL , um den Chat-Bereich zu öffnen.
3. Geben Sie die folgende Aufforderung ein, um SQL zur Überprüfung der Anzahl der Datensätze in der Tabelle `VENUE` zu generieren:

   ```
   How many venues are there?
   ```

   ```
   SELECT
     COUNT(*) AS num_venues
   FROM
     tickit.venue
   ```

   Wählen Sie Zu Notebook hinzufügen aus, um dem geöffneten Notebook zwei Zellen hinzuzufügen. Eine Markdown-Zelle „How many venues are there?“ und eine mit dem generierten SQL.

   Wählen Sie in der SQL-Zelle Ausführen aus, um das Ergebnis zu erhalten:

   ```
   count
   ------
   202
   ```

4. Um nach einer anderen Version von SQL zu fragen, wählen Sie SQL neu generieren aus. Sie erhalten die folgende Antwort:

```
SELECT
  venuestate,
  COUNT(*) AS num_venues
FROM
  tickit.venue
GROUP BY
  venuestate
```

Wählen Sie Zu Notebook hinzufügen aus, um dem geöffneten Notebook zwei weitere Zellen hinzuzufügen. Eine Markdown-Zelle „How many venues are there?“ und eine mit dem generierten SQL.

Wählen Sie in der SQL-Zelle die Option Ausführen aus, um das Ergebnis, eine Auflistung der Bundesstaaten der Veranstaltungsorte nach Anzahl, zu erhalten.

```
venuestate num_venues
----------------------
MA         4
OH         8
MI         5
...
```

5. Der generative SQL-Assistent kann Annahmen darüber treffen, was Sie fragen. Obwohl es in der Datenbank keine Widgets gibt, können Sie dennoch fragen. In diesem Fall erhalten Sie die Meldung, dass kein SQL generiert werden konnte.

```
How many widgets are there?
```

```
I was not able to generate any SQL
```

6. Wenn Sie mehr über Ihre Datenbank erfahren, können Sie spezifischere Fragen zum Generieren von SQL stellen. Sie wissen beispielsweise, dass die Datenbank Verkaufsdaten zu mehreren Monaten im Jahr 2008 enthält. Geben Sie die folgende Aufforderung ein, um SQL zur Ermittlung der Anzahl der Verkäufe im November 2008 zu generieren:

```
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
```

Wählen Sie Zu Notebook hinzufügen aus, um dem geöffneten Notebook zwei Zellen hinzuzufügen. Eine Markdown-Zelle „How many sales were there in November 2008?“ und eine mit dem generierten SQL.

Wählen Sie in der SQL-Zelle Ausführen aus, um das Ergebnis zu erhalten:

```
num_sales
-----
0
```

Sie erkennen, dass dies nicht das Ergebnis ist, das Sie erwartet haben.

7. Sie stellen fest, dass das Prädikat `date.month='November'` erwartet, dass der Monat in der DATE-Tabelle durch eine Abkürzung des Monatsnamens dargestellt wird. Sie ändern das Prädikat in `d.month='NOV'` und führen das SQL erneut aus.

```
SELECT
  COUNT(*)
FROM
  sales
  JOIN date ON sales.dateid = date.dateid
WHERE
  date.month = 'NOV'
  AND date.year = 2008
```

Wählen Sie in der SQL-Zelle Ausführen aus, um neue Ergebnisse zu erhalten.

```
count
-----
14261
```

8. Wenn Sie eine Frage stellen, die versucht, die verbundene Datenbank zu ändern, wird eine Warnmeldung zusammen mit dem empfohlenen SQL zurückgegeben. Geben Sie die folgende Aufforderung ein, um SQL zum Einfügen von Daten in eine Tabelle zu generieren:

```
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.
```

Wenn Sie Zu Notebook hinzufügen auswählen, um dem geöffneten Notebook zwei Zellen hinzuzufügen und das SQL auszuführen, schlägt das SQL fehl.

```
ERROR: syntax error at or near "," Position: 132 [ErrorId:
 1-6546764a-011df2691778846219ce6ec2]
```

In diesem Szenario wurden nur einige grundlegende Möglichkeiten zur Interaktion mit dem generativen SQL in Query Editor v2 veranschaulicht. Sie können noch mehr mit dieser generativen KI-Technologie experimentieren, um leichter mit der Erstellung von SQL zur Abfrage Ihrer Datenbank beginnen zu können.

Laden von Daten in eine Datenbank

Mit dem Abfrage-Editor v2 können Sie Daten in eine Datenbank in einem Amazon-Redshift-Cluster oder einer Amazon-Redshift-Arbeitsgruppe laden.

Laden von Beispieldaten

Der Abfrage-Editor v2 umfasst Beispieldaten und -Notebooks, die in eine Beispieldatenbank und ein entsprechendes Schema geladen werden können.

Um Beispieldaten zu laden, wählen Sie das

-

Symbol aus, das den zu ladenden Beispieldaten zugeordnet ist. Der Abfrage-Editor v2 lädt dann die Daten in ein Schema in der Datenbank `sample_data_dev` und erstellt einen Ordner mit gespeicherten Notebooks in Ihrem Ordner Notebooks.

Die folgenden Beispieldatensätze sind verfügbar.

Tickit

In den meisten Beispielen der Amazon-Redshift-Dokumentation werden Beispieldaten namens `tickit` verwendet. Diese Daten umfassen sieben Tabellen, zwei Faktentabellen und fünf Dimensionen. Wenn Sie diese Daten laden, wird das Schema `tickit` mit Beispieldaten aktualisiert. Weitere Informationen über `tickit`-Daten finden Sie unter Beispieldatenbank im Datenbankentwicklerhandbuch zu Amazon Redshift.

tpch

Diese Daten werden für ein Benchmarking zur Entscheidungsunterstützung verwendet. Wenn Sie diese Daten laden, wird das Schema `tpch` mit Beispieldaten aktualisiert. Weitere Informationen zu `tpch`-Daten finden Sie unter TPC-H.

tpcds

Diese Daten werden für ein Benchmarking zur Entscheidungsunterstützung verwendet. Wenn Sie diese Daten laden, wird das Schema `tpcds` mit Beispieldaten aktualisiert. Weitere Informationen zu `tpcds`-Daten finden Sie unter TPC-DS.

Daten aus Amazon S3 laden

Sie können Amazon-S3-Daten in eine vorhandene oder neue Tabelle laden.

Daten in eine vorhandene Tabelle laden

Der Abfrage-Editor v2 nutzt den Befehl COPY, um Daten aus Amazon S3 zu laden. Der Befehl COPY wird im Assistenten „Load data“ (Daten laden) des Abfrage-Editors v2 generiert und verwendet. Er unterstützt viele Parameter, die für die COPY-Befehlssyntax zum Kopieren aus Amazon S3 verfügbar sind. Weitere Informationen über den Befehl COPY und seine Optionen zum Laden von Daten aus Amazon S3 finden Sie unter COPY aus dem Amazon-Simple-Storage-Service im Datenbankentwicklerhandbuch zu Amazon Redshift.

1. Vergewissern Sie sich, dass die Tabelle bereits in der Datenbank erstellt wurde, in die Sie Daten laden möchten.
2. Vergewissern Sie sich in der Strukturansicht von Query Editor v2, dass Sie mit der Zieldatenbank verbunden sind, bevor Sie fortfahren. Sie können über das Kontextmenü (rechte Maustaste) eine Verbindung zu dem Cluster oder der Arbeitsgruppe herstellen, in den/die die Daten geladen werden.

   Wählen Sie Load data (Daten laden) aus.
3. Wählen Sie für Datenquelle die Option Aus S3-Bucket laden aus.
4. Wählen Sie unter S3 URIs die Option Browse S3 (S3 durchsuchen) aus, um nach dem Amazon S3 Bucket zu suchen, der die zu ladenden Daten enthält.
5. Wenn sich der angegebene Amazon-S3-Bucket nicht in derselben AWS-Region wie die Ziel-Tabelle befindet, wählen Sie den S3-Dateispeicherort (S3 file location) für die AWS-Region aus, in der die Daten gespeichert sind.
6. Wählen Sie This file is a manifest file (Dies ist eine Manifestdatei), wenn die Amazon-S3-Datei tatsächlich ein Manifest ist, das mehrere Amazon-S3-Bucket-URIs enthält.
7. Wählen Sie das File format (Dateiformat) für die hochzuladende Datei. Die unterstützten Datenformate sind CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET und ORC. Abhängig vom angegebenen Dateiformat können Sie die jeweiligen File options (Dateioptionen) auswählen. Sie können auch Data is encrypted (Daten sind verschlüsselt) auswählen, wenn die Daten verschlüsselt sind. Geben Sie dann den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels ein, mit dem die Daten verschlüsselt werden.

Wenn Sie CSV oder DELIMITER auswählen, können Sie auch das Trennzeichen auswählen und angeben, ob Sie die Kopfzeilen ignorieren möchten, wenn es sich bei der angegebenen Anzahl von Zeilen tatsächlich um Spaltennamen und nicht um zu ladende Daten handelt.

8. Wählen Sie eine Komprimierungsmethode aus, mit der Ihre Datei komprimiert werden soll. Die Standardeinstellung ist keine Komprimierung.
9. (Optional) In den Advanced settings (erweiterten Einstellungen) finden Sie verschiedene Data conversion parameters (Datenkonvertierungsparameter) und Load operations (Ladeoperationen). Geben Sie diese Informationen nach Bedarf für Ihre Datei ein.

   Weitere Informationen zu Datenkonvertierung und Datenladeparametern finden Sie unter Data conversion parameters (Datenkonvertierungsparameter) und Data load operations (Datenladeoperationen) im Amazon Redshift Database Developer Guide (Datenbankleitfaden zu Amazon Redshift).
10. Wählen Sie Next (Weiter).
11. Wählen Sie Bestehende Tabelle laden aus.
12. Bestätigen oder wählen Sie den Standort der Zieltabelle (Target table), einschließlich Cluster oder Arbeitsgruppe, Datenbank, Schema und Name der Tabelle, in die die Daten geladen werden.
13. Wählen Sie eine IAM role (IAM-Rolle) aus, die über die erforderlichen Berechtigungen zum Laden von Daten aus Amazon S3 verfügt.
14. (Optional) Wählen Sie Spaltennamen aus, um sie in das Feld Column mapping (Spaltenzuordnung) einzugeben, damit die Spalten in der Reihenfolge der Eingabedatendatei zugeordnet werden.
15. Wählen Sie Load data (Daten laden), um das Laden der Daten zu starten.

    Nach Abschluss des Ladens wird der Abfrage-Editor mit dem generierten COPY-Befehl angezeigt, der zum Laden Ihrer Daten verwendet wurde. Das Result (Ergebnis) von COPY wird angezeigt. Bei Erfolg können Sie nun mithilfe von SQL Daten aus der geladenen Tabelle auswählen. Wenn ein Fehler auftritt, stellen Sie eine Systemansicht-Abfrage (STL_LOAD_ERRORS), um weitere Details zu erfahren. Informationen über Fehler beim Befehl COPY finden Sie unter STL_LOAD_ERRORS im Datenbankentwicklerhandbuch zu Amazon Redshift.

Wenn Sie Daten in eine neue Tabelle laden, erstellt Query Editor v2 zuerst die Tabelle in der Datenbank und lädt die Daten dann als separate Aktionen in demselben Workflow.

So laden Sie Daten in eine neue Tabelle

Der Abfrage-Editor v2 nutzt den Befehl COPY, um Daten aus Amazon S3 zu laden. Der Befehl COPY wird im Assistenten „Load data“ (Daten laden) des Abfrage-Editors v2 generiert und verwendet. Er unterstützt viele Parameter, die für die COPY-Befehlssyntax zum Kopieren aus Amazon S3 verfügbar sind. Weitere Informationen über den Befehl COPY und seine Optionen zum Laden von Daten aus Amazon S3 finden Sie unter COPY aus dem Amazon-Simple-Storage-Service im Datenbankentwicklerhandbuch zu Amazon Redshift.

1. Vergewissern Sie sich in der Strukturansicht von Query Editor v2, dass Sie mit der Zieldatenbank verbunden sind, bevor Sie fortfahren. Sie können über das Kontextmenü (rechte Maustaste) eine Verbindung zu dem Cluster oder der Arbeitsgruppe herstellen, in den/die die Daten geladen werden.

   Wählen Sie

   Load data (Daten laden) aus.
2. Wählen Sie für Datenquelle die Option Aus S3-Bucket laden aus.
3. Wählen Sie unter S3 URIs die Option Browse S3 (S3 durchsuchen) aus, um nach dem Amazon S3 Bucket zu suchen, der die zu ladenden Daten enthält.
4. Wenn sich der angegebene Amazon-S3-Bucket nicht in derselben AWS-Region wie die Ziel-Tabelle befindet, wählen Sie den S3-Dateispeicherort (S3 file location) für die AWS-Region aus, in der die Daten gespeichert sind.
5. Wählen Sie This file is a manifest file (Dies ist eine Manifestdatei), wenn die Amazon-S3-Datei tatsächlich ein Manifest ist, das mehrere Amazon-S3-Bucket-URIs enthält.
6. Wählen Sie das File format (Dateiformat) für die hochzuladende Datei. Die unterstützten Datenformate sind CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET und ORC. Abhängig vom angegebenen Dateiformat können Sie die jeweiligen File options (Dateioptionen) auswählen. Sie können auch Data is encrypted (Daten sind verschlüsselt) auswählen, wenn die Daten verschlüsselt sind. Geben Sie dann den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels ein, mit dem die Daten verschlüsselt werden.

   Wenn Sie CSV oder DELIMITER auswählen, können Sie auch das Trennzeichen auswählen und angeben, ob Sie die Kopfzeilen ignorieren möchten, wenn es sich bei der angegebenen Anzahl von Zeilen tatsächlich um Spaltennamen und nicht um zu ladende Daten handelt.

7. Wählen Sie eine Komprimierungsmethode aus, mit der Ihre Datei komprimiert werden soll. Die Standardeinstellung ist keine Komprimierung.
8. (Optional) In den Advanced settings (erweiterten Einstellungen) finden Sie verschiedene Data conversion parameters (Datenkonvertierungsparameter) und Load operations (Ladeoperationen). Geben Sie diese Informationen nach Bedarf für Ihre Datei ein.

   Weitere Informationen zu Datenkonvertierung und Datenladeparametern finden Sie unter Data conversion parameters (Datenkonvertierungsparameter) und Data load operations (Datenladeoperationen) im Amazon Redshift Database Developer Guide (Datenbankleitfaden zu Amazon Redshift).
9. Wählen Sie Next (Weiter).
10. Wählen Sie Neue Tabelle laden aus.

    Die Tabellenspalten werden aus den Eingabedaten abgeleitet. Sie können die Definition des Tabellenschemas ändern, indem Sie Spalten und Tabellendetails hinzufügen. Um zum abgeleiteten Tabellenschema von Query Editor v2 zurückzukehren, wählen Sie Auf Standardwerte zurücksetzen aus.
11. Bestätigen oder wählen Sie den Standort der Zieltabelle, einschließlich Cluster oder Arbeitsgruppe, Datenbank und Schema, in die die Daten geladen werden. Geben Sie einen Namen für die zu erstellende Tabelle ein.
12. Wählen Sie eine IAM role (IAM-Rolle) aus, die über die erforderlichen Berechtigungen zum Laden von Daten aus Amazon S3 verfügt.
13. Wählen Sie Tabelle erstellen aus, um die Tabelle unter Verwendung der angezeigten Definition zu erstellen.

    Eine Zusammenfassung der Tabellendefinition zur Überprüfung wird angezeigt. Die Tabelle wird in der Datenbank erstellt. Um die Tabelle später zu löschen, führen Sie einen SQL-Befehl DROP TABLE aus. Weitere Informationen finden Sie unter DROP TABLE im Datenbankentwicklerhandbuch zu Amazon Redshift.
14. Wählen Sie Load data (Daten laden), um das Laden der Daten zu starten.

    Nach Abschluss des Ladens wird der Abfrage-Editor mit dem generierten COPY-Befehl angezeigt, der zum Laden Ihrer Daten verwendet wurde. Das Result (Ergebnis) von COPY wird angezeigt. Bei Erfolg können Sie nun mithilfe von SQL Daten aus der geladenen Tabelle auswählen. Wenn ein Fehler auftritt, stellen Sie eine Systemansicht-Abfrage (STL_LOAD_ERRORS), um weitere Details zu erfahren. Informationen über Fehler beim Befehl

COPY finden Sie unter STL_LOAD_ERRORS im Datenbankentwicklerhandbuch zu Amazon Redshift.

Laden von Daten aus einer lokalen Datei – Einrichtung und Workflow

Sie können Daten aus einer lokalen Datei in eine vorhandene oder neue Tabelle laden.

Einrichtung durch den Administrator für das Laden von Daten aus einer lokalen Datei

Ihr Administrator für den Abfrage-Editor v2 muss den gemeinsamen Amazon-S3-Bucket im Fenster Account settings (Kontoeinstellungen) angeben. Die Kontobenutzer müssen mit den richtigen Berechtigungen konfiguriert werden.

- Erforderliche IAM-Berechtigungen: Die Benutzer, die die Funktion zum Laden von Daten aus einer lokalen Datei verwenden sollen, müssen über die Berechtigungen `s3:ListBucket`, `s3:GetBucketLocation`, `s3:putObject`, `s3:getObject` und `s3:deleteObject` verfügen. *`optional-prefix`* kann angegeben werden, um die Verwendung dieses Buckets im Zusammenhang mit dem Abfrage-Editor v2 auf Objekte mit diesem Präfix zu beschränken. Diese Option könnten Sie verwenden, wenn Sie denselben Amazon-S3-Bucket auch für andere Zwecke als den Abfrage-Editor v2 verwenden. Weitere Informationen zu Buckets und Präfixen finden Sie unter Verwalten des Benutzerzugriffs auf bestimmte Ordner im Benutzerhandbuch zu Amazon Simple Storage Service. Um sicherzustellen, dass kein benutzerübergreifender Datenzugriff zulässig ist, empfehlen wir dem Administrator für Query Editor v2, eine Amazon-S3-Bucket-Richtlinie zu verwenden, um den Objektzugriff auf der Grundlage von `aws:userid` einzuschränken. Im folgenden Beispiel werden Amazon-S3-Berechtigungen für einen *`<staging-bucket-name>`* gewährt. Dabei besteht nur Lese-/Schreibzugriff auf Amazon-S3-Objekte mit dem Präfix `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}/*"
            ]
        }
    ]
}
```

- Datentrennung: Die Benutzer sollten keinen Zugriff auf die Daten der anderen Benutzer haben (auch nicht kurzzeitig). Beim Laden aus einer lokalen Datei wird der Amazon-S3-Staging-Bucket verwendet, der vom Administrator für den Abfrage-Editor v2 eingerichtet wurde. Konfigurieren Sie die Bucket-Richtlinie für den Staging-Bucket, um für eine Datentrennung zwischen Benutzern zu sorgen. Das folgende Beispiel zeigt eine Bucket-Richtlinie, die die Daten der Benutzer von *<staging-bucket-name>* trennt.

```
{
 "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}/*"
            ]
         }
    ]
}
```

Laden von Daten aus einer lokalen Datei

So laden Sie Daten aus einer lokalen Datei in eine vorhandene Tabelle

Ihr Administrator für Query Editor v2 muss den gemeinsamen Amazon-S3-Bucket im Fenster Kontoeinstellungen angeben. Query Editor v2 lädt die lokale Datei automatisch in einen von Ihrem Konto verwendeten gemeinsamen Amazon-S3-Bucket hoch und verwendet dann den Befehl COPY zum Laden von Daten. Der Befehl COPY wird im Fenster „Load local file“ (Lokale Datei laden) des Abfrage-Editors v2 generiert und ausgeführt. Er unterstützt viele Parameter, die für die COPY-Befehlssyntax zum Kopieren aus Amazon S3 verfügbar sind. Weitere Informationen über den Befehl COPY und seine Optionen zum Laden von Daten aus Amazon S3 finden Sie unter COPY aus Amazon S3 im Datenbankentwicklerhandbuch zu Amazon Redshift.

1. Vergewissern Sie sich, dass die Tabelle bereits in der Datenbank erstellt wurde, in die Sie Daten laden möchten.
2. Vergewissern Sie sich in der Strukturansicht des Abfrageeditors v2, dass Sie mit der Zieldatenbank verbunden sind. Sie können über das Kontextmenü (rechte Maustaste) eine Verbindung zu dem Cluster oder der Arbeitsgruppe herstellen, in den/die die Daten geladen werden.
3. Wählen Sie Load data (Daten laden) aus.
4. Wählen Sie für Data source (Datenquelle) die Option Load from local file (Aus lokaler Datei laden) aus.
5. Wählen Sie Durchsuchen aus, um nach der Datei zu suchen, die die Daten für Datei laden enthält. Standardmäßig werden Dateien mit der Erweiterung `.csv`, `.avro`, `.parquet` und `.orc` angezeigt, Sie können jedoch auch andere Dateitypen auswählen. Die maximale -Dateigröße beträgt 5 MB.
6. Wählen Sie das File format (Dateiformat) für die hochzuladende Datei. Die unterstützten Datenformate sind CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET und ORC. Abhängig vom angegebenen Dateiformat können Sie die jeweiligen File options (Dateioptionen) auswählen. Sie können auch Data is encrypted (Daten sind verschlüsselt) auswählen, wenn die Daten verschlüsselt sind. Geben Sie dann den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels ein, mit dem die Daten verschlüsselt werden.

Wenn Sie CSV oder DELIMITER auswählen, können Sie auch das Trennzeichen auswählen und angeben, ob Sie die Kopfzeilen ignorieren möchten, wenn es sich bei der angegebenen Anzahl von Zeilen tatsächlich um Spaltennamen und nicht um zu ladende Daten handelt.

7. (Optional) In den Advanced settings (erweiterten Einstellungen) finden Sie verschiedene Data conversion parameters (Datenkonvertierungsparameter) und Load operations (Ladeoperationen). Geben Sie diese Informationen nach Bedarf für Ihre Datei ein.

   Weitere Informationen zu Datenkonvertierung und Datenladeparametern finden Sie unter Data conversion parameters (Datenkonvertierungsparameter) und Data load operations (Datenladeoperationen) im Amazon Redshift Database Developer Guide (Datenbankleitfaden zu Amazon Redshift).

8. Wählen Sie Next (Weiter).
9. Wählen Sie Bestehende Tabelle laden aus.
10. Bestätigen oder wählen Sie den Standort der Zieltabelle (Target table), einschließlich Cluster oder Arbeitsgruppe, Datenbank, Schema und Name der Tabelle, in die die Daten geladen werden.
11. (Optional) Sie können Spaltennamen auswählen, um sie in das Feld Column mapping (Spaltenzuordnung) einzugeben, damit die Spalten in der Reihenfolge der Eingabedatendatei zugeordnet werden.
12. Wählen Sie Load data (Daten laden), um das Laden der Daten zu starten.

    Wenn der Ladevorgang abgeschlossen ist, wird eine Nachricht mit der Mitteilung angezeigt, ob der Ladevorgang erfolgreich war oder nicht. Bei Erfolg können Sie nun mithilfe von SQL Daten aus der geladenen Tabelle auswählen. Wenn ein Fehler auftritt, stellen Sie eine Systemansicht-Abfrage (STL_LOAD_ERRORS), um weitere Details zu erfahren. Informationen über Fehler beim Befehl COPY finden Sie unter STL_LOAD_ERRORS im Datenbankentwicklerhandbuch zu Amazon Redshift.

    Die Vorlage für den Befehl COPY, die zum Laden von Daten verwendet wurde, wird in Ihrem Abfrageverlauf (Query history) angezeigt. In der Vorlage für den Befehl COPY sind einige der verwendeten Parameter aufgeführt, die Vorlage kann jedoch nicht direkt in einer Registerkarte des Editors ausgeführt werden. Weitere Informationen zum Abfrageverlauf finden Sie unter Abfrage- und Registerkarten-Verlauf anzeigen.

Wenn Sie Daten in eine neue Tabelle laden, erstellt Query Editor v2 zuerst die Tabelle in der Datenbank und lädt die Daten dann als separate Aktionen in demselben Workflow.

So laden Sie Daten aus einer lokalen Datei in eine neue Tabelle

Ihr Administrator für den Abfrage-Editor v2 muss den gemeinsamen Amazon-S3-Bucket im Fenster Account settings (Kontoeinstellungen) angeben. Die lokale Datei wird automatisch in einen von Ihrem Konto verwendeten gemeinsamen Amazon-S3-Bucket hochgeladen. Anschließend verwendet der Abfrage-Editor v2 den Befehl COPY zum Laden von Daten. Der Befehl COPY wird im Fenster „Load local file“ (Lokale Datei laden) des Abfrage-Editors v2 generiert und ausgeführt. Er unterstützt viele Parameter, die für die COPY-Befehlssyntax zum Kopieren aus Amazon S3 verfügbar sind. Weitere Informationen über den Befehl COPY und seine Optionen zum Laden von Daten aus Amazon S3 finden Sie unter COPY aus Amazon S3 im Datenbankentwicklerhandbuch zu Amazon Redshift.

1. Vergewissern Sie sich in der Strukturansicht des Abfrageeditors v2, dass Sie mit der Zieldatenbank verbunden sind. Sie können über das Kontextmenü (rechte Maustaste) eine Verbindung zu dem Cluster oder der Arbeitsgruppe herstellen, in den/die die Daten geladen werden.
2. Wählen Sie Load data (Daten laden) aus.
3. Wählen Sie für Data source (Datenquelle) die Option Load from local file (Aus lokaler Datei laden) aus.
4. Wählen Sie Durchsuchen aus, um nach der Datei zu suchen, die die Daten für Datei laden enthält. Standardmäßig werden Dateien mit der Erweiterung `.csv`, `.avro`, `.parquet` und `.orc` angezeigt, Sie können jedoch auch andere Dateitypen auswählen. Die maximale -Dateigröße beträgt 5 MB.
5. Wählen Sie das File format (Dateiformat) für die hochzuladende Datei. Die unterstützten Datenformate sind CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET und ORC. Abhängig vom angegebenen Dateiformat können Sie die jeweiligen File options (Dateioptionen) auswählen. Sie können auch Data is encrypted (Daten sind verschlüsselt) auswählen, wenn die Daten verschlüsselt sind. Geben Sie dann den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels ein, mit dem die Daten verschlüsselt werden.

   Wenn Sie CSV oder DELIMITER auswählen, können Sie auch das Trennzeichen auswählen und angeben, ob Sie die Kopfzeilen ignorieren möchten, wenn es sich bei der angegebenen Anzahl von Zeilen tatsächlich um Spaltennamen und nicht um zu ladende Daten handelt.

6. (Optional) In den Advanced settings (erweiterten Einstellungen) finden Sie verschiedene Data conversion parameters (Datenkonvertierungsparameter) und Load operations (Ladeoperationen). Geben Sie diese Informationen nach Bedarf für Ihre Datei ein.

   Weitere Informationen zu Datenkonvertierung und Datenladeparametern finden Sie unter Data conversion parameters (Datenkonvertierungsparameter) und Data load operations (Datenladeoperationen) im Amazon Redshift Database Developer Guide (Datenbankleitfaden zu Amazon Redshift).

7. Wählen Sie Next (Weiter).
8. Wählen Sie Neue Tabelle laden aus.
9. Bestätigen oder wählen Sie den Standort der Zieltabelle, einschließlich Cluster oder Arbeitsgruppe, Datenbank und Schema, in die die Daten geladen werden. Geben Sie einen Namen für die zu erstellende Tabelle ein.
10. Wählen Sie Tabelle erstellen aus, um die Tabelle unter Verwendung der angezeigten Definition zu erstellen.

    Eine Zusammenfassung der Tabellendefinition zur Überprüfung wird angezeigt. Die Tabelle wird in der Datenbank erstellt. Um die Tabelle später zu löschen, führen Sie einen SQL-Befehl DROP TABLE aus. Weitere Informationen finden Sie unter DROP TABLE im Datenbankentwicklerhandbuch zu Amazon Redshift.

11. Wählen Sie Load data (Daten laden), um das Laden der Daten zu starten.

    Wenn der Ladevorgang abgeschlossen ist, wird eine Nachricht mit der Mitteilung angezeigt, ob der Ladevorgang erfolgreich war oder nicht. Bei Erfolg können Sie nun mithilfe von SQL Daten aus der geladenen Tabelle auswählen. Wenn ein Fehler auftritt, stellen Sie eine Systemansicht-Abfrage (STL_LOAD_ERRORS), um weitere Details zu erfahren. Informationen über Fehler beim Befehl COPY finden Sie unter STL_LOAD_ERRORS im Datenbankentwicklerhandbuch zu Amazon Redshift.

    Die Vorlage für den Befehl COPY, die zum Laden von Daten verwendet wurde, wird in Ihrem Abfrageverlauf (Query history) angezeigt. In der Vorlage für den Befehl COPY sind einige der verwendeten Parameter aufgeführt, die Vorlage kann jedoch nicht direkt in einer Registerkarte des Editors ausgeführt werden. Weitere Informationen zum Abfrageverlauf finden Sie unter Abfrage- und Registerkarten-Verlauf anzeigen.

Erstellen und Ausführen von Abfragen

Sie können eine Abfrage im Editor eingeben oder eine gespeicherte Abfrage aus der Liste Queries (Abfragen) auswählen und auf Run (Ausführen) gehen.

Beim Standardwert von Limit 100 sind die Ergebnisse auf 100 Zeilen begrenzt. Sie können diese Option deaktivieren, damit eine größere Ergebnismenge zurückzugeben wird. Wenn Sie diese Option deaktivieren, können Sie die Option LIMIT in Ihre SQL-Anweisung aufnehmen, wenn Sie sehr große Ergebnismengen vermeiden möchten. Weitere Informationen finden Sie unter ORDER BY-Klausel im Datenbankentwicklerhandbuch zu Amazon Redshift.

Um einen Abfrageplan im Ergebnisbereich anzuzeigen, aktivieren Sie Explain (Erläuterung). Aktivieren Sie Explain graph (Diagramm erläutern), damit die Ergebnisse auch eine grafische Darstellung des Erläuterungsplans anzeigen.

Um eine Abfrage im Ordner Queries (Abfragen) zu speichern, wählen Sie Save (Speichern) aus.

Bei einer erfolgreichen Abfrage wird eine Erfolgsmeldung angezeigt. Wenn die Abfrage Informationen zurückgibt, werden die Ergebnisse im Abschnitt Results (Ergebnisse) gezeigt. Wenn die Anzahl der Ergebnisse den Anzeigebereich überschreitet, erscheinen oben im Ergebnisbereich Zahlen. Sie können die Zahlen auswählen, um die Ergebnisse auf aufeinanderfolgenden Seiten anzuzeigen.

Sie können den Abschnitt Result (Ergebnis) für jede Spalte filtern und sortieren. Um Filterkriterien in die Ergebnisspaltenüberschrift einzugeben, bewegen Sie den Mauszeiger über die Spalte. Es erscheint ein Menü ( ), wo Sie Kriterien zum Filtern eingeben können.

Wenn die Abfrage einen Fehler enthält, zeigt der Abfrage-Editor v2 eine Fehlermeldung im Ergebnisbereich an. Die Nachricht enthält Informationen dazu, wie die Abfrage korrigiert werden kann.

Sie können die Ergebnisse Ihrer Abfrage exportieren oder kopieren, indem Sie das Kontextmenü (Rechtsklick) im Ergebnisbereich wie folgt verwenden:

- Wählen Sie Export result set (Ergebnissatz exportieren) und entweder JSON oder CSV aus, um den gesamten Satz von Zeilenergebnissen in eine Datei herunterzuladen. Die Anzahl der Zeilen im Ergebnissatz kann durch die Option Limit oder die SQL-`limit`-Klausel in der Abfrage beschränkt werden. Die maximale Größe des heruntergeladenen Ergebnissatzes beträgt 5 MB.

- Wenn keine Zeilen ausgewählt sind, wählen Sie Export current page (Aktuelle Seite exportieren) und entweder JSON oder CSV aus, um die Zeilen von der aktuellen Seite in eine Datei herunterzuladen.
- Wenn Zeilen ausgewählt sind, wählen Sie Export selected rows (Ausgewählte Zeilen exportieren) und entweder JSON oder CSV aus, um die Zeilen herunterzuladen, die für eine Datei ausgewählt sind.
- Nachdem Zeilen ausgewählt sind, wählen Sie Copy rows (Zeilen kopieren) aus, um die ausgewählten Zeilen in die Zwischenablage zu kopieren.
- Nachdem Zeilen ausgewählt sind, wählen Sie Copy rows with headers (Zeilen mit Überschriften kopieren) aus, um die ausgewählten Zeilen mit den Spaltenüberschriften in die Zwischenablage zu kopieren.

Sie können auch die Tastenkombination Strg+C unter Windows oder Cmd+C unter macOS verwenden, um Daten von der aktuellen Ergebnisseite in die Zwischenablage zu kopieren. Wenn keine Zeilen ausgewählt sind, wird die Zelle mit Fokus in die Zwischenablage kopiert. Nachdem Zeilen ausgewählt sind, werden die ausgewählten Zeilen in die Zwischenablage kopiert.

Um eine neue Abfrage-Registerkarte hinzuzufügen, wählen Sie das Symbol

und dann die Option Editor aus, die in der Zeile mit den Abfrage-Registerkarten angezeigt wird. Die Abfrage-Registerkarte verwendet eine `Isolated session` oder auch nicht. Bei einer isolierten Verbindung sind die Ergebnisse eines SQL-Befehls, z. B. das Erstellen einer temporären Tabelle, auf einer anderen Editor-Registerkarte nicht sichtbar. Wenn Sie eine Editor-Registerkarte im Abfrage-Editor v2 öffnen, ist die Standardeinstellung eine isolierte Sitzung.

Eine Abfrage ausführen

1. Führen Sie im Abfragebereich einen der folgenden Schritte aus:
   - Geben Sie eine Abfrage ein.
   - Fügen Sie eine Abfrage ein, die Sie kopiert haben.
   - Wählen Sie den Ordner Queries (Abfragen), öffnen Sie das Kontextmenü (rechte Maustaste) über einer gespeicherten Abfrage und wählen Sie Open query (Abfrage öffnen) aus.
2. Vergewissern Sie sich, dass Sie den richtigen Wert für den Cluster oder die Workgroup (Arbeitsgruppe) und die Database (Datenbank) für das SQL ausgewählt haben, das Sie ausführen möchten.

Zunächst können Sie Ihren Cluster oder Ihre Workgroup (Arbeitsgruppe) in der Strukturansicht auswählen. Wählen Sie Ihre Database (Datenbank) auch in der Strukturansicht.

Sie können Cluster oder Workgroup (Arbeitsgruppe) sowie Database (Datenbank) innerhalb jeder Editor-Registerkarte mit dem Dropdown-Steuerelement neben der Kopfzeile Isolated session (Isolierte Sitzung) der jeweiligen Editor-Registerkarte ändern.

Für jede Editor-Registerkarte wählen Sie aus, ob der SQL-Befehl in einer Isolated session (Isolierte Sitzung) ausgeführt werden soll. Eine isolierte Sitzung hat eine eigene Verbindung mit einer Datenbank. Verwenden Sie diese, um SQL auszuführen, das von anderen Abfrage-Editor-Sitzungen isoliert ist. Weitere Informationen zu Verbindungen finden Sie unter Öffnen des Abfrage-Editors v2.

3. Wählen Sie Run (Ausführen) aus.

   Der Bereich Result (Ergebnis) öffnet sich. Dort werden die Ergebnisse angezeigt.

Den Erläuterungsplan für eine Abfrage anzeigen

1. Wählen Sie die Abfrage aus.
2. Aktivieren Sie Explain (Erläutern).

   Standardmäßig ist das Explain graph(Erläuterungsdiagramm) ebenfalls aktiviert.
3. Wählen Sie Ausführen aus.

   Die Abfrage wird ausgeführt und der Erläuterungsplan wird im Bereich Result (Ergebnis) der Abfrage angezeigt.

Die Abfragen-Editor v2 unterstützt die folgenden Funktionen:

- Sie können Abfragen mit mehreren SQL-Anweisungen auf einer Abfrageregisterkarte erstellen. Die Abfragen werden seriell ausgeführt und es werden mehrere Ergebnisregisterkarten für die einzelnen Abfragen geöffnet.
- Sie können Abfragen mit Sitzungsvariablen und temporären Tabellen erstellen.
- Sie können Abfragen mit austauschbaren Parametern erstellen, die durch `${parameter}` bestimmt sind. Sie können Ihre SQL-Abfrage mit mehreren austauschbaren Parametern erstellen und denselben Parameter an mehreren Stellen in Ihrer SQL-Anweisung verwenden.

Wenn die Abfrage ausgeführt wird, wird ein Fenster angezeigt, in das Sie den Wert des Parameters eingeben. Jedes Mal, wenn Sie die Abfrage ausführen, wird das Fenster angezeigt, in dem Sie Ihre Parameterwerte eingeben können.

Ein Beispiel finden Sie unter Beispiel: Umsatz größer als ein bestimmter Parameter.

- Abfragen werden automatisch versioniert. Sie können eine frühere Version einer auszuführenden Abfrage auswählen.
- Sie müssen nicht warten, bis eine Abfrage abgeschlossen ist, bevor Sie mit dem Workflow fortfahren. Abfragen werden weiterhin ausgeführt, auch wenn Sie den Abfrage-Editor schließen.
- Beim Erstellen von Abfragen wird das automatische Vervollständigen von Schema-, Tabellen- und Spaltennamen unterstützt.

Die SQL-Editor unterstützt die folgenden Funktionen:

- Die in SQL verwendeten Anfangs- und Endklammern haben übereinstimmende Farben. Im Editor werden vertikale Linien angezeigt, um Ihnen beim Zuordnen von Klammern zu helfen.
- Sie können Abschnitte Ihres SQL reduzieren und erweitern.
- Sie können Text in Ihrem SQL suchen und ersetzen.
- Sie können Tastenkombinationen für verschiedene allgemeine Bearbeitungsaufgaben verwenden.
- Im Editor werden SQL-Fehler hervorgehoben, um ein einfaches Auffinden von Problembereichen zu ermöglichen.

Eine Demo zu den Bearbeitungsfunktionen finden Sie im folgenden Video: Neue und verbesserte Bearbeitungserfahrung im Amazon-Redshift-Abfrage-Editor v2.

Abfragebeispiele

Im Folgenden finden Sie Beschreibungen der verschiedenen Abfragetypen, die Sie ausführen können.

Die in vielen dieser Abfragen verwendeten Daten stammen aus dem `tickit`-Beispielschema. Weitere Informationen zum Laden der `tickit`-Beispieldaten finden Sie unter Laden von Beispieldaten. Weitere Informationen über `tickit`-Beispieldaten finden Sie unter Beispieldatenbank im Datenbankentwicklerhandbuch zu Amazon Redshift.

Wenn Sie diese Beispielabfragen ausführen, bestätigen Sie, dass Sie die richtige Datenbank im Editor ausgewählt haben, z. B. `sample_data_dev`.

Themen

- Beispiel: Setzen von Sitzungsvariablen
- Beispiel: Top-Veranstaltung nach Gesamtumsatz
- Beispiel: Umsatz größer als ein bestimmter Parameter
- Beispiel: Erstellen einer temporären Tabelle
- Beispiel: Auswahl aus einer temporären Tabelle

Beispiel: Setzen von Sitzungsvariablen

Mit dem folgenden Befehl wird der `search_path`-Server-Konfigurationsparameter für die Sitzung auf public (öffentlich) gesetzt. Weitere Informationen finden Sie unter SET und search_pathim Datenbankentwicklerhandbuch zu Amazon Redshift.

```
set search_path to public;
```

Beispiel: Top-Veranstaltung nach Gesamtumsatz

Die folgende Abfrage findet die Veranstaltung mit dem größten Umsatz.

```
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname
order by 3;
```

Es folgt eine unvollständige Liste der Ergebnisse.

```
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
...
```

Beispiel: Umsatz größer als ein bestimmter Parameter

Die folgende Abfrage findet Umsätze, bei denen die verkaufte Menge größer ist als der durch `${numberoforders}` bestimmte Parameter. Wenn der Parameterwert 7 lautet, hat das Ergebnis 60 Zeilen. Wenn Sie die Abfrage ausführen, zeigt der Abfrage-Editor v2 das Fenster Run query form (Abfrageformular ausführen) an, auf dem der Wert von Parametern in der SQL-Anweisung gesammelt wird.

```
select salesid, qtysold
from sales
where qtysold > ${numberoforders}
order by 2;
```

Es folgt eine unvollständige Liste der Ergebnisse.

```
salesid qtysold
20005 8
21279 8
130232 8
42737 8
74681 8
67103 8
105533 8
91620 8
121552 8
...
```

Beispiel: Erstellen einer temporären Tabelle

Die folgende Anweisung erstellt die temporäre Tabelle eventsalestemp indem Informationen aus den Tabellen sales und events ausgewählt werden.

```
create temporary table eventsalestemp as
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname;
```

Beispiel: Auswahl aus einer temporären Tabelle

Die folgende Anweisung wählt Ereignisse, Gesamtaufträge und Gesamtumsatz aus der temporären Tabelle eventsalestemp, geordnet nach der Gesamtzahl der Bestellungen.

```
select eventname,  totalorders,  totalsales
from eventsalestemp
order by 2;
```

Es folgt eine unvollständige Liste der Ergebnisse.

```
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
...
```

Erstellen und Ausführen von Notebooks

Mithilfe von Notebooks können Sie mehrere SQL-Abfragen in einem einzigen Dokument organisieren, kommentieren und freigeben. Einem Notebook lassen sich mehrere SQL-Abfrage- und Markdown-Zellen hinzufügen. Notebooks bieten die Möglichkeit, Abfragen und Erklärungen im Zusammenhang mit einer Datenanalyse unter Verwendung mehrerer Abfrage- und Markdown-Zellen in einem einzigen Dokument zu gruppieren. Sie können Text hinzufügen und das Erscheinungsbild mithilfe der Markdown-Syntax formatieren, um Kontext und zusätzliche Informationen für Ihre Datenanalyse bereitzustellen. Sie können Ihre Notebooks für Teammitglieder freigeben.

Für die Verwendung von Notebooks müssen Sie Ihrem IAM-Prinzipal (einem IAM-Benutzer oder einer IAM-Rolle) die Berechtigung für Notebooks hinzufügen. Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift. Sie können die Berechtigung zu einer der von Abfrage-Editor v2 verwalteten Richtlinien hinzufügen. Weitere Informationen finden Sie unter Zugreifen auf den Abfrage-Editor v2.

Sie können die Zellen eines Notebooks sequenziell ausführen (Run all). Die SQL-Abfragezelle eines Notebooks verfügt über fast dieselben Funktionen wie eine Registerkarte im Abfrage-Editor.

Weitere Informationen finden Sie unter Erstellen und Ausführen von Abfragen. Im Folgenden sind die Unterschiede zwischen einer Registerkarte im Abfrage-Editor und einer SQL-Zelle in einem Notebook aufgeführt.

- Es gibt kein Steuerelement zur Ausführung von `Explain` in einer SQL-Anweisung in einem Notebook.
- Sie können nur ein Diagramm pro SQL-Zelle in einem Notebook erstellen.

Sie können Notebooks in Dateien, die mit Abfrage-Editor v2 erstellt wurden, exportieren und importieren. Die Dateierweiterung lautet `.ipynb` und die Dateigröße kann maximal 5 MB betragen. Die SQL- und Markdown-Zellen werden in der Datei gespeichert. Ein Cluster oder eine Arbeitsgruppe und eine Datenbank werden nicht im exportierten Notebook gespeichert. Wenn Sie ein importiertes Notebook öffnen, wählen Sie den Cluster oder die Arbeitsgruppe und die Datenbank aus, in dem/denen es ausgeführt werden soll. Nach Ausführung von SQL-Zellen können Sie auf der Registerkarte „Results“ (Ergebnisse) auswählen, ob die aktuelle Ergebnisseite als Diagramm angezeigt werden soll. Die Ergebnismenge einer Abfrage wird nicht im Notebook gespeichert.

Bei Ausführung eines Notebooks über die Optionen Alle ausführen oder Ausführen wird ein Bereich Ausführungsstatus verfügbar. Wählen Sie das Symbol

aus, um den Bereich zu öffnen. Dieser Bereich enthält eine Zusammenfassung des Status der letzten Ausführung der SQL-Zellen in Ihrem Notebook mit Alle ausführen oder Ausführen. Wenn Sie mehrere SQL-Zellen ausführen, können Sie auf einen Blick den Status, die verstrichene Zeit und einige Details zur Ausführung sehen. Sie können die angezeigten Zellen nach Status filtern: `All`, `Succeeded`, `Error`, `In progress` oder `Canceled`. Sie können diesen Bereich auch verwenden, um zu einer SQL-Zelle im Editor zu navigieren.

So erstellen Sie ein Notebook

1. Wählen Sie im Navigator-Menü

   Editor aus.
2. Wählen Sie

   und dann Notebook aus.

Standardmäßig wird eine SQL-Abfragezelle im Notebook angezeigt.

3. Führen Sie in der SQL-Abfragezelle einen der folgenden Schritte aus:

   - Geben Sie eine Abfrage ein.
   - Fügen Sie eine Abfrage ein, die Sie kopiert haben.

4. (Optional) Wählen Sie das

   -Symbol und dann Markdown aus, um eine Markdown-Zelle hinzuzufügen, in der Sie beschreibenden oder erklärenden Text mithilfe der Standard-Markdown-Syntax schreiben können.

5. (Optional) Wählen Sie das

   -Symbol und dann SQL aus, um eine SQL-Zelle einzufügen.

Mit dem Symbol

(Stiftsymbol) können Sie Notebooks umbenennen.

Über das Menü

(Mehr) können Sie auch die folgenden Operationen in einem Notebook ausführen:

- Share with my team (Für mein Team freigeben) – Zum Freigeben des Notebooks für Ihr Team gemäß den Tags. Weitere Informationen finden Sie unter Teilen einer Abfrage.
- Export (Exportieren) – Zum Exportieren des Notebooks in eine lokale Datei mit der Erweiterung `.ipynb`.
- Save version (Version speichern) – Zum Erstellen einer Version des Notebooks. Wenn Sie verschiedene Versionen eines Notebooks anzeigen möchten, navigieren Sie zu Ihren gespeicherten Notebooks und öffnen Sie Version history (Versionsverlauf).

- Duplica
  (Duplizieren) – Zum Erstellen einer Kopie des Notebooks und Öffnen dieser Kopie in einer neuen Notebook-Registerkarte.
- Shortcu
  (Tastenkombinationen) – Zum Anzeigen der verfügbaren Tastenkombinationen beim Erstellen eines Notebooks.

So öffnen Sie ein gespeichertes Notebook

1. Wählen Sie im Navigator-Menü

   Notebooks aus. Ihre gespeicherten Notebooks und Notebook-Ordner werden angezeigt.
2. Wählen Sie das zu öffnende Notebook aus und doppelklicken Sie darauf.

Auf der Notebook-Registerkarte können Sie eigene Notebooks (Option My notebooks), Notebooks, die von Ihnen freigegeben wurden (Option Shared by me), und Notebooks, die für Ihr Team freigegeben wurden (Option Shared to my team), anzeigen.

Um ein Notebook aus einer lokalen Datei in My notebooks (Eigene Notebooks) zu importieren, wählen Sie

Import (Importieren) aus und navigieren Sie dann zu der `.ipynb`-Datei, die Ihr Notebook enthält. Das Notebook wird in den aktuell geöffneten Notebook-Ordner importiert. Sie können das Notebook anschließend im Notebook-Editor öffnen.

Im Kontextmenü (rechte Maustaste) eines Notebooks können Sie folgende Aktionen ausführen:

- Open notebook (Notebook öffnen) – Zum Öffnen des Notebooks im Editor.
- Save version (Version speichern) – Zum Speichern einer Version des Notebooks.
- Version history (Versionsverlauf) – Zum Anzeigen der Versionen eines Notebooks. Im Fenster Version history (Versionsverlauf) können Sie Versionen löschen und zurücksetzen. Sie können auch ein Notebook aus der aktuell ausgewählten Version erstellen.
- Edit tags (Tags bearbeiten) – Zum Erstellen und Bearbeiten von Tags in einem Notebook.
- Share with my team (Für mein Team freigeben) – Zum Freigeben eines Notebooks für Ihr Team.

Um ein Notebook für Ihr Team freizugeben, müssen Sie sicherstellen, dass das Prinzipal-Tag `sqlworkbench-team` auf denselben Wert wie bei den übrigen Teammitgliedern in Ihrem Konto eingestellt ist. Beispielsweise könnte ein Administrator den Wert für jeden in der Buchhaltungsabteilung auf `accounting-team` einstellen. Ein Beispiel finden Sie unter Für die Verwendung des Abfrage-Editors v2 erforderliche Berechtigungen .

- Export (Exportieren) – Zum Exportieren eines Notebooks in eine lokale Datei.
- Rename (Umbenennen) – Zum Umbenennen eines Notebooks.
- Duplicate (Duplizieren) – Zum Erstellen einer Kopie eines Notebooks.
- Delete (Löschen) – Zum Löschen eines Notebooks.

Eine Demo zu Notebooks finden Sie im folgenden Video: Amazon Redshift SQL Notebooks in query editor v2 (Amazon-Redshift-SQL-Notebooks in Abfrage-Editor v2).

Abfragen der AWS Glue Data Catalog

Sie können den Abfrage-Editor v2 verwenden, um Daten abzufragen, die in Ihrem AWS Glue Data Catalog katalogisiert sind. Standardmäßig AWS Glue Data Catalog wird die als Abfrage-Editor v2-Datenbank mit dem Namen aufgeführt`awsdatacatalog`. Das Abfragen von AWS Glue Data Catalog ist nicht in allen Amazon AWS-Regionen Redshift verfügbar. Verwenden Sie den Befehl SHOW, um festzustellen, ob diese Funktion verfügbar ist. Weitere Informationen zu finden Sie AWS Glue unter Was ist? AWS Glue im AWS Glue Entwicklerhandbuch.

> **Note**
>
> Das Abfragen von AWS Glue Data Catalog wird nur in Amazon Redshift RA3-Knotenclustern und Amazon Redshift Serverless unterstützt.

Mit den folgenden SQL-Befehlen können Sie Ihr Data Warehouse konfigurieren und die AWS Glue katalogisierten Datenbankobjekte anzeigen:

- SHOW – um anzuzeigen, ob `awsdatacatalog` für das aktuell verbundene Data Warehouse gemountet ist. Wenn Sie zum Beispiel den Parameterwert `data_catalog_auto_mount` anzeigen möchten, führen Sie den folgenden Befehl aus:

```
SHOW data_catalog_auto_mount;
```

Weitere Informationen finden Sie unter SHOW im Entwicklerhandbuch für Amazon Redshift Database.

- ALTER SYSTEM – um die Konfiguration von `data_catalog_auto_mount` auf Systemebene zu ändern. Wenn Sie zum Beispiel den Parameterwert `data_catalog_auto_mount` in on ändern möchten, führen Sie den folgenden Befehl aus:

```
ALTER SYSTEM SET data_catalog_auto_mount = on;
```

Die Änderung wird wirksam, wenn ein bereitgestellter Cluster neu gestartet wird oder eine Serverless-Arbeitsgruppe automatisch angehalten und fortgesetzt wird. Weitere Informationen finden Sie unter ALTER SYSTEM im Entwicklerhandbuch für Amazon Redshift Database.

- SHOW SCHEMAS – zeigt eine Liste von Schemata an. Die Schemas in der genannten Datenbank stellen die AWS Glue Datenbanken `awsdatacatalog` dar, die in der katalogisiert sind. AWS Glue Data Catalog Wenn Sie diese Schemata beispielsweise anzeigen möchten, führen Sie folgenden Befehl aus:

```
SHOW SCHEMAS FROM DATABASE awsdatacatalog;
```

Weitere Informationen finden Sie unter SHOW SCHEMAS im Entwicklerhandbuch für Amazon Redshift Database.

- SHOW TABLES – zeigt eine Liste von Tabellen in einem Schema an. Um beispielsweise die Tabellen in der genannten AWS Glue Data Catalog Datenbank anzuzeigen, die sich im Schema `myglue` Run befinden`awsdatacatalog`, gehen Sie wie folgt vor:

```
SHOW TABLES FROM SCHEMA awsdatacatalog.myschema;
```

Weitere Informationen finden Sie unter SHOW TABLES im Entwicklerhandbuch für Amazon Redshift Database.

- SHOW COLUMNS – zeigt eine Liste von Spalten in einer Tabelle an. Um beispielsweise die Spalten in der genannten AWS Glue Data Catalog Datenbank anzuzeigen`awsdatacatalog`, die sich in Schema `myglue` und Table `mytable` Run befinden:

```
SHOW COLUMNS FROM TABLE awsdatacatalog.myglue.mytable;
```

Weitere Informationen finden Sie unter SHOW COLUMNS im Entwicklerhandbuch für Amazon Redshift Database.

Gehen Sie wie folgt vor, um Ihrem IAM-Benutzer oder Ihrer IAM-Rolle die AWS Glue Data Catalog Berechtigung zur Abfrage von zu erteilen

1. Stellen Sie in der Strukturansicht mithilfe der Authentifizierungsmethode Datenbankbenutzername und -passwort eine Verbindung mit Ihrer ursprünglichen Datenbank in Ihrem bereitgestellten Cluster oder Ihrer Serverless-Arbeitsgruppe her. Verwenden Sie beispielsweise für eine Verbindung mit der Datenbank `dev` den Administratorbenutzernamen und das -passwort, die Sie bei der Erstellung des Clusters oder der Arbeitsgruppe verwendet haben.
2. Führen Sie auf einer Registerkarte des Editors die folgende SQL-Anweisung aus, um einem IAM-Benutzer Zugriff auf den AWS Glue Data Catalog zu gewähren.

   ```
   GRANT USAGE ON DATABASE awsdatacatalog to "IAM:myIAMUser"
   ```

   `IAM:myIAMUser` ist dabei ein IAM-Benutzer, dem Sie Nutzungsrechte für den AWS Glue Data Catalog gewähren möchten. Bei einer IAM-Rolle können Sie alternativ Nutzungsrechte für *`IAMR:myIAMRole`* erteilen.
3. Bearbeiten oder löschen Sie in der Strukturansicht die Verbindung zu dem Cluster oder der Arbeitsgruppe, den/die Sie zuvor erstellt haben. Stellen Sie auf eine der folgenden Arten eine Verbindung mit Ihrem Cluster oder Ihrer Arbeitsgruppe her:
   - Wenn Sie von einem Cluster aus auf die Datenbank von `awsdatacatalog` zugreifen möchten, müssen Sie die Authentifizierungsmethode Temporäre Anmeldeinformationen unter Verwendung Ihrer IAM-Identität verwenden. Weitere Informationen zu dieser Authentifizierungsmethode finden Sie unter Herstellen einer Verbindung mit einer Amazon-Redshift-Datenbank. Möglicherweise muss der Administrator für Ihren Abfrage-Editor v2 die Kontoeinstellungen für das Konto konfigurieren, damit diese Authentifizierungsmethode im Verbindungsfenster angezeigt wird.
   - Wenn Sie von einer Arbeitsgruppe aus auf die Datenbank von `awsdatacatalog` zugreifen möchten, müssen Sie die Authentifizierungsmethode Verbundbenutzer verwenden. Weitere Informationen zu dieser Authentifizierungsmethode finden Sie unter Herstellen einer Verbindung mit einer Amazon-Redshift-Datenbank.
4. Mit der erteilten Berechtigung können Sie Ihre IAM-Identität verwenden, um SQL-Abfragen für Ihren AWS Glue Data Catalog auszuführen.

Nach Herstellung der Verbindung können Sie den Abfrage-Editor v2 verwenden, um Daten abzufragen, die im AWS Glue Data Catalog katalogisiert sind. Wählen Sie in der Strukturansicht des Abfrage-Editors v2 den Cluster oder die Arbeitsgruppe und die Datenbank `awsdatacatalog` aus. Vergewissern Sie sich, dass im Editor- oder Notebook-Bereich der richtige Cluster bzw. die richtige Arbeitsgruppe ausgewählt ist. Bei der ausgewählten Datenbank sollte es sich um die ursprüngliche Amazon-Redshift-Datenbank handeln, beispielsweise `dev`. Informationen zum Erstellen von Abfragen finden Sie unter Erstellen und Ausführen von Abfragen und Erstellen und Ausführen von Notebooks. Die Datenbank namens `awsdatacatalog` ist für den Verweis auf die externe Data-Catalog-Datenbank in Ihrem Konto reserviert. Es sind nur schreibgeschützte Abfragen für die Datenbank `awsdatacatalog` möglich. Verwenden Sie für den Verweis auf die Tabelle in Ihrer SELECT-Anweisung eine dreiteilige Notation. Dabei ist der erste Teil der Datenbankname, der zweite Teil der AWS Glue Datenbankname und der dritte Teil der AWS Glue Tabellenname.

```
SELECT * FROM awsdatacatalog.<aws-glue-db-name>.<aws-glue-table-name>;
```

Sie können verschiedene Szenarien ausführen, in denen die AWS Glue Data Catalog Daten gelesen und Amazon Redshift Redshift-Tabellen gefüllt werden.

Das folgende SQL-Beispiel verbindet zwei Tabellen, die in definiert sind. 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;
```

Das folgende SQL-Beispiel erstellt eine Amazon Redshift Redshift-Tabelle und füllt sie mit Daten aus einer Verknüpfung von zwei AWS Glue Tabellen.

```
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;
```

Abfragen eines Data Lake

Sie können Daten in einem Amazon S3-Data Lake abfragen. Zuerst erstellen Sie ein externes Schema, um auf die externe Datenbank im AWS Glue Data Catalog zu verweisen. Anschließend können Sie Daten im Amazon S3-Data Lake abfragen.

Demo: Einen Data Lake abfragen

Eine Demo zum Abfragen eines Data Lake finden Sie im folgenden Video. Fragen Sie Ihren Data Lake mit dem Abfrage-Editor v2 von Amazon Redshift ab.

Voraussetzungen

Bevor Sie mit Ihrem Data Lake in Query Editor v2 arbeiten, vergewissern Sie sich, dass in Ihrer Amazon-Redshift-Umgebung Folgendes eingerichtet wurde:

- Crawling Ihrer Amazon-S3-Daten unter Verwendung von AWS Glue und Aktivieren Ihres Datenkatalogs für AWS Lake Formation.
- Erstellen einer IAM-Rolle für Amazon Redshift unter Verwendung des AWS Glue-aktivierten Datenkatalogs für AWS Lake Formation Weitere Informationen zu diesem Verfahren finden Sie unter So erstellen Sie eine IAM-Rolle für Amazon Redshift mit einem für AWS Lake Formation aktivierten AWS Glue Data Catalog. Weitere Informationen zur Verwendung von Redshift Spectrum und Lake Formation finden Sie unter Verwendung von Redshift Spectrum mit AWS Lake Formation.
- Gewähren von SELECT-Berechtigungen für die Tabelle, um diese in der Lake-Formation-Datenbank abzufragen. Weitere Informationen zu diesem Verfahren finden Sie unter So gewähren Sie SELECT-Berechtigungen für eine Tabelle, um diese in der Lake-Formation-Datenbank abzufragen.

  Sie können in der Lake-Formation-Konsole (https://console.aws.amazon.com/lakeformation/) im Abschnitt Berechtigungen auf der Seite Data-Lake-Berechtigungen überprüfen, ob die IAM-Rolle, die AWS Glue-Datenbank und die Tabellen über die richtigen Berechtigungen verfügen.
- Bestätigung, dass Ihr verbundener Benutzer berechtigt ist, Schemata in der Amazon-Redshift-Datenbank zu erstellen und auf Daten in Ihrem Data Lake zuzugreifen. Wenn Sie in Query Editor v2 eine Verbindung zu einer Datenbank herstellen, wählen Sie eine Authentifizierungsmethode aus, die Anmeldeinformationen beinhaltet. Dabei kann es sich um einen Datenbankbenutzer oder einen IAM-Benutzer handeln. Der verbundene Benutzer muss über die richtigen Berechtigungen und Datenbankrechte verfügen, wie z. B. `superuser`. Der `admin`-Benutzer von Amazon Redshift, der den Cluster oder die Arbeitsgruppe erstellt hat, verfügt über `superuser`-Berechtigungen und kann Schemata erstellen und die Redshift-Datenbank verwalten. Weitere Informationen zum Herstellen einer Verbindung zu einer Datenbank mit Query Editor v2 finden Sie unter Herstellen einer Verbindung mit einer Amazon-Redshift-Datenbank.

Erstellen eines externen Schemas

Um Daten in einem Amazon S3 Data Lake abzufragen, erstellen Sie zunächst ein externes Schema. Ein externes Schema verweist auf eine Datenbank in einem externen AWS Glue Data Catalog.

1. Wählen Sie in der Editor-Ansicht von Query Editor v2 die Option

   Erstelle
   und dann Schema aus.
2. Geben Sie einen Schema name (Schemennamen) ein.
3. Wählen Sie unter Schematyp die Option Extern aus.
4. Unter den Details für den Datenkatalog wird für Region standardmäßig die AWS-Region verwendet, in der sich Ihre Redshift-Datenbank befindet.
5. Wählen Sie die AWS Glue-Datenbank aus, der das externe Schema zugeordnet werden soll und die Verweise auf die AWS Glue-Tabellen enthält.
6. Wählen Sie eine IAM-Rolle für Amazon Redshift aus, die über die erforderlichen Berechtigungen zum Abfragen von Daten in Amazon S3 verfügt.
7. Wählen Sie optional eine IAM-Rolle aus, die über die Berechtigung für den Datenkatalog verfügt.
8. Wählen Sie Create schema (Schema erstellen) aus.

   Das Schema wird in der Strukturansicht unter Ihrer Datenbank angezeigt.

Wenn Sie beim Erstellen des Schemas die Fehlermeldung „Berechtigung verweigert“ für Ihre Datenbank erhalten, überprüfen Sie, ob der verbundene Benutzer über die Datenbankberechtigung zum Erstellen eines Schemas verfügt.

Abfragen Ihrer Daten in Amazon S3-Data Lake

Verwenden Sie das Schema, das Sie im vorherigen Verfahren erstellt haben.

1. Wählen Sie in der Strukturansicht das Schema aus.
2. Um eine Tabellendefinition anzuzeigen, wählen Sie eine Tabelle aus. Die Tabellenspalten und Datentypen werden angezeigt.
3. Um eine Tabelle abzufragen, wählen Sie die Tabelle aus und wählen Sie im Kontextmenü (Rechtsklickmenü) Tabelle auswählen aus, um eine Abfrage zu generieren.
4. Führen Sie die Abfrage im Editor aus.

Das folgende Beispiel-SQL wurde von Query Editor v2 generiert, um alle Zeilen in der AWS Glue-Tabelle `flightscsv` abzufragen. In der Ausgabe sind die Spalten und Zeilen der Einfachheit halber verkürzt.

```
SELECT * FROM "dev"."mydatalake_schema"."flightscsv";

year    quarter   month   dom  day_of_week   fl_date    unique_carrier  airline_id
  carrier   tail_num   fl_num
2016    4         10      19   3             10/19/16   OO              20304
  OO         N753SK    3086
2016    4         10      19   3             10/19/16   OO              20304
  OO         N753SK    3086
2016    4         10      19   3             10/19/16   OO              20304
  OO         N778SK    3087
2016 4          10      19   3            10/19/16   OO              20304
 OO         N778SK    3087
...
```

Arbeiten mit Datashares

Sie können einen Datashare erstellen, damit Benutzer in einem anderen Cluster die Daten abfragen können. Der Cluster mit den Daten, die Sie freigeben möchten, wird als Produzenten-Cluster bezeichnet. Sie erstellen einen Datashare im Produzenten-Cluster für die Datenbankobjekte, die Sie freigeben möchten. Sie können Schemata, Tabellen, Ansichten und benutzerdefinierte SQL-Funktionen (UDFs) freigeben. Der Cluster, für den Sie die Daten freigeben möchten, wird als Konsumenten-Cluster bezeichnet. Im Konsumenten-Cluster erstellen Sie eine Datenbank aus dem Datashare. Anschließend können Benutzer im Konsumenten-Cluster die Daten abfragen. Weitere Informationen finden Sie unter Erste Schritte mit der Datenfreigabe im Datenbankentwicklerhandbuch zu Amazon Redshift.

Erstellen von Datashares

Sie erstellen einen Datashare im Cluster, den Sie als Produzenten-Cluster verwenden möchten. Weitere Informationen zu den Überlegungen im Hinblick auf Datashares finden Sie unter Überlegungen zur Freigabe von Daten in Amazon Redshift im Datenbankentwicklerhandbuch zu Amazon Redshift.

1. Wählen Sie die zu verwendende Datenbank im Produzenten-Cluster aus.

2. Erstellen Sie einen Datashare. Zum Beispiel:

```
create datashare mysource;
```

3. Legen Sie Berechtigungen für den Datashare fest. Zum Beispiel:

```
grant alter, share on datashare mysource to admin;
```

4. Legen Sie Berechtigungen für die Datenbankobjekte fest, die Sie freigeben möchten. Zum Beispiel:

```
alter datashare mysource add schema public;
```

```
alter datashare mysource add table public.event;
```

5. Legen Sie Berechtigungen für den Konsumenten-Cluster-Namespace für den Zugriff auf den Datashare fest. Zum Beispiel:

```
grant usage on datashare mysource to namespace '2b12345-1234-5678-9012-
bb1234567890';
```

Anzeigen von Datashares

Sie können die Datashares, die Sie im Produzenten-Cluster erstellt haben, anzeigen.

1. Wählen Sie den Produzenten-Cluster aus.
2. Zeigen Sie die Datashares an. Zum Beispiel:

```
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
```

Erstellen der Konsumentendatenbank

Im Konsumenten-Cluster erstellen Sie eine Datenbank aus dem Datashare. Diese Schritte beschreiben, wie Sie Daten zwischen zwei Clustern im selben Konto freigeben. Informationen zur gemeinsamen Nutzung von Daten zwischen AWS Konten finden Sie unter AWS Kontenübergreifendes Teilen von Daten im Amazon Redshift Database Developer Guide.

Sie können SQL-Befehle oder die Baumansicht des Abfrage-Editors v2 verwenden, um die Datenbank zu erstellen.

So verwenden Sie SQL

1. Erstellen Sie eine Datenbank aus dem Datashare für Ihr Konto und den Namespace des Produzenten-Clusters. Zum Beispiel:

```
create database share_db from datashare mysource of account '123456789012'
 namespace 'p1234567-8765-4321-p10987654321';
```

2. Legen Sie Berechtigungen fest, damit Benutzer auf die Datenbank und das Schema zugreifen können. Zum Beispiel:

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

So verwenden Sie die Baumansicht des Abfrage-Editors v2

1. Wählen Sie

Create (Erstellen) aus und danach Database (Datenbank).
2. Geben Sie einen Database name (Datenbanknamen) ein.
3. (Optional) Wählen Sie Users and groups (Benutzer und Gruppen) und dort einen Database user (Datenbankbenutzer) aus.
4. Klicken Sie auf Create using a datashare (Mit einem Datashare erstellen).
5. Wählen Sie den Datashare aus.
6. Wählen Sie Datenbank erstellen aus.

Die
neue D
Datenbank wird in der Baumansicht des Abfrage-Editors v2 angezeigt.

7. Legen Sie Berechtigungen fest, damit Benutzer auf die Datenbank und das Schema zugreifen können. Zum Beispiel:

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

Abfragen von Datashare-Objekten

Im Konsumenten-Cluster können Sie Datashare-Objekte unter Verwendung der vollqualifizierten Objektnamen abfragen, die mit der dreiteiligen Notation ausgedrückt werden: Datenbank, Schema und Name des Objekts.

1. Wählen Sie in der Baumansicht des Abfrage-Editors v2 das Schema aus.
2. Um eine Tabellendefinition anzuzeigen, wählen Sie eine Tabelle aus.

   Die Tabellenspalten und Datentypen werden angezeigt.
3. Um eine Tabelle abzufragen, wählen Sie die Tabelle aus und verwenden Sie das Kontextmenü (rechte Maustaste), um Select table (Tabelle auswählen) auszuwählen.
4. Fragen Sie Tabellen mithilfe von SELECT Befehlen ab. Zum Beispiel:

```
select top 10 * from test_db.public.event;
```

Planung einer Abfrage mit dem Query Editor v2

Sie können einen Zeitplan für die Ausführung einer SQL-Anweisung mit dem Amazon Redshift Query Editor v2 erstellen. Sie erstellen einen Zeitplan, um die SQL-Anweisung in Zeitintervallen auszuführen, die Ihren Geschäftsanforderungen entsprechen. Wenn die geplante Abfrage ausgeführt werden soll, wird die Abfrage von Amazon gestartet EventBridge und verwendet die Amazon Redshift Data API.

So erstellen Sie einen Zeitplan für die Ausführung einer SQL-Anweisung

1. Wählen Sie in der Ansicht Editor die Option Zeitplan aus, um einen Zeitplan für die Ausführung einer SQL-Anweisung zu erstellen.
2. Wenn Sie den Zeitplan definieren, geben Sie die folgenden Informationen an.
   - Die IAM-Rolle, die die erforderlichen Berechtigungen zum Ausführen der Abfrage übernimmt Diese IAM-Rolle ist auch Ihrem Cluster oder Ihrer Arbeitsgruppe angefügt.
   - Die Authentifizierungswerte für entweder AWS Secrets Manager temporäre Anmeldeinformationen zur Autorisierung des Zugriffs auf Ihren Cluster oder Ihre Arbeitsgruppe. Diese Authentifizierungsmethoden werden von der Daten-API unterstützt. Weitere Informationen finden Sie unter Authentifizieren einer geplanten Abfrage.
   - Den Cluster oder die Arbeitsgruppe, in dem/der sich Ihre Datenbank befindet
   - Den Namen der Datenbank, die die Daten enthält, die abgefragt werden sollen
   - Der Name der geplanten Abfrage und ihre Beschreibung. Der Abfrage-Editor v2 stellt dem angegebenen Namen der geplanten Abfrage das Präfix „QS2-“ voran. Der Query Editor v1 stellt Namen von geplanten Abfragen das Präfix „QS-“ voran.
   - Die SQL-Anweisung, die nach dem Zeitplan ausgeführt werden soll
   - Die Zeitplanfrequenz- und Wiederholungsoptionen oder einen cron-formatierten Wert, der den Zeitplan definiert. Weitere Informationen finden Sie unter Cron Expressions im Amazon CloudWatch Events-Benutzerhandbuch.
   - Optional können Sie Amazon-SNS-Standardbenachrichtigungen aktivieren, um die geplante Abfrage zu überwachen. Möglicherweise müssen Sie die E-Mail-Adresse bestätigen, die Sie für die Amazon-SNS-Benachrichtigung angegeben haben. Sehen Sie in Ihrem Posteingang nach, ob Sie einen Link zur Bestätigung der E-Mail-Adresse für die Amazon-SNS-Benachrichtigung erhalten haben. Weitere Informationen finden Sie unter E-Mail-Benachrichtigungen im Entwicklerhandbuch zu Amazon Simple Notification Service. Wenn Ihre Anfrage ausgeführt wird, Sie aber keine Nachrichten sehen, die in Ihrem SNS-Thema veröffentlicht wurden, finden Sie weitere Informationen unter Meine Regel wird ausgeführt, aber ich sehe keine Nachrichten, die in meinem Amazon SNS SNS-Thema veröffentlicht wurden, im EventBridge Amazon-Benutzerhandbuch.

3. Wählen Sie Abfrage planen aus, um den Zeitplan zu speichern und zu aktivieren und den Zeitplan der Liste der Abfragen in der Ansicht Geplante Abfragen hinzuzufügen.

In der Ansicht Geplante Abfragen alle geplanten Abfragen für Ihre Cluster und Arbeitsgruppen aufgeführt. In dieser Ansicht können Sie Details zur geplanten Abfrage anzeigen, den Zeitplan aktivieren oder deaktivieren, den Zeitplan bearbeiten und die geplante Abfrage löschen. Wenn Sie Abfragedetails anzeigen, können Sie auch den Verlauf der Ausführung der Abfrage mit dem Zeitplan einsehen.

> **Note**
>
> Eine planmäßige Abfrageausführung ist nur 24 Stunden in der Liste Planverlauf verfügbar. Abfragen, die nach einem Zeitplan ausgeführt werden, werden nicht in der Ansicht Abfrageverlauf von Abfrage-Editor v2 angezeigt.

Festlegen von Berechtigungen zum Planen einer Abfrage

Um Abfragen zu planen, muss der AWS Identity and Access Management (IAM-) Benutzer, der den Zeitplan und die dem Zeitplan zugeordnete IAM-Rolle definiert, mit den IAM-Berechtigungen für die Verwendung von Amazon EventBridge und der Amazon Redshift Data API konfiguriert sein. Wenn Sie E-Mails aus geplanten Abfragen erhalten möchten, muss die Amazon-SNS-Benachrichtigung, die optional angegeben werden kann, ebenfalls konfiguriert werden.

Im Folgenden werden die Aufgaben beschrieben, mit denen AWS verwaltete Richtlinien zur Erteilung von Berechtigungen verwendet werden. Abhängig von Ihrer Umgebung möchten Sie jedoch möglicherweise die zulässigen Berechtigungen einschränken.

Bearbeiten Sie den IAM-Benutzer, der beim Query Editor v2 angemeldet ist, mithilfe der IAM-Konsole (https://console.aws.amazon.com/iam/).

- Zusätzlich zu den Berechtigungen zum Ausführen von Amazon Redshift- und Query Editor v2-Vorgängen können Sie die `AmazonEventBridgeFullAccess` und die `AmazonRedshiftDataFullAccess` AWS verwalteten Richtlinien an einen IAM-Benutzer anhängen.
- Sie können auch die Berechtigungen einer Rolle zuweisen und die Rolle dem Benutzer zuweisen.

Weisen Sie eine Richtlinie, die die Berechtigung `sts:AssumeRole` erteilt, dem Ressourcen-ARN der IAM-Rolle zu, die Sie angeben, wenn Sie die geplante Abfrage definieren. Weitere Informationen zur Übernahme von Rollen finden Sie unter Erteilen von Berechtigungen an einen Benutzer zum Wechseln von Rollen im IAM-Benutzerhandbuch.

Das folgende Beispiel zeigt eine Berechtigungsrichtlinie, die die IAM-Rolle `myRedshiftRole` im Konto `123456789012` übernimmt. Die IAM-Rolle `myRedshiftRole` ist auch die IAM-Rolle, die dem Cluster oder der Arbeitsgruppe angefügt ist, in dem bzw. der die geplante Abfrage ausgeführt wird.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AssumeIAMRole",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::123456789012:role/myRedshiftRole"
            ]
        }
    ]
}
```

Aktualisieren Sie die Vertrauensrichtlinie der IAM-Rolle, die für die Planung der Abfrage verwendet wurde, damit der IAM-Benutzer sie übernehmen kann.

```
{
            "Sid": "AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/myIAMusername"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Bearbeiten Sie die IAM-Rolle, die Sie angeben, um die Ausführung der geplanten Abfrage zuzulassen, mithilfe der IAM-Konsole (https://console.aws.amazon.com/iam/).

- Ordnen Sie die `AmazonRedshiftDataFullAccess` und `AmazonEventBridgeFullAccess` AWS verwalteten Richtlinien der IAM-Rolle zu. Die verwaltete Richtlinie `AmazonRedshiftDataFullAccess` erteilt `redshift-serverless:GetCredentials` nur Berechtigungen für Redshift-Serverless-Arbeitsgruppen, die mit dem Schlüssel `RedshiftDataFullAccess` gekennzeichnet sind.

Authentifizieren einer geplanten Abfrage

Wenn Sie eine Abfrage planen, verwenden Sie beim Ausführen der SQL-Anweisung eine der folgenden Authentifizierungsmethoden. Jede Methode erfordert eine andere Kombination von Eingaben im Query Editor v2. Diese Authentifizierungsmethoden werden von der Daten-API unterstützt, die zur Ausführung Ihrer SQL-Anweisungen verwendet wird.

Der Datenbankbenutzer oder die Rolle, der bzw. die zum Ausführen der Abfrage verwendet wird, muss über die erforderlichen Datenbankberechtigungen verfügen. Führen Sie den folgenden SQL-Befehl aus, um der Tabelle `mytable` zum Beispiel `IAMR:MyRedshiftQEv2Scheduler`-Berechtigungen zu erteilen.

```
GRANT all ON TABLE mytable TO "IAMR:MyRedshiftQEv2Scheduler";
```

Wenn Sie die Liste der Datenbankbenutzer in Ihrem Cluster oder Ihrer Arbeitsgruppe anzeigen möchten, fragen Sie die Systemansicht `PG_USER_INFO` ab.

> **Note**
>
> Jede Redshift Serverless-Arbeitsgruppe, für die Sie Abfragen planen, muss mit dem Schlüssel gekennzeichnet werden. `RedshiftDataFullAccess` Weitere Informationen finden Sie unter Autorisieren des Zugriffs auf die Amazon Redshift Data API.
> Als Alternative zum Kennzeichnen der Arbeitsgruppe können Sie der IAM-Rolle (die im Zeitplan angegeben ist) eine Inline-Richtlinie hinzufügen, die `redshift-serverless:GetCredentials` erlaubt. Beispielsweise:
>
> ```
> {
>     "Version": "2012-10-17",
>     "Statement": [
>         {
> ```

```
            "Sid": "UseTemporaryCredentialsForAllServerlessWorkgroups",
            "Effect": "Allow",
            "Action": "redshift-serverless:GetCredentials",
            "Resource": [
                "arn:aws:redshift-serverless:*:*:workgroup/*"
            ]
        }
    ]
}
```

AWS Secrets Manager

Geben Sie bei dieser Methode einen Secret-Wert für secret-arn an, der in AWS Secrets Manager gespeichert ist. Dieses Secret enthält Anmeldeinformationen zum Verbinden mit Ihrer Datenbank. Möglicherweise haben Sie bei der Erstellung Ihres Clusters oder Ihrer Arbeitsgruppe ein Geheimnis mit den richtigen Anmeldeinformationen erstellt. Das Secret muss mit dem Schlüssel `RedshiftDataFullAccess` markiert sein. Wenn der Tag-Schlüssel noch nicht vorhanden ist, verwenden Sie die AWS Secrets Manager Konsole, um ihn hinzuzufügen. Hinweise zum Erstellen eines Geheimnisses finden Sie unterEin Geheimnis für Datenbankverbindungsdaten erstellen.

Weitere Informationen zu den Mindestberechtigungen finden Sie unter Erstellen und Verwalten von Secrets mit AWS Secrets Manager im AWS Secrets Manager -Benutzerhandbuch.

Temporäre Anmeldeinformationen

Geben Sie bei dieser Methode Ihre Werte für Datenbankname und Datenbankbenutzer an, wenn Sie eine Verbindung mit einer Datenbank in einem Cluster herstellen. Sie müssen nur Ihren Wert für Datenbankname angeben, wenn Sie eine Verbindung mit einer Datenbank in einer Arbeitsgruppe herstellen.

Wenn Sie eine Verbindung mit einem Cluster herstellen, erteilt die `AmazonRedshiftDataFullAccess`-Richtlinie dem Datenbankbenutzer mit dem Namen `redshift_data_api_user` Berechtigung für `redshift:GetClusterCredentials`. Wenn Sie zum Ausführen der SQL-Anweisung einen anderen Datenbankbenutzer verwenden möchten, fügen Sie der Ihrem Cluster zugewiesenen IAM-Rolle eine Richtlinie hinzu, um `redshift:GetClusterCredentials` zu erlauben. Mit der folgenden Beispielrichtlinie werden die Datenbankbenutzer `awsuser` und `myuser` zugelassen.

```
{
```

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

Festlegen von Berechtigungen zum Anzeigen des Zeitplanverlaufs der Abfrage

Damit Benutzer den Zeitplanverlauf der Abfrage anzeigen können, bearbeiten Sie die IAM-Rolle (die im Zeitplan angegeben ist) Vertrauensstellungen, um Berechtigungen hinzuzufügen.

Das folgende Beispiel zeigt eine Vertrauensrichtlinie in einer IAM-Rolle, die es dem IAM-Benutzer *myIAMusername* erlaubt, den Zeitplanverlauf einer Abfrage anzuzeigen. Anstatt einem IAM-Benutzer `sts:AssumeRole`-Berechtigung zu erteilen, können Sie diese Berechtigung wahlweise einer IAM-Rolle gewähren.

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

Überwachung der geplanten Abfrage

Für das Amazon-SNS-Thema, das Sie für den Versand von E-Mail-Benachrichtigungen angeben, erstellen Sie das Amazon-SNS-Thema mit dem Abfrage-Editor v2, indem Sie zum Abschnitt SNS-Benachrichtigungen navigieren, Aktivieren für die Überwachung und SNS-Thema erstellen auswählen. Der Abfrage-Editor v2 erstellt das Amazon SNS SNS-Thema und fügt der Zugriffsrichtlinie für Amazon EventBridge einen Service Principal hinzu. Das folgende Beispiel zeigt eine Zugriffsrichtlinie, die im Amazon-SNS-Thema erstellt wurde. In dem Beispiel werden die Themen AWS-Region *us-west-2*, AWS-Konto *123456789012* und Amazon SNS verwendet. *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"
    }
  ]
}
```

Wenn die geplante Abfrage ausgeführt wird, sendet Amazon SNS AWS Benachrichtigungs-E-Mails. *Das folgende Beispiel zeigt eine E-Mail, die an myemail@example.com für die geplante Abfrage QS2-May25A gesendet wurde, die auf AWS-Region eu-north-1 in AWS-Konto 123456789012 ausgeführt wurde, wobei das Amazon SNS SNS-Benachrichtigungsthema May25a-SNS verwendet wurde.*

```
{"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
```

Fehlerbehebung bei der Einrichtung oder Planung einer Abfrage

Beachten Sie Folgendes, wenn Sie Probleme beim Planen einer Abfrage haben.

Abfragen, die nicht ausgeführt werden

Prüfen Sie, ob die im Zeitplan verwendete IAM-Rolle berechtigt ist, die temporären Cluster-Anmeldeinformationen abzurufen. Die Berechtigung für bereitgestellte Cluster lautet `redshift:GetClusterCredentialsWithIAM`. Die Berechtigung für Redshift-Serverless-Arbeitsgruppen lautet `redshift-serverless:GetCredentials`.

Der geplante Verlauf wird nicht angezeigt

Der IAM-Benutzer oder die IAM-Rolle, mit der Sie sich bei der Konsole angemeldet haben, wurde nicht zur Vertrauensrichtlinie der IAM-Rolle hinzugefügt, die für die Planung der AWS Abfrage verwendet wurde.

Wenn Sie die Verbindung AWS Secrets Manager für die geplante Abfrage verwenden, vergewissern Sie sich, dass das Geheimnis mit dem Schlüssel gekennzeichnet ist. `RedshiftDataFullAccess`

Wenn die geplante Abfrage eine AWS Secrets Manager Verbindung verwendet, muss der IAM-Rolle, die für die Planung der Abfrage verwendet wird, der Rolle das Äquivalent einer verwalteten Richtlinie `SecretsManagerReadWrite` zugewiesen sein.

Der Status des Abfrageverlaufs lautet **`Failed`**

In der SYS_QUERY_HISTORY-Systemansicht finden Sie Einzelheiten darüber, warum die Abfrage fehlgeschlagen ist. Ein häufiges Problem ist, dass der Datenbankbenutzer oder die Rolle, der bzw. die für die Ausführung der Abfrage verwendet wurde, möglicherweise nicht über die erforderliche Berechtigung zum Ausführen der SQL-Anweisung verfügte. Weitere Informationen finden Sie unter Authentifizieren einer geplanten Abfrage.

Mit der folgenden SQL-Anweisung wird die SYS_QUERY_HISTORY-Ansicht abgefragt, um fehlgeschlagene Abfragen zurückzugeben.

```
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';
```

Details zu einer bestimmten fehlgeschlagenen geplanten Abfrage finden Sie unter Details zu geplanten Abfragen finden Sie mit AWS CloudShell.

Details zu geplanten Abfragen finden Sie mit AWS CloudShell

Sie können AWS CloudShell es verwenden, um Details zu einer Zeitplanabfrage herauszufinden. Sie müssen über die entsprechenden Berechtigungen verfügen, um die im folgenden Verfahren beschriebenen AWS CLI Befehle ausführen zu können.

So zeigen Sie die Ergebnisse einer geplanten Abfrage an

1. Öffnen Sie auf der AWS Konsole die AWS CloudShell Eingabeaufforderung. Weitere Informationen zu AWS CloudShell finden Sie unter Was ist AWS CloudShell im AWS CloudShell Benutzerhandbuch.
2. Übernehmen Sie die IAM-Rolle der geplanten Abfrage. Um die Rolle zu übernehmen, suchen Sie im Abfrage-Editor v2 nach der IAM-Rolle, die der geplanten Abfrage zugeordnet ist, und verwenden Sie sie im AWS CLI Befehl in AWS CloudShell. `scheduler`Geben Sie beispielsweise für die Rolle einen AWS STS Befehl ein, um die Rolle zu übernehmen, die von der geplanten Abfrage verwendet wird.

```
aws sts assume-role –role-arn "arn:aws:iam::123456789012:role/scheduler" –role-
session-name "scheduler-test"
```

Die zurückgegebenen Anmeldeinformationen sehen ähnlich wie die folgenden aus.

```
"Credentials": {
"AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
"SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
"SessionToken": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...",
"Expiration": "2023-08-18T18:19:44+00:00"
},
"AssumedRoleUser": {
"AssumedRoleId": "AROA35B2NH6WBTP7ONL4E:scheduler-test",
"Arn": "arn:aws:sts::123456789012:assumed-role/scheduler/scheduler-test"
}
}
```

3. Erstellen Sie Umgebungsvariablen unter AWS CLI Verwendung der Anmeldeinformationen, die bei der Übernahme der IAM-Rolle angezeigt werden. Sie müssen diese Tokens vor ihrer Ablaufzeit verwenden. Sie geben beispielsweise Folgendes in AWS CloudShell ein.

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
export AWS_SESSION_TOKEN=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...
```

4. Um den Fehler einer fehlgeschlagenen Abfrage anzuzeigen, führen Sie den AWS CLI Befehl zur Beschreibung einer Anweisung aus. Die ID der SQL-Anweisung stammt von der ID, die im Abschnitt Planverlauf einer geplanten Abfrage im Abfrage-Editor v2 angezeigt wird.

```
aws redshift-data describe-statement –id 130d2620-05d2-439c-b7cf-815d9767f513
```

In diesem Beispiel führt der geplante SQL-Code `select * from users limit 100` zu einem SQL-Fehler, weil die Tabelle `users` nicht vorhanden ist.

```
{
"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"
}
```


Demo der Planung einer Abfrage

Eine Demo der Planung einer Abfrage sehen Sie im folgenden Video.Video-Demo der Planung einer Abfrage.

Visualisieren von Abfrageergebnissen

Wenn Sie eine Abfrage ausgeführt haben und die Ergebnisse angezeigt werden, können Sie Chart (Diagramm) aktivieren, um eine grafische Darstellung der aktuellen Ergebnisseite anzuzeigen. Sie können die folgenden Steuerelemente verwenden, um Inhalt, Struktur und Aussehen Ihres Diagramms zu definieren:

-

Trace

Stellt eine Reihe verwandter grafischer Markierungen in einem Diagramm dar. Sie können in einem Diagramm mehrere Traces definieren.

Typ

Sie können den Trace-Typ definieren, um Daten als eine der folgenden darzustellen:

- Streudiagramm für ein Streudiagramm oder ein Blasendiagramm.
- Balkendiagramm zur Darstellung von Datenkategorien mit vertikalen oder horizontalen Balken.
- Flächendiagramm zum Definieren gefüllter Bereiche.
- Histogramm, das Balken verwendet, um die Frequenzverteilung darzustellen.
- Kreisdiagramm für eine kreisförmige Darstellung von Daten, bei denen jedes Stück einen Prozentsatz des Ganzen darstellt.

- Trichter- oder Trichterflächendiagramm zur Darstellung von Daten in verschiedenen Phasen eines Prozesses.
- Das OHLC (open-high-low-close) -Diagramm wird häufig für Finanzdaten verwendet, um offene, hohe, niedrige und geschlossene Werte entlang der X-Achse darzustellen, die normalerweise Zeitintervalle darstellt.
- Kerzendiagramm zur Darstellung eines Wertebereichs für eine Kategorie über einen Zeitraum.
- Wasserfalldiagramm, um darzustellen, wie ein Anfangswert durch eine Reihe von Zwischenwerten zunimmt oder abnimmt. Werte können Zeitintervalle oder Kategorien darstellen.
- Liniendiagramm zur Darstellung von Wertänderungen im Laufe der Zeit.

X-Achse

Sie geben eine Tabellenspalte an, die Werte enthält, die entlang der X-Achse dargestellt werden sollen. Spalten, die beschreibende Werte enthalten, stellen normalerweise dimensionale Daten dar. Spalten, die quantitative Werte enthalten, stellen normalerweise Sachdaten dar.

Y-Achse

Sie geben eine Tabellenspalte an, die Werte enthält, die entlang der Y-Achse dargestellt werden sollen. Spalten, die beschreibende Werte enthalten, stellen normalerweise dimensionale Daten dar. Spalten, die quantitative Werte enthalten, stellen normalerweise Sachdaten dar.

Nebenhandlungen

Sie können zusätzliche Darstellungen von Diagrammdaten definieren.

Transformationen

Sie können Transformationen definieren, um Trace-Daten zu filtern. Sie verwenden eine geteilte Transformation, um mehrere Traces aus einer einzigen Quell-Trace anzuzeigen. Sie verwenden eine Aggregat-Transformation, um eine Trace als Durchschnitt oder Minimum darzustellen. Sie verwenden eine Sortiertransformation, um ein Trace zu sortieren.

Allgemeines Erscheinungsbild

Sie können Standardeinstellungen für Hintergrundfarbe, Randfarbe, Farbskalen zum Entwerfen von Paletten, Textstil und -formaten, Titelstil und -format sowie Modusleiste festlegen. Sie können Interaktionen für Ziehen, Klicken und Zeigen mit der Maus definieren. Sie können Metatext definieren. Sie können Standarddarstellungen für Traces, Achsen, Legenden und Anmerkungen definieren.

Wählen Sie Traces (Ablaufverfolgungen) aus, um die Ergebnisse als Diagramm anzuzeigen. Wählen Sie bei Type den Diagrammstil als Bar (Säulen), Line (Linien) usw. Bei Orientation (Ausrichtung), können Sie Vertical (Vertikal) oder Horizontal auswählen. Wählen Sie mit X die Tabellenspalte für die horizontale Achse aus. Wählen Sie mit Y die Tabellenspalte für die vertikale Achse aus.

Um das Diagramm zu aktualisieren, wählen Sie Refresh (Aktualisieren) aus. Wählen Sie Full screen (Vollbild) aus, um die Diagrammanzeige zu erweitern.

Einen Alarm erstellen

1. Führen Sie eine Abfrage aus und erhalten Sie Ergebnisse.
2. Aktivieren Sie Charts (Diagramme) aus.
3. Wählen Sie Trace (Nachverfolgung) und visualisieren Sie Ihre Daten.
4. Wählen Sie einen der folgenden Diagrammstile aus:

    - Streuung
    - Säulen
    - Flächen
    - Histogramm
    - Kreis
    - Trichter
    - Trichterflächen
    - OHLC () open-high-low-close
    - Kerzen
    - Wasserfall
    - Linien
5. Wählen Sie Style (Stil) aus, um das Erscheinungsbild wie Farben, Achsen, Legende und Anmerkungen anzupassen. Sie können Text, Formen und Bilder hinzufügen.
6. Wählen Sie Annotations (Ergänzungen) aus, um Text, Formen und Bilder hinzuzufügen.

Ein Diagramm speichern

1. Wählen Sie Save Chart (Diagramm speichern) aus.
2. Geben Sie einen Namen für das Diagramm an.
3. Wählen Sie Save (Speichern) aus.

Ein Diagramm exportieren

1. Wählen Sie Export aus.
2. Wählen Sie PNG oder JPEG aus.
3. Legen Sie die Breite und Höhe des Diagramms fest.
4. Wählen Sie Export aus.
5. Öffnen Sie die Datei in Ihrer Standard-Grafikanwendung oder speichern Sie sie unter dem Standardnamen.

Nach einem gespeicherten Diagramm suchen und es öffnen

1. Wählen Sie die Registerkarte Charts (Diagramme) aus.
2. Öffnen Sie das gewünschte Diagramm.

Diagramme in Ordnern organisieren

1. Wählen Sie im Navigationsbereich Charts (Diagramme) aus.
2. Wählen Sie New folder (Neuer Ordner) aus und geben Sie ihm einen Namen.
3. Wählen Sie Create (Erstellen) aus, um den Ordner auf der Registerkarte Charts (Diagramme) zu erstellen.

   Sie können Diagramme mit dem Befehl in den Ordner hinein und aus dem Ordner verschieben. drag-and-drop

Beispiel: Ein Kreisdiagramm zur grafischen Darstellung der Abfrageergebnisse erstellen

Im folgenden Beispiel wird die Tabelle Sales (Umsatz) aus der Beispieldatenbank verwendet. Weitere Informationen finden Sie unter Beispieldatenbank im Datenbankentwicklerhandbuch zu Amazon Redshift.

Im Folgenden finden Sie die Abfrage, die Sie ausführen, um die Daten für das Kreisdiagramm bereitzustellen.

```
select top 5 eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
```

```
where sales.eventid=event.eventid group by eventname
order by 3;
```

Ein Kreisdiagramm für die Top-Veranstaltung nach Gesamtumsatz erstellen

1. Führen Sie die Abfrage aus.
2. Aktivieren Sie im Bereich mit den Abfrageergebnissen Chart (Diagramm).
3. Wählen Sie Trace aus.
4. Wählen Sie unter Type den Typ Pie (Kreis) aus.
5. Wählen Sie bei Values (Werte) totalsales aus.
6. Wählen Sie bei Labels (Markierungen) eventname aus.
7. Wählen Sie bei Style den Stil General (Allgemein) aus.
8. Wählen Sie unter Colorscales (Farbskalen) die Option Categorical (Kategorisch) und dann Pastel2 aus.

Beispiel: Ein Kombinationsdiagramm zum Vergleich von Umsatz und Verkäufen erstellen

Führen Sie die Schritte in diesem Beispiel aus, um ein Diagramm zu erstellen, das ein Balkendiagramm für Umsatzdaten und ein Liniendiagramm für Verkaufsdaten kombiniert. Im folgenden Beispiel wird die Tabelle Sales (Verkäufe) aus der Ticket-Beispieldatenbank verwendet. Weitere Informationen finden Sie unter Beispieldatenbank im Datenbankentwicklerhandbuch zu Amazon Redshift.

Im Folgenden finden Sie die Abfrage, die Sie ausführen, um die Daten für das Diagramm bereitzustellen.

```
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;
```

So erstellen Sie ein Kombinationstabelle zum Vergleich von Umsatz und Verkäufen

1. Führen Sie die Abfrage aus.
2. Aktivieren Sie im Bereich mit den Abfrageergebnissen Chart (Diagramm).
3. Wählen Sie unter trace o für Type (Typ) die Option Bar (Balken) aus.
4. Wählen Sie für Xeventname aus.
5. Wählen Sie für Ytotal_price aus.

   Das Balkendiagramm wird mit Ereignisnamen entlang der X-Achse angezeigt.
6. Wählen Sie unter Style (Stil) Traces aus.
7. Geben Sie für Name die Option Revenue (Umsatz) ein.
8. Wählen Sie unter Style (Stil) die Option Axes (Achsen) aus.
9. Wählen Sie für Title (Titel) die Option Y aus und öffnen Sie Revenue (Umsatz).

   Die Bezeichnung Revenue (Umsatz) wird auf der linken Y-Achse angezeigt.
10. Wählen Sie unter Structure (Struktur) Traces aus.
11. Wählen Sie

    Trace
    aus.

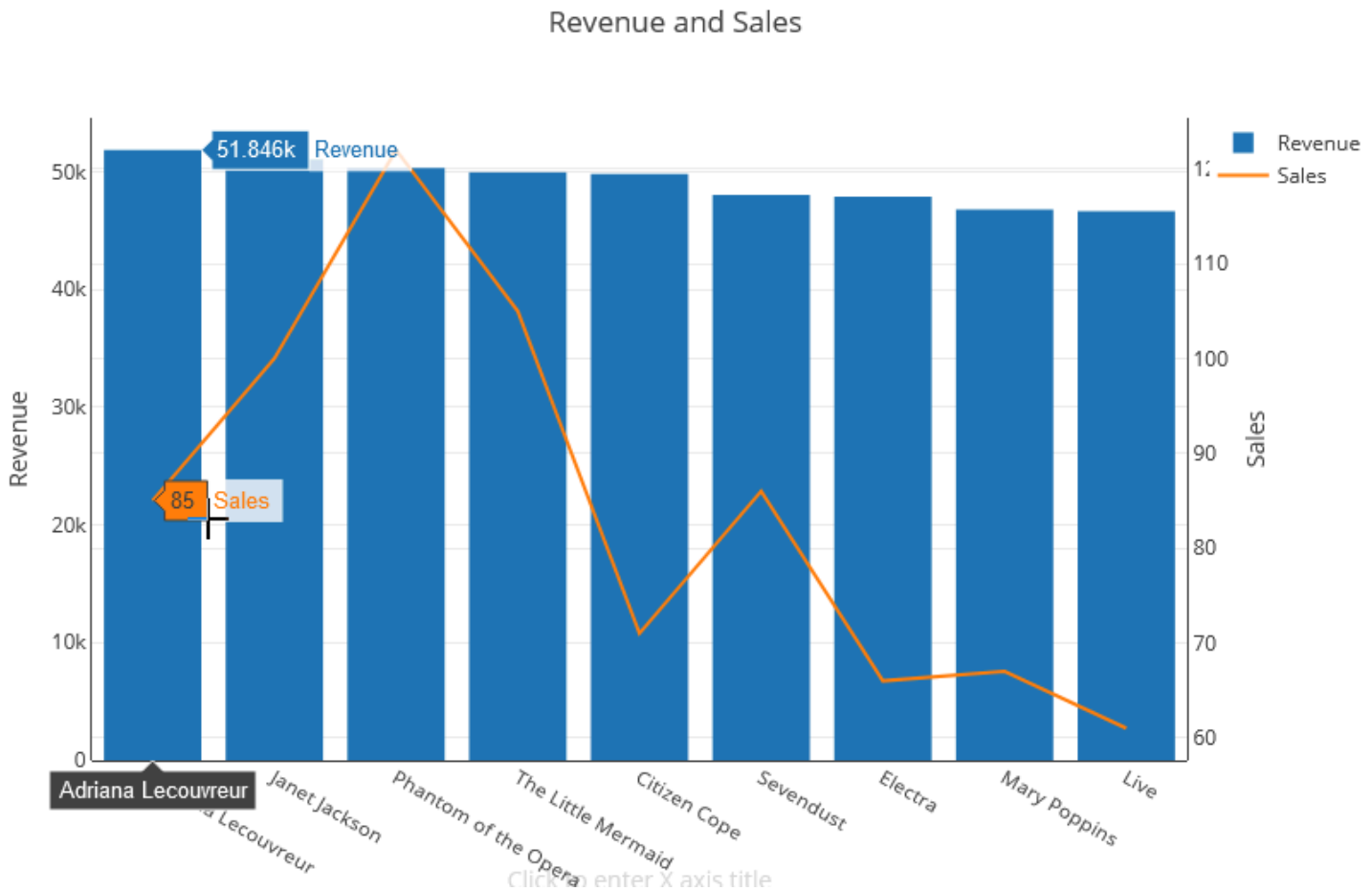
    Die Optionen „Trace 1“ werden angezeigt.
12. Wählen Sie für Type (Typ) die Option Line (Linie) aus.
13. Wählen Sie für Xeventname aus.
14. Wählen Sie für Ytotal_qty_sold aus.

15. Wählen Sie unter Axes To Use (Zu verwendende Achsen) für Y Axis (Y-Achse) die Option

    +

    aus.

    Die Y Axis (Y-Achse) zeigt Y2 an.
16. Wählen Sie unter Style (Stil), Axes (Achsen) aus.
17. Wählen Sie unter Titles (Titel) Y2 aus.
18. Geben Sie für NameSales (Verkäufe) ein.
19. Wählen Sie unter Lines (Linien) Y:Sales (Y:Verkäufe) aus.
20. Wählen unter Axis Line (Achsen-Linie) die Option Show (Anzeigen) und für Position die Option Right (Rechts) aus.



Demo: Visualisierungen mit dem Abfrage-Editor v2 von Amazon Redshift erstellen

Eine Demo zum Erstellen von Visualisierungen finden Sie im folgenden Video. Erstellen von Visualisierungen mit dem Abfrage-Editor v2 von Amazon Redshift.

Zusammenarbeiten und Teilen im Team

Sie können Abfragen mit Ihrem Team teilen.

Ein Team ist für eine Gruppe von Benutzern definiert, die zusammenarbeiten und Ressourcen des Abfrage-Editors v2 gemeinsam nutzen. Ein Administrator kann ein Team erstellen, indem er einer IAM-Rolle ein Tag hinzufügt. Weitere Informationen finden Sie unter Für die Verwendung des Abfrage-Editors v2 erforderliche Berechtigungen .

Speichern, suchen und löschen von Abfragen

Bevor Sie Ihre Abfrage mit Ihrem Team teilen können, speichern Sie sie. Sie können gespeicherte Abfragen anzeigen und löschen.

Eine Abfrage speichern

1. Bereiten Sie Ihre Abfrage vor und wählen Sie Save (Speichern) aus.
2. Geben Sie einen Titel für die Abfrage ein.
3. Wählen Sie Speichern.

Nach gespeicherten Abfragen suchen

1. Wählen Sie im Navigationsbereich Queries (Abfragen) aus.
2. Sie können verschiedene Abfragen sehen: My queries (Meine Abfragen), Shared by me (Von mir geteilt) bzw. Shared to my team (Für mein Team freigegeben). Diese Abfragen können als einzelne Abfragen oder in dafür erstellten Ordnern angezeigt werden.

Eine gespeicherte Abfrage bearbeiten oder löschen

1. Öffnen Sie das Kontextmenü (rechte Maustaste) für eine gespeicherte Abfrage.
2. Wählen Sie Delete (Löschen) und bestätigen Sie die Aktion.

Gespeicherte Abfragen in Ordnern organisieren

1. Wählen Sie im Navigationsbereich Queries (Abfragen) aus.
2. Wählen Sie New folder (Neuer Ordner) aus und geben Sie ihm einen Namen.
3. Wählen Sie Create (Erstellen) aus, sodass der Ordner auf der Registerkarte Queries (Abfragen) entsteht.

   Sie können nun Abfragen mithilfe von in den Ordner und aus diesem verschieben drag-and-drop.

Teilen einer Abfrage

Sie können eigene Abfragen mit Ihrem Team teilen. Sie können auch den Verlauf der gespeicherten Abfragen anzeigen und Abfrageversionen verwalten.

Um eine Abfrage mit Ihrem Team zu teilen, müssen Sie sicherstellen, dass das Prinzipal-Tag `sqlworkbench-team` auf den gleichen Wert wie bei den übrigen Teammitgliedern in Ihrem Konto eingestellt ist. Beispielsweise könnte ein Administrator den Wert für jeden in der Buchhaltungsabteilung auf `accounting-team` einstellen. Ein Beispiel finden Sie unter Für die Verwendung des Abfrage-Editors v2 erforderliche Berechtigungen .

Eine Abfrage mit einem Team teilen

1. Wählen Sie im Navigationsbereich Queries (Abfragen) aus.
2. Öffnen Sie das Kontextmenü der Abfrage, die Sie teilen möchten (rechte Maustaste) und wählen Sie Share with my team (Mit meinem Team teilen) aus.
3. Wählen Sie das Team oder die Teams aus, mit denen Sie die Abfrage teilen möchten, und wählen Sie dann Save sharing options (Freigabeoptionen speichern) aus.

Jede gespeicherte SQL-Abfrage wird vom Abfrage-Editor v2 als neue Version gespeichert. Sie können frühere Abfrageversionen durchsuchen, eine Kopie einer Abfrage speichern oder eine Abfrage wiederherstellen.

Abfrageversionen verwalten

1. Wählen Sie im Navigationsbereich Queries (Abfragen) aus.
2. Öffnen Sie das Kontextmenü für die Abfrage (rechte Maustaste), mit der Sie arbeiten möchten.

3. Wählen Sie auf Version history (Versionshistorie) aus, um eine Liste von Versionen der Abfrage zu öffnen.
4. Auf der Seite Version history (Versionshistorie) haben Sie folgende Möglichkeiten:
   - Revert to selected (Zurück zur Auswahl) – Kehren Sie zur ausgewählten Version zurück und setzen Sie Ihre Arbeit mit dieser Version fort.
   - Save selected under (Auswahl speichern unter) – Erstellen Sie im Editor eine neue Abfrage.

Abfragen für Datenbanken mit dem Abfrage-Editor

Die Verwendung des Abfrage-Editors ist ein einfacher Weg, Abfragen für Datenbanken auszuführen, die von Ihrem Amazon-Redshift-Cluster gehostet werden. Nachdem Sie Ihren Cluster erstellt haben, können Sie mit dem Abfrage-Editor in der Amazon-Redshift-Konsole sofort Abfragen ausführen.

> **Note**
>
> Mit diesem ursprünglichen Abfrage-Editor können Sie in Amazon Redshift Serverless keine Daten abfragen. Verwenden Sie stattdessen den Abfrage-Editor v2 von Amazon Redshift.

Im Februar 2021 wurde ein aktualisierter Abfrage-Editor bereitgestellt und die Autorisierungsberechtigungen zur Verwendung des Abfrage-Editors wurden geändert. Der neue Abfrage-Editor verwendet die Amazon Redshift Data API, um Abfragen auszuführen. Die `AmazonRedshiftQueryEditor` Richtlinie, bei der es sich um eine AWS verwaltete Richtlinie AWS Identity and Access Management (IAM) handelt, wurde aktualisiert und umfasst nun die erforderlichen Berechtigungen. Wenn Sie über eine benutzerdefinierte IAM-Richtlinie verfügen, müssen Sie diese aktualisieren. Verwenden Sie `AmazonRedshiftQueryEditor` als Leitfaden. Die Änderungen an `AmazonRedshiftQueryEditor` umfassen unter anderem:

- Die Berechtigung zum Verwalten der Abfrage-Editor-Anweisungsergebnisse erfordert den Benutzer „Anweisungsinhaber“.
- Die Berechtigung zur Verwendung von Secrets Manager zum Verbinden mit einer Datenbank wurde hinzugefügt.

Weitere Informationen finden Sie unter Erforderliche Berechtigungen zur Verwendung des Abfrage-Editors der Amazon-Redshift-Konsole.

Wenn Sie über den neuen Abfrage-Editor eine Verbindung mit Ihrem Cluster herstellen, können Sie eine von zwei Authentifizierungsmethoden verwenden, wie unter Verbinden mit dem Abfrage-Editor beschrieben.

Mit dem Abfrageeditor können Sie Folgendes tun:

- Sie können einzelne SQL-Abfrageanweisungen ausführen.
- Sie können eine bis zu 100 MB große CSV-Datei (Datei mit durch Kommas getrennten Werten) mit Ergebnismengen herunterladen.
- Sie können Abfragen zur weiteren Verwendung speichern. Sie können Abfragen in der Region Europa (Paris), der Region Asien-Pazifik (Osaka), der Region Asien-Pazifik (Hongkong) und der Region Naher Osten (Bahrain) nicht speichern.
- Sie können Abfragelaufzeitdetails für benutzerdefinierte Tabellen anzeigen.
- Planen Sie Abfragen zur Ausführung zu einem späteren Zeitpunkt.
- Zeigen Sie einen Verlauf von Abfragen an, die Sie im Abfrage-Editor erstellt haben.
- Führen Sie Abfragen für Cluster mit verbessertem VPC-Routing aus.

Überlegungen zum Abfrage-Editor

Beachten Sie Folgendes bei der Arbeit mit Abfragen, wenn Sie den Abfrage-Editor verwenden:

- Die maximale Dauer einer Abfrage beträgt 24 Stunden.
- Die maximale Abfrageergebnisgröße beträgt 100 MB. Wenn ein Aufruf mehr als 100 MB an Antwortdaten zurückgibt, wird der Aufruf beendet.
- Die maximale Aufbewahrungszeit für Abfrageergebnisse beträgt 24 Stunden.
- Die maximale Größe von Abfrageanweisungen beträgt 100 KB.
- Der Cluster muss sich in einer auf dem Amazon-VPC-Service basierenden Virtual Private Cloud (VPC) befinden.
- Im Abfrageeditor können Sie keine Transaktionen verwenden. Weitere Informationen zu Transaktionen finden Sie unter BEGINNEN im Datenbankentwicklerhandbuch zu Amazon Redshift.
- Sie können Abfragen mit bis zu 3 000 Zeichen speichern.

Aktivieren des Zugriffs auf den Abfrage-Editor

Um den Abfrageeditor aufzurufen, benötigen Sie eine Berechtigung. Um den Zugriff zu ermöglichen, empfehlen wir, die `AmazonRedshiftQueryEditor` und die `AmazonRedshiftReadOnlyAccess` AWS verwalteten Richtlinien für IAM-Berechtigungen der IAM-Rolle zuzuordnen, die Sie für den Zugriff auf Ihren Cluster verwenden. Anschließend können Sie die Rolle einem Benutzer zuweisen. Sie können zum Zuweisen von IAM-Richtlinien die IAM-Konsole (https://console.aws.amazon.com/iam/) verwenden. Weitere Informationen finden Sie unter Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon Redshift.

Wenn Sie bereits einen Benutzer für den Zugriff auf Amazon Redshift erstellt haben, können Sie diesem Benutzer die `AmazonRedshiftQueryEditor` und die `AmazonRedshiftReadOnlyAccess` AWS verwalteten Richtlinien mithilfe einer zugewiesenen Rolle zuordnen. Falls Sie noch keinen Benutzer erstellt haben, erstellen Sie einen und fügen Sie die Richtlinie der IAM-Rolle an. Weisen Sie die Rolle dann dem Benutzer zu.

Die AWS verwaltete Richtlinie `AmazonRedshiftQueryEditor` ermöglicht die Aktion`redshift:GetClusterCredentials`, die standardmäßig Superuser-Zugriff auf die Datenbank gewährt. Über einen der folgenden Schritte können Sie den Zugriff beschränken:

- Erstellen Sie eine benutzerdefinierte Richtlinie, die den Aufruf von `redshift:GetClusterCredentials` erlaubt und die Ressource auf einen bestimmten Wert für `DbUser` beschränkt.
- Fügen Sie eine Richtlinie hinzu, die die Erlaubnis für `redshift:GetClusterCredentials` verweigert. Jeder Benutzer, dem eine Rolle mit dieser Berechtigung zugewiesen wurde, muss sich mit temporären Anmeldeinformationen beim Abfrage-Editor anmelden. Diese Ablehnungsrichtlinie wird durch das Beispiel veranschaulicht.

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

Weitere Informationen zum Erstellen einer Rolle mit den erforderlichen Berechtigungen finden Sie unter Erstellen Sie eine IAM-Rolle mit Anrufberechtigungen GetClusterCredentials.

Jeder Benutzer, dem über die AWS verwaltete Richtlinie Zugriff auf den Amazon Redshift Redshift-Abfrage-Editor gewährt wurde, `AmazonRedshiftQueryEditor` kann alle Geheimnisse auflisten. Diese Richtlinie erlaubt jedoch nur das Erstellen und Abrufen von Secrets, die mit dem Schlüssel `RedshiftQueryOwner` und dem Wert `${aws:userid}` markiert sind. Wenn Sie den Schlüssel über den Amazon Redshift Query Editor erstellen, wird der Schlüssel automatisch markiert. Um ein Secret zu verwenden, das nicht mit dem Amazon-Redshift-Abfrage-Editor erstellt wurde, bestätigen Sie, dass das Secret mit dem Schlüssel `RedshiftQueryOwner` und einem Wert Ihrer eindeutigen IAM-Benutzer-ID markiert ist, z. B. `AIDACKCEVSQ6C2EXAMPLE`.

Die erforderlichen Berechtigungen für die Verwendung des Amazon Redshift Redshift-Abfrage-Editors sind AmazonRedshiftQueryEditorund AmazonRedshiftReadOnlyAccess.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Verbinden mit dem Abfrage-Editor

Wenn Sie sich mit dem Abfrage-Editor mit einem Cluster verbinden, verwenden Sie eine der folgenden Authentifizierungsmethoden. Jede Methode erfordert eine andere Kombination von Eingaben von der Amazon-Redshift-Konsole.

AWS Secrets Manager

Geben Sie bei dieser Methode einen Secret-Wert für secret-arn an, der in AWS Secrets Manager gespeichert ist. Dieses Secret enthält Anmeldeinformationen zum Verbinden mit Ihrer Datenbank.

Temporäre Anmeldeinformationen

Geben Sie mit dieser Methode Ihre database- und db-user-Werte an.

Speichern von Datenbankanmeldedaten in AWS Secrets Manager

Wenn Sie den Abfrage-Editor aufrufen, können Sie die Anmeldeinformationen für den Cluster unter Verwendung eines Secrets in AWS Secrets Managerübergeben. Zum Übergeben der Anmeldeinformationen auf diese Weise geben Sie den Namen oder den Amazon-Ressourcennamen (ARN) des Secrets an.

Weitere Informationen zu den Mindestberechtigungen finden Sie unter Erstellen und Verwalten von Secrets mit AWS Secrets Manager im AWS Secrets Manager -Benutzerhandbuch.

So speichern Sie Ihre Anmeldeinformationen in einem Secret für einen Amazon-Redshift-Cluster

1. Wird verwendet AWS Secrets Manager , um einen geheimen Schlüssel zu erstellen, der Anmeldeinformationen für den Cluster enthält. Wenn Sie Store a new secret (Neues Secret speichern) auswählen, wählen Sie Credentials for Redshift cluster (Anmeldedaten für Redshift-Cluster) aus. Speichern Sie einen Wert für User name (Benutzername) (der Datenbankbenutzer),Password (Passwort) und DB cluster (DB-Cluster) (Cluster-ID) in Ihrem Secret.

   Anweisungen finden Sie unter Erstellen eines Basis-Secrets im AWS Secrets Manager -Benutzerhandbuch.
2. Verwenden Sie die AWS Secrets Manager Konsole, um die Details für das von Ihnen erstellte Geheimnis anzuzeigen, oder führen Sie den `aws secretsmanager describe-secret` AWS CLI Befehl aus.

Wenn Sie sich dafür entschieden haben, die Admin-Anmeldeinformationen Ihres Clusters zu verwenden AWS Secrets Manager, können Sie mit Ihren in Secrets Manager gespeicherten Admin-Anmeldeinformationen eine Verbindung zur Datenbank herstellen.

Arbeiten mit dem Abfrage-Editor

Im folgenden Beispiel verwenden Sie den Abfrageeditor, um die folgenden Aufgaben auszuführen:

- SQL-Befehle ausführen
- Abfrageausführungsdetails anzeigen
- Abfrage speichern
- Ergebnissatz einer Abfrage sortieren

Für das folgende Beispiel benötigen Sie einen vorhandenen Amazon-Redshift-Cluster. Wenn Sie über keinen Cluster verfügen, erstellen Sie einen mithilfe des in beschriebenen Verfahrens Erstellen eines Clusters.

So verwenden Sie den Abfrage-Editor in der Amazon-Redshift-Konsole

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü die Option Query editor (Abfrage-Editor) aus und stellen Sie dann eine Verbindung zu einer Datenbank in Ihrem Cluster her.
3. Wählen Sie unter Schema die Option öffentlich aus, um eine neue Tabelle auf der Grundlage dieses Schemas zu erstellen.
4. Geben Sie den folgenden Befehl in das Fenster des Abfrageeditors ein und wählen Sie Run query (Abfrage ausführen) aus, um eine neue Tabelle zu erstellen.

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

5. Klicken Sie auf Clear (Löschen).
6. Geben Sie den folgenden Befehl in das Fenster des Abfrageeditors ein und wählen Sie Run query (Abfrage ausführen) aus, um Zeilen zur Tabelle hinzuzufügen.

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

7. Klicken Sie auf Clear (Löschen).

8. Geben Sie den folgenden Befehl in das Fenster des Abfrageeditors ein und wählen Sie Run query (Abfrage ausführen) aus, um die neue Tabelle abzufragen.

```
select * from shoes;
```

Die Query results (Abfrageergebnisse) zeigen die Ergebnisse an.

Art des Schuhs	Farbe
sandals	black
loafers	brown

9. Wählen Sie Execution (Ausführung) aus, um die Ausführungsdetails anzuzeigen.
10. Wählen Sie Data (Daten) und Export (Exportieren) aus, um die Suchergebnisse als Datei herunterzuladen.

Planen einer Abfrage

> **Important**
>
> Der Amazon Redshift Query Editor v2 unterstützt jetzt die Planung einer Abfrage. Wir empfehlen die Verwendung des Query Editor v2. Weitere Informationen finden Sie unter Planung einer Abfrage mit dem Query Editor v2.

Um einen Zeitplan für die Ausführung einer SQL-Anweisung zu erstellen, können Sie den Abfrage-Editor in der Amazon-Redshift-Konsole verwenden. Sie können einen Zeitplan erstellen, um Ihre SQL-Anweisung in Zeitintervallen auszuführen, die Ihren Geschäftsanforderungen entsprechen. Wenn die geplante Abfrage ausgeführt werden soll, EventBridge initiiert Amazon die Abfrage.

So erstellen Sie einen Zeitplan für die Ausführung einer SQL-Anweisung

1. Öffnen Sie die Konsole und den Abfrage-Editor wie unter Arbeiten mit dem Abfrage-Editor beschrieben. Sie können diesen Abfrage-Editor nur mit bereitgestellten Clustern verwenden.
2. Wählen Sie Schedule (Zeitplan), um einen Zeitplan für die Ausführung einer SQL-Anweisung zu erstellen.

Wenn Sie den Zeitplan definieren, geben Sie die folgenden Informationen an:

- Eine IAM-Rolle, die verwendet wird, um die erforderlichen Berechtigungen zum Ausführen der Abfrage zu übernehmen. Weitere Informationen finden Sie unter Festlegen von Berechtigungen zum Planen einer Abfrage.
- Die Authentifizierungswerte für entweder AWS Secrets Manager oder temporäre Anmeldeinformationen zur Autorisierung des Zugriffs auf Ihren Cluster. Weitere Informationen finden Sie unter Authentifizieren einer geplanten Abfrage.
- Den Namen der geplanten Abfrage und eine einzige SQL-Anweisung, die ausgeführt werden soll.
- Die Zeitplanfrequenz- und Wiederholungsoptionen oder einen cron-formatierten Wert.
- Optional können Sie Amazon-SNS-Benachrichtigungen aktivieren, um die geplante Abfrage zu überwachen. Wenn Ihre Anfrage ausgeführt wird, Sie aber keine Nachrichten sehen, die in Ihrem SNS-Thema veröffentlicht wurden, finden Sie weitere Informationen unter Meine Regel wird ausgelöst, aber ich sehe keine in meinem Amazon SNS SNS-Thema veröffentlichten Nachrichten im EventBridge Amazon-Benutzerhandbuch.

Sie können geplante Abfragen auch über die Amazon-Redshift-Konsole verwalten und aktualisieren. Abhängig von Ihrer Konsolenversion werden geplante Abfragen möglicherweise an folgenden Stellen aufgelistet:

- Auf der Registerkarte Schedules (Zeitpläne) auf der Detailseite Ihres Clusters.
- Auf der Registerkarte Scheduled queries (Geplante Abfragen) im Abfrage-Editor.

Wenn Sie an einer dieser Stellen Schedule name (Zeitplanname) auswählen, können Sie die Definition Ihrer geplanten Abfrage anzeigen und bearbeiten.

Einrichten von Berechtigungen zum Planen einer Abfrage in der Amazon-Redshift-Konsole

Um Abfragen zu planen, müssen der AWS Identity and Access Management (IAM-) Benutzer, der den Zeitplan definiert, und die dem Zeitplan zugeordnete IAM-Rolle wie folgt konfiguriert werden.

Führen Sie für den IAM-Benutzer, der in der Amazon-Redshift-Konsole angemeldet ist, die folgenden Schritte aus:

- Ordnen Sie die `AmazonEventBridgeFullAccess` AWS verwaltete Richtlinie einer IAM-Rolle zu.
- Weisen Sie eine Richtlinie mit der `sts:AssumeRole`-Berechtigung der IAM-Rolle zu, die Sie angeben, wenn Sie die geplante SQL-Anweisung definieren.

  Das folgende Beispiel zeigt eine Richtlinie, die eine angegebene IAM-Rolle übernimmt.

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

Führen Sie für die IAM-Rolle, die Sie angeben, damit der Scheduler eine Abfrage ausführen kann, die folgenden Schritte aus:

- Stellen Sie sicher, dass diese IAM-Rolle den EventBridge Dienstprinzipal () `events.amazonaws.com` angibt. Unten sehen Sie ein Beispiel für eine Vertrauensstellung.

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

Weitere Informationen zum Erstellen einer IAM-Rolle für EventBridge Ereignisse finden Sie unter. Für die Verwendung des Amazon EventBridge Schedulers sind Berechtigungen erforderlich

- Hängen Sie die `AmazonRedshiftDataFullAccess` AWS verwaltete Richtlinie an die IAM-Rolle an.
- Damit Benutzer den Zeitplanverlauf anzeigen können, bearbeiten Sie die IAM-Rolle und fügen Sie die Berechtigung `sts:AssumeRole` hinzu.

Im Folgenden finden Sie ein Beispiel für eine Vertrauensrichtlinie in einer IAM-Rolle.

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

Authentifizieren einer geplanten Abfrage

Wenn Sie eine Abfrage planen, verwenden Sie eine der folgenden Authentifizierungsmethoden, wenn die Abfrage-SQL-Anweisung ausgeführt wird. Jede Methode erfordert eine andere Kombination von Eingaben von der Amazon-Redshift-Konsole.

AWS Secrets Manager

Geben Sie bei dieser Methode einen Secret-Wert für secret-arn an, der in AWS Secrets Manager gespeichert ist. Dieses Secret enthält Anmeldeinformationen zum Verbinden mit Ihrer Datenbank. Das Secret muss mit dem Schlüssel `RedshiftDataFullAccess` markiert sein.

Weitere Informationen zu den Mindestberechtigungen finden Sie unter Erstellen und Verwalten von Secrets mit AWS Secrets Manager im AWS Secrets Manager -Benutzerhandbuch.

Temporäre Anmeldeinformationen

Geben Sie mit dieser Methode Ihre database- und db-user-Werte an.

Die `AmazonRedshiftDataFullAccess`-Richtlinie gewährt dem Datenbankbenutzer namens `redshift_data_api_user` die Berechtigung für `redshift:GetClusterCredentials`. Wenn Sie zum Ausführen der SQL-Anweisung einen anderen Datenbankbenutzer verwenden möchten, fügen Sie der IAM-Rolle eine Richtlinie hinzu, um `redshift:GetClusterCredentials` zu erlauben. Mit der folgenden Beispielrichtlinie werden die Datenbankbenutzer `awsuser` und `myuser` zugelassen.

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

Erstellen Sie eine EventBridge Amazon-Regel, die ausgeführt wird, wenn eine Abfrage abgeschlossen ist

Sie können eine Ereignisregel erstellen, um eine Benachrichtigung zu senden, wenn eine Abfrage abgeschlossen ist. Informationen zum Verfahren mit der EventBridge Amazon-Konsole finden Sie im EventBridge Amazon-Benutzerhandbuch unter Erstellen von EventBridge Amazon-Regeln, die auf Ereignisse reagieren. Weitere Informationen zu Ereignismustern finden Sie unter EventBridge Amazon-Ereignismuster im EventBridge Amazon-Benutzerhandbuch.

Das folgende Beispielereignis wird beispielsweise gesendet, wenn eine Abfrage `FINISHED` ist.

```
{
    "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
    }
}
```

Sie können eine Ereignismusterregel erstellen, um das Ereignis zu filtern.

```
{
    "source": [
        "aws.redshift-data"
    ],
    "detail-type": [
        "Redshift Data Statement Status Change"
    ],
    "detail": {
        "state": [
            "FINISHED"
        ]
    }
}
```

Herstellen einer Verbindung zu einem Amazon Redshift Data Warehouse mithilfe von SQL-Client-Tools

Sie können über SQL-Client-Tools über Java Database Connectivity (JDBC) -, Python- und Open Database Connectivity (ODBC) -Verbindungen eine Verbindung zu Amazon Redshift Data

Warehouses herstellen. Amazon Redshift stellt keine SQL-Client-Tools oder -Bibliotheken bereit oder installiert sie. Um diese Tools oder Bibliotheken für die Arbeit mit Daten in Ihren Data Warehouses zu verwenden, installieren Sie sie auf Ihrem Client-Computer oder Ihrer Amazon EC2 EC2-Instance. Sie können die meisten SQL-Client-Tools verwenden, die JDBC-, Python oder ODBC-Treiber unterstützen.

Anhand der Liste der Abschnitte am Ende dieses Themas können Sie Schritt für Schritt durch die Konfiguration Ihres Client-Computers oder Ihrer Amazon EC2 EC2-Instance für die Verwendung einer JDBC-, Python- oder ODBC-Verbindung gehen. In den Themen werden auch verwandte Sicherheitsoptionen für die Client-Verbindung zum Server erörtert. Darüber hinaus finden Sie Informationen zur Einrichtung und Verbindung von SQL-Client-Tools wie SQL Workbench/J, einem Tool von Drittanbietern, und Amazon Redshift RSQL. Sie können diese Tools ausprobieren, wenn Sie noch kein Business Intelligence-Tool zur Verfügung haben. In diesem Abschnitt erfahren Sie auch, wie Sie programmgesteuert eine Verbindung zu Ihrem Data Warehouse herstellen. Und wenn Sie beim Versuch, eine Verbindung zu Ihrem Data Warehouse herzustellen, auf Probleme stoßen, können Sie sich die Informationen zur Problembehebung ansehen, um Lösungen zu finden.

Empfehlungen für die Verbindung mit Client-Tools

Wenn Sie über eine IP-Adresse eine Verbindung zu Ihrem Redshift-Cluster herstellen, kann dies zu zusätzlichen Ausfallzeiten führen, wenn es zu einem Ausfall oder einem Verbindungsverlust kommt und der Cluster in einer neuen Availability Zone (AZ) online geschaltet wird. Wenn Sie jedoch weiterhin möchten, dass Ihre Anwendung über eine IP-Adresse eine Verbindung zu Redshift herstellt, verwenden Sie die private IP-Adresse, die an den Endpunkt des Clusters virtual-private-cloud (VPC) angehängt ist. Sie finden dies in den Cluster-Details unter Netzwerk und Sicherheit auf der Registerkarte Eigenschaften.

> **Note**
>
> Wenn Ihre Anwendung die IP-Adresse des Leader-Knotens für den Zugriff auf den Redshift-Cluster verwendet, empfiehlt es sich, sie so zu ändern, dass sie die Cluster-Endpunkt-URL verwendet. Weitere Informationen finden Sie unter Verbindungen in Amazon Redshift konfigurieren.

Themen

- Konfigurieren von Verbindungen in Amazon Redshift

- Konfigurieren von Sicherheitsoptionen für Verbindungen
- Herstellen von Verbindungen von Client-Tools aus und mit Code
- Verbinden mit SQL Workbench/J
- Stellen Sie programmgesteuert Connect zu Ihrem Data Warehouse her
- Verwenden eines Authentifizierungsprofils zur Verbindung mit Amazon Redshift
- Beheben von Problemen mit Verbindungen in Amazon Redshift

Konfigurieren von Verbindungen in Amazon Redshift

Im folgenden Abschnitt erfahren Sie, wie Sie JDBC-, Python- und ODBC-Verbindungen zur Herstellung von Verbindungen zu Ihrem Cluster von SQL-Client-Tools aus konfigurieren. In diesem Abschnitt wird die Einrichtung von JDBC-, Python- und ODBC-Verbindungen beschrieben. Außerdem wird beschrieben, wie Secure Sockets Layer (SSL) und Serverzertifikate zur Verschlüsselung der Kommunikation zwischen Client und Server verwendet werden.

JDBC-, Python- und ODBC-Treiber für Amazon Redshift

Um mit Daten in Ihrem Cluster zu arbeiten, benötigen Sie JDBC-, Python- oder ODBC-Treiber, um Verbindungen von Ihrem Client-Computer oder Ihrer Instance aus herstellen zu können. Sie kodieren Ihre Anwendungen für die Verwendung von JDBC-, Python- oder ODBC-API-Operationen für den Zugriff auf Daten und verwenden SQL-Client-Tools, die JDBC, Python oder ODBC unterstützen.

Amazon Redshift stellt JDBC-, Python- und ODBC-Treiber zum Download bereit. Diese Treiber werden von AWS Support unterstützt. PostgreSQL-Treiber sind nicht getestet und werden vom Amazon-Redshift-Team nicht unterstützt. Verwenden Sie die Amazon-RedShift-spezifischen Treiber, wenn Sie eine Verbindung zu einem Amazon-Redshift-Cluster herstellen. Die Amazon-Redshift-Treiber bieten die folgenden Vorteile:

- Unterstützung für IAM, SSO und Verbundauthentifizierung.
- Unterstützung für neue Amazon-Redshift-Datentypen.
- Unterstützung für Authentifizierungsprofile.
- Verbesserte Leistung in Verbindung mit Amazon-Redshift-Verbesserungen.

Weitere Informationen zum Download der JDBC- und ODBC-Treiber und zur Konfigurierung von Verbindungen für Ihren Cluster finden Sie unter Konfigurieren einer Verbindung für JDBC-

Treiberversion 2.1 für Amazon Redshift, Konfigurieren des Amazon-Redshift-Python-Konnektors und Konfigurierung einer ODBC-Verbindung.

Weitere Informationen zur Verwaltung von IAM-Identitäten, einschließlich bewährter Methoden für IAM-Rollen, finden Sie unter Identity and Access Management in Amazon Redshift.

Suche der Zeichenfolge für die Verbindung mit dem Cluster

Um Ihren Cluster mit Ihrem SQL-Client-Tool zu verbinden, benötigen Sie die Cluster-Verbindungszeichenfolge. Sie finden die Cluster-Verbindungszeichenfolge in der Amazon-Redshift-Konsole auf der Detailseite eines Clusters.

So finden Sie die Verbindungszeichenfolge für einen Cluster:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü die Option Clusters (Cluster) und dann in der Liste den Cluster-Namen aus, um die Details zu dem Cluster aufzurufen.
3. Die JDBC-URL- und ODBC-URL-Verbindungszeichenfolgen finden Sie zusammen mit zusätzlichen Details im Abschnitt Allgemeine Informationen. Jede Zeichenfolge basiert auf der AWS Region, in der der Cluster ausgeführt wird. Klicken Sie auf das Symbol neben der entsprechenden Verbindungszeichenfolge, um sie zu kopieren.

Um eine Verbindung zu einem Cluster-Endpunkt herzustellen, können Sie die Cluster-Endpunkt-URL aus einer DescribeClusters API-Anfrage verwenden. Das folgende Beispiel zeigt eine Cluster-Endpunkt-URL.

```
mycluster.cmeaswqeuae.us-east-2.redshift.amazonaws.com
```

Wenn Sie einen benutzerdefinierten Domain-Namen für Ihren Cluster eingerichtet haben, können Sie diesen auch verwenden, um eine Verbindung mit Ihrem Cluster herzustellen. Weitere Hinweise zum Erstellen eines benutzerdefinierten Domain-Namens finden Sie unter Einrichten eines benutzerdefinierten Domain-Namens.

> **Note**
>
> Wenn Sie eine Verbindung herstellen, benutzen Sie nicht die IP-Adresse eines Cluster-Knotens oder die IP-Adresse des VPC-Endpunkts. Benutzen Sie immer den Redshift-

Endpunkt, um einen unnötigen Ausfall zu vermeiden. Die einzige Ausnahme bei der Benutzung der Endpunkt-URL ist die Verwendung eines benutzerdefinierten Domain-Namens. Weitere Informationen finden Sie unter Verwendung eines benutzerdefinierten Domain-Namens für Client-Verbindungen.

Konfigurieren einer Verbindung für JDBC-Treiberversion 2.1 für Amazon Redshift

Für zahlreiche SQL-Client-Tools von Drittanbietern können Sie eine Verbindung mit JDBC-Treiberversion 2.1 verwenden, um Ihren Amazon-Redshift-Cluster zu verbinden. Der Amazon-Redshift-JDBC-Konnektor stellt eine Open-Source-Lösung bereit. Sie können den Quellcode durchsuchen, Verbesserungen anfordern, Probleme melden und Beiträge bereitstellen.

Informationen zur Verwendung einer JDBC-Verbindung finden Sie in den folgenden Abschnitten.

Themen

- Herunterladen von Version 2.1 des JDBC-Treibers für Amazon Redshift
- Installieren von Version 2.1 des JDBC-Treibers für Amazon Redshift
- Abrufen der JDBC-URL
- Erstellen der Verbindungs-URL
- Konfigurieren von TCP-Keepalives für Ihre JDBC-Verbindung
- Konfigurieren Ihrer JDBC-Verbindung mit Apache Maven
- Konfigurieren von Authentifizierung und SSL
- Konfigurieren der Protokollierung
- Konvertieren von Datentypen
- Unterstützung für vorbereitete Anweisungen verwenden
- Unterschiede zwischen den Versionen 2.1 und 1.x des JDBC-Treibers
- Erstellen von Initialisierungsdateien (.ini) für JDBC-Treiberversion 2.1
- Konfigurationsoptionen der JDBC-Treiberversion 2.1
- Bisherige Versionen der JDBC-Treiberversion 2.1

Herunterladen von Version 2.1 des JDBC-Treibers für Amazon Redshift

Amazon Redshift bietet Treiber für Tools, die mit der JDBC 4.2 API kompatibel sind. Der Klassenname für diesen Treiber ist `com.amazon.redshift.Driver`.

Ausführliche Informationen zur Installation des JDBC-Treibers, Referenzen zu JDBC-Treiberbibliotheken und zur Registrierung der Treiberklasse finden Sie in den folgenden Themen.

Überprüfen Sie für jeden Computer, auf dem Sie JDBC-Treiberversion 2.1 für Amazon Redshift verwenden, ob Java Runtime Environment (JRE) 8.0 installiert ist.

Wenn Sie den Amazon-Redshift-JDBC-Treiber für die Datenbank-Authentifizierung verwenden, muss der Pfad Ihrer Java-Klasse das AWS SDK for Java 1.11.118 oder höher enthalten. Falls Sie es nicht AWS SDK for Java installiert haben, laden Sie die ZIP-Datei mit JDBC 4.2-kompatiblen Treibern und treiberabhängigen Bibliotheken für das SDK herunter: AWS

- JDBC 4.2-kompatible Treiberversion 2.1 und vom AWS SDK-Treiber abhängige Bibliotheken Verwenden Sie in der Region China (Peking) den folgenden Link: SDK-Treiber abhängige Bibliotheken AWS

  Diese ZIP-Datei enthält die JDBC 4.2-kompatible Treiberversion 2.1 und die vom AWS SDK for Java 1.x treiberabhängigen Bibliotheksdateien. Entpacken Sie die abhängigen JAR-Dateien an denselben Speicherort wie den JDBC-Treiber. Nur der JDBC-Treiber muss sich in CLASSPATH befinden.

  Diese ZIP-Datei enthält nicht das komplette AWS SDK for Java 1.x. Es enthält jedoch das AWS SDK for Java 1.x-Treiberbibliotheken, die für die AWS Identity and Access Management (IAM-) Datenbankauthentifizierung erforderlich sind.

  Verwenden Sie diesen Amazon Redshift JDBC-Treiber mit dem AWS SDK, das für die IAM-Datenbankauthentifizierung erforderlich ist.

  Informationen zur Installation des vollständigen AWS SDK for Java 1.x finden Sie unter AWS SDK for Java 1.x im AWS SDK for Java Developer Guide.
- JDBC 4.2-kompatible Treiberversion 2.1 (ohne AWS SDK) Verwenden Sie in der Treiberversion 2.1 (ohne SDK) AWS

Lesen Sie die Softwarelizenz und das Änderungsprotokoll der JDBC-Treiberversion 2.1:

- Lizenz der JDBC-Treiberversion 2.1
- Änderungsprotokoll der JDBC-Treiberversion 2.1

Die JDBC-Treiberversionen 1.2.27.1051 und höher unterstützen in Amazon Redshift gespeicherte Prozeduren. Weitere Informationen finden Sie unter Erstellen von gespeicherten Prozeduren in Amazon Redshift im Datenbankentwicklerhandbuch zu Amazon Redshift.

Installieren von Version 2.1 des JDBC-Treibers für Amazon Redshift

Um die Amazon Redshift JDBC 4.2-kompatible Treiberversion 2.1 und die treiberabhängigen Bibliotheken für das AWS SDK zu installieren, extrahieren Sie die Dateien aus dem ZIP-Archiv in das Verzeichnis Ihrer Wahl.

Um die Amazon Redshift JDBC 4.2-kompatible Treiberversion 2.1 (ohne AWS SDK) zu installieren, kopieren Sie die JAR-Datei in das Verzeichnis Ihrer Wahl.

Um mithilfe des Amazon-Redshift-JDBC-Treibers auf einen Amazon-Redshift-Datenspeicher zuzugreifen, müssen Sie die Konfiguration wie folgt durchführen.

Themen

- Verweisen auf die JDBC-Treiberbibliotheken
- Registrieren der Treiberklasse

Verweisen auf die JDBC-Treiberbibliotheken

Die JDBC-Anwendung oder der Java-Code, mit der bzw. dem Sie eine Verbindung zu Ihren Daten herstellen, muss auf die JAR-Dateien des Treibers zugreifen. Geben Sie in der Anwendung oder im Code alle JAR-Dateien an, die Sie aus dem Zip-Archiv extrahiert haben.

Verwenden des Treibers in einer JDBC-Anwendung

JDBC-Anwendungen bieten in der Regel eine Reihe von Konfigurationsoptionen zum Hinzufügen einer Liste von Treiberbibliotheksdateien. Verwenden Sie die bereitgestellten Optionen, um alle JAR-Dateien aus dem Zip-Archiv als Teil der Treiberkonfiguration in die Anwendung aufzunehmen. Weitere Informationen finden Sie in der Dokumentation zu Ihrer JDBC-Anwendung.

Verwenden des Treibers in Java-Code

Sie müssen alle Treiberbibliotheksdateien in den Klassenpfad aufnehmen. Dies ist der Pfad, den die Java Runtime Environment nach Klassen und anderen Ressourcendateien durchsucht. Weitere Informationen finden Sie in der entsprechenden Java-SE-Dokumentation, um den Klassenpfad für Ihr Betriebssystem festzulegen.

- Windows: https://docs.oracle.com/javase/7/docs/technotes/tools/windows/classpath.html
- Linux und Solaris: https://docs.oracle.com/javase/7/docs/technotes/tools/solaris/classpath.html
- macOS: Der standardmäßige macOS-Klassenpfad ist das Verzeichnis, in dem der JDBC-Treiber installiert ist.

Registrieren der Treiberklasse

Stellen Sie sicher, dass Sie die entsprechende Klasse für Ihre Anwendung registrieren. Die folgenden Klassen werden verwendet, um den Amazon-Redshift-JDBC-Treiber mit Amazon-Redshift-Datenspeichern zu verbinden:

- `Driver` Klassen erweitern `java.sql.Driver`.
- `DataSource`-Klassen erweitern `javax.sql.DataSource` und `javax.sql.ConnectionPoolDataSource`.

Der Treiber unterstützt die folgenden vollständig qualifizierten Klassennamen, die unabhängig von der JDBC-Version sind:

- `com.amazon.redshift.jdbc.Driver`
- `com.amazon.redshift.jdbc.DataSource`

Das folgende Beispiel zeigt, wie die DriverManager Klasse verwendet wird, um eine Verbindung für JDBC 4.2 herzustellen.

```
            private static Connection connectViaDM() throws Exception
{
Connection connection = null;
connection = DriverManager.getConnection(CONNECTION_URL);
return connection;
}
```

Das folgende Beispiel zeigt, wie Sie mithilfe der `DataSource`-Klasse eine Verbindung herstellen.

```
 private static Connection connectViaDS() throws Exception
{
```

```
Connection connection = null;
11
Amazon Redshift JDBC Driver Installation and Configuration Guide
DataSource ds = new com.amazon.redshift.jdbc.DataSource
();
ds.setURL(CONNECTION_URL);
connection = ds.getConnection();
return connection;
}
```

Abrufen der JDBC-URL

Sie müssen die JDBC-URL Ihres Clusters kennen, bevor Sie aus einem SQL-Client-Tool eine Verbindung mit Ihrem Amazon-Redshift-Cluster herstellen können. Die JDBC-URL hat das folgende Format: `jdbc:redshift://`*`endpoint`*`:`*`port`*`/`*`database`*.

Die Felder des vorhergehenden Formats haben die folgenden Werte.

Field (Feld)	Value (Wert)
`jdbc`	Das Protokoll für die Verbindung.
`redshift`	Das Unterprotokoll, das die Verwendung des Amazon-Redshift-Treibers angibt, um eine Verbindung mit der Datenbank herzustellen.
`endpoint`	Der Endpunkt für den Amazon-Redshift-Cluster.
`port`	Die Portnummer, die Sie beim Starten des Clusters angegeben haben. Wenn Sie eine Firewall haben, muss dieser Port geöffnet sein, damit Sie ihn verwenden können.
`database`	Die Datenbank, die Sie für Ihren Cluster erstellt haben.

Im Folgenden wird ein Beispiel für eine JDBC-URL gezeigt:`jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev`

Achten Sie darauf, die URL-Werte, z. B. SessionToken Werte, im URL-codierten Format einzugeben.

Informationen darüber, wie Sie Ihre JDBC-Verbindung herstellen können, finden Sie unter Suche der Zeichenfolge für die Verbindung mit dem Cluster.

Wenn der Client-Computer keine Verbindung mit der Datenbank herstellen kann, können Sie mögliche Fehler beheben. Weitere Informationen finden Sie unter Beheben von Problemen mit Verbindungen in Amazon Redshift.

Erstellen der Verbindungs-URL

Verwenden Sie die Verbindungs-URL, um Verbindungsinformationen für den Datenspeicher bereitzustellen, auf den Sie zugreifen. Im Folgenden finden Sie das Format der Verbindungs-URL für die Amazon-Redshift-JDBC-Treiberversion 2.1. Hier ist [Host] der Endpunkt des Amazon-Redshift-Servers und [Port] die Nummer des TCP-Ports (Transmission Control Protocol), den der Server für Clientanforderungen verwendet.

```
jdbc:redshift://[Host]:[Port]
```

Im Folgenden finden Sie das Format einer Verbindungs-URL, die einige optionale Einstellungen angibt.

```
jdbc:redshift://[Host]:[Port]/[database];[Property1]=[Value];
[Property2]=[Value];
```

Beispiel: Sie möchten eine Verbindung mit Port 9000 auf einem Amazon-Redshift-Cluster in der Region USA West (Nordkalifornien) auf herstellen AWS. Sie möchten auch auf die Datenbank `dev` zugreifen und die Verbindung mithilfe eines Benutzernamens und eines Passworts authentifizieren. In diesem Fall verwenden Sie die folgende Verbindungs-URL.

```
jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/
dev;UID=amazon;PWD=amazon
```

Sie können die folgenden Zeichen verwenden, um Konfigurationsoptionen vom Rest der URL-Zeichenfolge zu trennen:

- ;
- ?

Beispielsweise sind die folgenden URL-Zeichenfolgen gleichwertig:

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

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

Sie können die folgenden Zeichen verwenden, um Konfigurationsoptionen in der URL-Zeichenfolge voneinander zu trennen:

- ;
- &

Beispielsweise sind die folgenden URL-Zeichenfolgen gleichwertig:

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

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

Das folgende URL-Beispiel gibt die Protokollebene 6 und den Pfad für die Protokolle an.

```
jdbc:redshift://redshift.amazonaws.com:5439/dev;DSILogLevel=6;LogPath=/home/user/logs;
```

Duplizieren Sie keine Eigenschaften in der Verbindungs-URL.

Eine vollständige Liste der Konfigurationsoptionen, die Sie angeben können, finden Sie unter Konfigurationsoptionen der JDBC-Treiberversion 2.1.

> **Note**
>
> Wenn Sie eine Verbindung herstellen, benutzen Sie nicht die IP-Adresse eines Cluster-Knotens oder die IP-Adresse des VPC-Endpunkts. Benutzen Sie immer den Redshift-Endpunkt, um einen unnötigen Ausfall zu vermeiden. Die einzige Ausnahme bei der Benutzung der Endpunkt-URL ist die Verwendung eines benutzerdefinierten Domain-Namens. Weitere Informationen finden Sie unter Verwendung eines benutzerdefinierten Domain-Namens für Client-Verbindungen.

Konfigurieren von TCP-Keepalives für Ihre JDBC-Verbindung

Standardmäßig ist der Amazon-Redshift-JDBC-Treiber für die Verwendung von TCP-Keepalives zur Verhinderung von Timeouts von Verbindungen konfiguriert. Sie können festlegen, wann der Treiber mit dem Senden von Keepalive-Paketen beginnt. Sie können die Funktion auch deaktivieren, indem

Sie die entsprechenden Eigenschaften in der Verbindungs-URL festlegen. Weitere Informationen zur Syntax der Verbindungs-URL finden Sie unter Erstellen der Verbindungs-URL.

Property (Eigenschaft)	Description (Beschreibung)
`TCPKeepAlive`	Um TCP-Keepalives zu deaktivieren, setzen Sie diese Eigenschaft auf `FALSE`.

Konfigurieren Ihrer JDBC-Verbindung mit Apache Maven

Apache Maven ist ein Tool für die Verwaltung und Untersuchung von Softwareprojekten. Das AWS SDK for Java unterstützt Apache Maven-Projekte. Weitere Informationen finden Sie unter Verwendung des SDK mit Apache Maven im AWS SDK for Java -Entwicklerhandbuch.

Wenn Sie Apache Maven verwenden, können Sie Ihre Projekte konfigurieren und erstellen, sodass diese einen Amazon-Redshift-JDBC-Treiber für die Verbindung mit Ihrem Amazon-Redshift-Cluster verwenden. Hierzu fügen Sie der Datei `pom.xml` Ihres Projekts den JDBC-Treiber als Abhängigkeit hinzu. Wenn Sie Apache Maven für die Erstellung Ihres Projekts verwenden und eine JDBC-Verbindung verwenden möchten, führen Sie die Schritte im folgenden Abschnitt aus.

Konfigurieren des JDBC-Treibers als Maven-Abhängigkeit

So konfigurieren Sie den JDBC-Treiber als Maven-Abhängigkeit

1. Fügen Sie entweder das Amazon-Repository oder das Maven-Central-Repository im Repositorys-Abschnitt Ihrer `pom.xml`-Datei hinzu.

   > **Note**
   >
   > Die URL im folgenden Codebeispiel gibt einen Fehler zurück, wenn sie in einem Browser verwendet wird. Sie können diese URL nur im Kontext eines Maven-Projekts verwenden.

   Verwenden Sie für ein Amazon-Maven-Repository Folgendes.

```
<repositories>
    <repository>
      <id>redshift</id>
```

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

Zum Herstellen der Verbindung mit Secure Sockets Layer (SSL) fügen Sie Ihrer `pom.xml`-Datei das folgende Repository hinzu.

```
<repositories>
    <repository>
      <id>redshift</id>
      <url>https://s3.amazonaws.com/redshift-maven-repository/release</url>
    </repository>
</repositories>
```

Fügen Sie für ein Maven-Central-Repository Folgendes zu Ihrer `pom.xml`-Datei hinzu.

```
<repositories>
    <repository>
      <id>redshift</id>
      <url>https://repo1.maven.org/maven2</url>
    </repository>
</repositories>
```

2. Deklarieren Sie im Abschnitt mit den Abhängigkeiten in Ihrer `pom.xml`-Datei die Version des Treibers, den Sie verwenden möchten.

   Amazon Redshift bietet Treiber für Tools, die mit der JDBC 4.2 API kompatibel sind. Informationen zu der von diesen Treibern unterstützten Funktionalität finden Sie unter Herunterladen von Version 2.1 des JDBC-Treibers für Amazon Redshift.

   Fügen Sie dem Treiber wie folgt eine Abhängigkeit hinzu.

   Ersetzen Sie *`driver-version`* im folgenden Beispiel mit Ihrer Treiberversion, z. B. `2.1.0.1`.

   Verwenden Sie für einen JDBC-4.2-kompatiblen Treiber Folgendes.

```
<dependency>
   <groupId>com.amazon.redshift</groupId>
   <artifactId>redshift-jdbc42</artifactId>
   <version>driver-version</version>
```

```
</dependency>
```

Der Klassenname für diesen Treiber ist `com.amazon.redshift.Driver`.

Die Amazon-Redshift-Maven-Treiber benötigen die folgenden optionalen Abhängigkeiten, wenn Sie die IAM-Datenbankauthentifizierung verwenden.

```
<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>
```

Aktualisieren des Treibers auf die neueste Version

Um den Amazon-Redshift-JDBC-Treiber auf die neueste Version zu aktualisieren oder zu ändern, ändern Sie zunächst den Versionsabschnitt der Abhängigkeit von der neuesten Version des Treibers. Dann bereinigen Sie Ihr Projekt mit dem Maven Clean Plugin, wie unten gezeigt.

```
mvn clean
```

Konfigurieren von Authentifizierung und SSL

Um Daten vor unbefugtem Zugriff zu schützen, erfordern Amazon-Redshift-Datenspeicher, dass alle Verbindungen mit Benutzeranmeldeinformationen authentifiziert werden. Einige Datenspeicher

erfordern auch, dass Verbindungen über das Secure Sockets Layer (SSL)-Protokoll hergestellt werden, entweder mit oder ohne unidirektionaler Authentifizierung.

Die Amazon-Redshift-JDBC-Treiberversion 2.1 bietet volle Unterstützung für diese Authentifizierungsprotokolle.

Die SSL-Version, die der Treiber unterstützt, hängt von der JVM-Version ab, die Sie verwenden. Informationen zu den SSL-Versionen, die von jeder Java-Version unterstützt werden, finden Sie unter Diagnose von TLS, SSL und HTTPS im Java Platform Group Product Management Blog.

Die SSL-Version, die für die Verbindung verwendet wird, ist die höchste Version, die sowohl vom Treiber als auch vom Server unterstützt wird, die zum Zeitpunkt der Verbindung bestimmt wird.

Konfigurieren Sie die Amazon-Redshift-JDBC-Treiberversion 2.1 für die Authentifizierung Ihrer Verbindung gemäß den Sicherheitsanforderungen des Redshift-Servers, mit dem Sie eine Verbindung herstellen.

Sie müssen immer Ihren Benutzernamen und Ihr Passwort für Redshift angeben, um die Verbindung zu authentifizieren. Abhängig davon, ob SSL auf dem Server aktiviert und erforderlich ist, müssen Sie den Treiber möglicherweise auch für die Verbindung über SSL konfigurieren. Möglicherweise müssen Sie eine unidirektionale SSL-Authentifizierung verwenden, damit der Client (der Treiber selbst) die Identität des Servers überprüft.

Sie geben die Konfigurationsinformationen an den Treiber in der Verbindungs-URL an. Weitere Informationen zur Syntax der Verbindungs-URL finden Sie unter Erstellen der Verbindungs-URL.

SSL gibt TLS/SSL an, sowohl Transport Layer Security als auch Secure Sockets Layer. Der Treiber unterstützt in der Branche übliche Versionen von TLS/SSL.

Nur mit Benutzername und Passwort

Wenn der Server, mit dem Sie eine Verbindung herstellen, kein SSL verwendet, müssen Sie nur Ihren Redshift-Benutzernamen und Ihr Passwort angeben, um die Verbindung zu authentifizieren.

So konfigurieren Sie die Authentifizierung nur mit Ihrem Redshift-Benutzernamen und Passwort

1. Legen Sie den Wert für die Eigenschaft `UID` auf Ihren Redshift-Benutzernamen fest, um auf den Amazon-Redshift-Server zuzugreifen.
2. Legen Sie die Eigenschaft PWD auf das Passwort fest, das Ihrem Redshift-Benutzernamen entspricht.

Verwenden von SSL ohne Identitätsüberprüfung

Wenn der Server, zu dem Sie eine Verbindung herstellen, SSL verwendet, aber keine Identitätsüberprüfung erfordert, können Sie den Treiber so konfigurieren, dass er eine nicht validierende SSL-Factory verwendet.

So konfigurieren Sie eine SSL-Verbindung ohne Identitätsprüfung

1. Legen Sie den Wert für die Eigenschaft `UID` auf Ihren Redshift-Benutzernamen fest, um auf den Amazon-Redshift-Server zuzugreifen.
2. Legen Sie die Eigenschaft `PWD` auf das Passwort fest, das Ihrem Redshift-Benutzernamen entspricht.
3. Legen Sie die Eigenschaft `SSLFactory` auf `com.amazon.redshift.ssl.NonValidatingFactory` fest.

Verwenden einer unidirektionalen SSL-Authentifizierung

Wenn der Server, zu dem Sie eine Verbindung herstellen, SSL verwendet und über ein Zertifikat verfügt, können Sie den Treiber so konfigurieren, dass er die Identität des Servers mithilfe einer unidirektionalen Authentifizierung überprüft.

Für die unidirektionale Authentifizierung ist ein signiertes, vertrauenswürdiges SSL-Zertifikat erforderlich, um die Identität des Servers zu überprüfen. Sie können den Treiber so konfigurieren, dass er ein bestimmtes Zertifikat verwendet oder auf ein Zertifikat zugreifen kann TrustStore , das das entsprechende Zertifikat enthält. Wenn Sie kein Zertifikat oder angeben TrustStore, verwendet der Treiber das Standard-Java TrustStore (normalerweise entweder `jssecacerts` oder`cacerts`).

So konfigurieren Sie die unidirektionale SSL-Authentifizierung

1. Legen Sie den Wert für die Eigenschaft UID auf Ihren Redshift-Benutzernamen fest, um auf den Amazon-Redshift-Server zuzugreifen.
2. Legen Sie die Eigenschaft PWD auf das Passwort fest, das Ihrem Redshift-Benutzernamen entspricht.
3. Legen Sie die Eigenschaft SSL auf true fest.
4. Stellen Sie die RootCert SSL-Eigenschaft auf den Speicherort Ihres Root-CA-Zertifikats ein.
5. Wenn Sie kein Standard-Java verwenden TrustStores, führen Sie einen der folgenden Schritte aus:

- Um ein Serverzertifikat anzugeben, setzen Sie die RootCert SSL-Eigenschaft auf den vollständigen Pfad des Zertifikats.
- Gehen Sie wie folgt vor TrustStore, um ein anzugeben:

  a. Verwenden Sie das Keytool-Programm, um dem Serverzertifikat, das Sie verwenden möchten TrustStore, das Serverzertifikat hinzuzufügen.

  b. Geben Sie das TrustStore und das Passwort an, das beim Starten der Java-Anwendung mit dem Treiber verwendet werden soll. Beispielsweise:

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

6. Wählen Sie eine aus:
   - Um das Zertifikat zu validieren, legen Sie die Eigenschaft SSLMode auf verify-ca fest.
   - Um das Zertifikat zu validieren und den Hostnamen im Zertifikat zu verifizieren, legen Sie die Eigenschaft SSLMode auf verify-full fest.

Konfigurieren der IAM-Authentifizierung

Wenn Sie eine Verbindung mit einem Amazon-Redshift-Server über die IAM-Authentifizierung herstellen, legen Sie die folgenden Eigenschaften als Teil Ihrer Datenquellen-Verbindungszeichenfolge fest.

Weitere Informationen zur IAM-Authentifizierung finden Sie unter Identity and Access Management in Amazon Redshift.

Verwenden Sie für die Verwendung der IAM-Authentifizierung eines der folgenden Verbindungszeichenfolgenformate:

Verbindungszeichenfolge	Beschreibung
`jdbc:redshift:iam:// [host]:[port]/[db]`	Eine reguläre Verbindungszeichenfolge. Der Treiber leitet die ClusterID und die Region vom Host ab.

Verbindungszeichenfolge	Beschreibung
`jdbc:redshift:iam:// [cluster-id]: [region]/[db]`	Der Treiber ruft Hostinformationen unter Berücksichtigung der ClusterID und der Region ab.
`jdbc:redshift:iam:// [host]/[db]`	Der Treiber ist standardmäßig auf Port 5439 eingestellt und leitet die ClusterID und die Region vom Host ab. Erlauben Sie den Zugriff auf den ausgewählten Port, je nachdem, welchen Port Sie beim Erstellen, Ändern oder Migrieren des Clusters ausgewählt haben.

Angeben von Profilen

Wenn Sie IAM-Authentifizierung verwenden, können Sie zusätzliche erforderliche oder optionale Verbindungseigenschaften unter einem Profilnamen angeben. Dadurch können Sie vermeiden, dass bestimmte Informationen direkt in die Verbindungszeichenfolge eingefügt werden. Sie geben den Profilnamen in der Verbindungszeichenfolge mithilfe der Eigenschaft Profile an.

Profile können der AWS Anmeldeinformationsdatei hinzugefügt werden. Das Standardverzeichnis für diese Datei ist: `~/.aws/credentials`

Sie können den Standardwert ändern, indem Sie den Pfad in der folgenden Umgebungsvariablen festlegen: `AWS_CREDENTIAL_PROFILES_FILE`

Weitere Informationen über Profile finden Sie unter Arbeiten mit AWS -Anmeldeinformationen im AWS SDK for Java.

Verwenden von Anmeldeinformation eines Instance-Profils

Wenn Sie eine Anwendung auf einer Amazon-EC2-Instance ausführen, die einer IAM-Rolle zugeordnet ist, können Sie eine Verbindung mit den Anmeldeinformationen des Instance-Profils herstellen.

Verwenden Sie dazu eines der IAM-Verbindungszeichenfolgenformate in der vorhergehenden Tabelle und legen Sie die Verbindungseigenschaft dbuser auf den Amazon-Redshift-Benutzernamen fest, mit dem Sie eine Verbindung herstellen.

Weitere Informationen zu Instance-Profilen finden Sie unter Zugriffsverwaltung im IAM-Benutzerhandbuch.

Verwenden von Anmeldeinformationsanbietern

Der Treiber unterstützt auch Plug-Ins für Anmeldeinformationen von den folgenden Services:

- Active Directory Federation Service (ADFS)
- JSON Web Tokens (JWT) Service
- Microsoft Azure Active Directory (AD) Service und Browser Microsoft Azure Active Directory (AD) Service
- Okta Service
- PingFederate Dienst
- Browser-SAML für SAML-Services wie Okta, Ping oder ADFS

Wenn Sie einen dieser Services verwenden, muss die Verbindungs-URL die folgenden Eigenschaften angeben:

- Plugin_Name – Der vollqualifizierte Klassenpfad für Ihre Anmeldeinformationsanbieter-Plug-In-Klasse.
- IdP_Host: – Der Host für den Service, den Sie zur Authentifizierung bei Amazon Redshift verwenden.
- IdP-Port – Der Port, auf den der Host für den Authentifizierungsdienst wartet. Nicht erforderlich für Okta.
- User – Der Benutzername für den idp_host-Server.
- Password – Das Passwort, das mit dem idp_host-Benutzernamen verknüpft ist.
- DbUser— Der Amazon Redshift Redshift-Benutzername, mit dem Sie sich verbinden.
- SSL_Insecure – gibt an, ob das IDP-Serverzertifikat verifiziert werden soll.
- Client_ID – Die Client-ID, die dem Benutzernamen im Azure-AD-Portal zugeordnet ist. Wird nur für Azure AD verwendet.
- Client_Secret – Das Client-Secret, das der Benutzer-ID im Azure-AD-Portal zugeordnet ist. Wird nur für Azure AD verwendet.
- IdP_Tenant— Die Azure-AD-Mandanten-ID für Ihre Amazon-Redshift-Anwendung. Wird nur für Azure AD verwendet.
- App_ID – Die Okta-App-ID für Ihre Amazon-Redshift-Anwendung. Wird nur für Okta verwendet.

- App_Name – Der optionale Okta-Appname für Ihre Amazon-Redshift-Anwendung. Wird nur für Okta verwendet.
- Partner_SPID – Der Wert der Partner-SPID (Service-Provider-ID). Wird nur für PingFederate verwendet.

Wenn Sie ein Browser-Plug-In für einen dieser Dienste verwenden, kann die Verbindungs-URL auch Folgendes enthalten:

- Login_URL – Die URL für die Ressource auf der Website des Identitätsanbieters, wenn die SAML- (Security Assertion Markup Language) oder Azure-AD-Services über ein Browser-Plug-In verwendet werden. Dieser Parameter ist erforderlich, wenn Sie ein Browser-Plug-In verwenden.

- Listen_Port— Der Port, den der Treiber verwendet, um die SAML-Antwort vom Identitätsanbieter abzurufen, wenn die SAML- oder Azure-AD-Services über ein Browser-Plug-In verwendet werden.

- IdP_Response_Timeout – Die Zeitspanne in Sekunden, die der Treiber auf die SAML-Antwort vom Identitätsanbieter wartet, wenn die SAML- oder Azure AD-Services über ein Browser-Plug-In verwendet werden.

Weitere Informationen zu Eigenschaften von Verbindungszeichenfolgen finden Sie unter Konfigurationsoptionen der JDBC-Treiberversion 2.1.

Konfigurieren der Protokollierung

Sie können die Protokollierung im Treiber aktivieren, um bei der Diagnose von Problemen zu helfen.

Sie können Treiberinformationen mit den folgenden Methoden protokollieren.

- Informationen zum Speichern der protokollierten Informationen in Protokolldateien finden Sie unter Verwendung der Protokolldateien.
- Informationen zum Senden von protokollierten Informationen an das LogStream oder, das in der LogWriter angegeben ist DriverManager, finden Sie unterVerwenden von LogStream oder LogWriter.

Sie geben die Konfigurationsinformationen an den Treiber in der Verbindungs-URL an. Weitere Informationen zur Syntax der Verbindungs-URL finden Sie unter Erstellen der Verbindungs-URL.

Verwendung der Protokolldateien

Aktivieren Sie die Protokollierung nur lange genug, um ein Problem zu erfassen. Die Protokollierung reduziert die Leistung und kann eine große Menge an Datenträgerplatz verbrauchen.

Geben Sie in Ihrer Verbindungs-URL den LogLevel Schlüssel ein, um die Protokollierung zu aktivieren, und geben Sie an, wie viele Details in den Protokolldateien enthalten sein sollen. In der folgenden Tabelle sind die Protokollierungsebenen aufgeführt, die von der Amazon-Redshift-JDBC-Treiberversion 2.1 bereitgestellt werden, angefangen bei der kürzesten bis hin zur ausführlichsten.

LogLevel Wert	Beschreibung
1	Protokollieren Sie schwerwiegende Fehlerere ignisse, die beim Treiber zum Abbruch führen.
2	Protokollieren Sie Fehlerereignisse, bei denen der Treiber weiter ausgeführt werden kann.
3	Protokollieren Sie Ereignisse, die zu einem Fehler führen können, wenn keine Aktion ausgeführt wird. Diese Protokollierungsebene und die Protokollierungsebenen über dieser Ebene protokollieren auch die Abfragen des Benutzers.
4	Protokollieren Sie allgemeine Informationen, die den Fortschritt des Treibers beschreiben.
5	Protokollieren Sie detaillierte Informationen, die nützlich für das Debugging des Treibers sind.
6	Protokollieren Sie alle Treiberaktivitäten.

So richten Sie die Protokollierung ein, die Protokolldateien verwendet

1. Stellen Sie die LogLevel Eigenschaft auf die gewünschte Informationsebene ein, die in Protokolldateien aufgenommen werden soll.
2. Stellen Sie die LogPath Eigenschaft auf den vollständigen Pfad zu dem Ordner ein, in dem Sie die Protokolldateien speichern möchten.

Die folgende Verbindungs-URL aktiviert beispielsweise die Protokollierungsebene 3 und speichert die Protokolldateien im Ordner C:\temp: `jdbc:redshift://redshift.company.us-west- 1.redshift.amazonaws.com:9000/Default;DSILogLevel=3; LogPath=C:\temp`

3. Um sicherzustellen, dass die neuen Einstellungen wirksam werden, starten Sie Ihre JDBC-Anwendung neu und stellen Sie erneut eine Verbindung zum Server her.

   Der Amazon Redshift JDBC-Treiber erzeugt die folgenden Protokolldateien an dem in der Eigenschaft angegebenen Speicherort: LogPath

   - Die Datei redshift_jdbc.log, die Treiberaktivitäten protokolliert, die nicht für eine Verbindung spezifisch sind.
   - Die Datei edshift_jdbc_connection_[Nummer].log für jede Verbindung mit der Datenbank, wobei [Nummer] eine Zahl ist, die jede Protokolldatei identifiziert. Diese Datei protokolliert Treiberaktivitäten, die für die Verbindung spezifisch sind.

Wenn der LogPath Wert ungültig ist, sendet der Treiber die protokollierten Informationen an den Standardausgabestream () `System.out`

Verwenden von LogStream oder LogWriter

Aktivieren Sie die Protokollierung nur lange genug, um ein Problem zu erfassen. Die Protokollierung reduziert die Leistung und kann eine große Menge an Datenträgerplatz verbrauchen.

Legen Sie den LogLevel Schlüssel in Ihrer Verbindungs-URL fest, um die Protokollierung zu aktivieren, und geben Sie die Menge an Details an, die an die gesendet werden LogStream oder in der LogWriter angegeben sind DriverManager.

Um die Protokollierung zu aktivieren, die das LogStream oder verwendet, gehen Sie wie folgt vor LogWriter:

1. Um den Treiber so zu konfigurieren, dass er allgemeine Informationen protokolliert, die den Fortschritt des Treibers beschreiben, setzen Sie die LogLevel Eigenschaft auf 1 oder INFO.
2. Um sicherzustellen, dass die neuen Einstellungen wirksam werden, starten Sie Ihre JDBC-Anwendung neu und stellen Sie erneut eine Verbindung zum Server her.

Um die Protokollierung zu deaktivieren, die das LogStream oder verwendet LogWriter:

1. Entfernen Sie die LogLevel Eigenschaft aus der Verbindungs-URL.
2. Um sicherzustellen, dass die neuen Einstellungen wirksam werden, starten Sie Ihre JDBC-Anwendung neu und stellen Sie erneut eine Verbindung zum Server her.

Konvertieren von Datentypen

Die Amazon-Redshift-JDBC-Treiberversion 2.1 unterstützt viele gängige Datenformate, die zu Amazon-Redshift-, SQL– und Java-Datentypen konvertiert werden.

In der folgenden Tabelle sind die unterstützten Datentyp-Mappings aufgeführt.

Amazon-Redshift-Typ	SQL-Typ	Java-Typ
BIGINT	SQL_BIGINT	Long
BOOLEAN	SQL_BIT	Boolesch
CHAR	SQL_CHAR	String
DATUM	SQL_TYPE_DATE	java.sql.Date
DECIMAL	SQL_NUMERIC	BigDecimal
DOUBLE PRECISION	SQL_DOUBLE	Double
GEOMETRY	SQL_ LONGVARBINARY	byte[]
INTEGER	SQL_INTEGER	Ganzzahl
OID	SQL_BIGINT	Long
SUPER	SQL_LONGVARCHAR	String
REAL	SQL_REAL	Gleitkommazahl
SMALLINT	SQL_SMALLINT	Short
TEXT	SQL_VARCHAR	String

Amazon-Redshift-Typ	SQL-Typ	Java-Typ
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
VARCHAR	SQL_VARCHAR	String

Unterstützung für vorbereitete Anweisungen verwenden

Der Amazon-Redshift-JDBC-Treiber unterstützt vorbereitete Anweisungen. Sie können vorbereitete Anweisungen verwenden, um die Leistung parametrisierter Abfragen zu verbessern, die während derselben Verbindung mehrmals ausgeführt werden müssen.

Eine vorbereitete Anweisung ist eine SQL-Anweisung, die auf der Serverseite kompiliert, aber nicht sofort ausgeführt wird. Die kompilierte Anweisung wird auf dem Server als PreparedStatement Objekt gespeichert, bis Sie das Objekt oder die Verbindung schließen. Solange dieses Objekt vorhanden ist, können Sie die vorbereitete Anweisung so oft wie nötig mit verschiedenen Parameterwerten ausführen, ohne die Anweisung erneut kompilieren zu müssen. Durch diesen reduzierten Aufwand können die Abfragen schneller ausgeführt werden.

Weitere Informationen zu vorbereiteten Anweisungen finden Sie unter „Verwenden von vorbereiteten Anweisungen“ im Tutorial „JDBC Basics“ von Oracle.

Sie können eine Anweisung vorbereiten, die mehrere Abfragen enthält. Beispiel: Die folgende vorbereitete Anweisung enthält zwei INSERT-Abfragen:

```
PreparedStatement pstmt = conn.prepareStatement("INSERT INTO
MyTable VALUES (1, 'abc'); INSERT INTO CompanyTable VALUES
(1, 'abc');");
```

Achten Sie darauf, dass diese Abfragen nicht von den Ergebnissen anderer Abfragen abhängen, die innerhalb derselben vorbereiteten Anweisung angegeben werden. Da Abfragen während des Vorbereitungsschritts nicht ausgeführt werden, wurden die Ergebnisse noch nicht zurückgegeben und stehen für andere Abfragen in derselben vorbereiteten Anweisung nicht zur Verfügung.

Beispielsweise ist die folgende vorbereitete Anweisung, die eine Tabelle erstellt und dann Werte in diese neu erstellte Tabelle einfügt, nicht zulässig:

```
PreparedStatement pstmt = conn.prepareStatement("CREATE
TABLE MyTable(col1 int, col2 varchar); INSERT INTO myTable
VALUES (1, 'abc');");
```

Wenn Sie versuchen, diese Anweisung vorzubereiten, gibt der Server einen Fehler zurück, der besagt, dass die Zieltabelle (MyTable) noch nicht existiert. Die CREATE-Abfrage muss ausgeführt werden, bevor die INSERT-Abfrage vorbereitet werden kann.

Unterschiede zwischen den Versionen 2.1 und 1.x des JDBC-Treibers

In diesem Abschnitt werden die Unterschiede in den Informationen beschrieben, die von den Versionen 2.1 und 1.x des JDBC-Treibers zurückgegeben werden. Der JDBC-Treiber Version 1.x wird eingestellt.

In der folgenden Tabelle sind die DatabaseMetadata Informationen aufgeführt, die von den Funktionen getDatabaseProduct Name () und getDatabaseProduct Version () für jede Version des JDBC-Treibers zurückgegeben werden. JDBC-Treiberversion 2.1 erhält die Werte beim Herstellen der Verbindung. JDBC-Treiberversion 1.x erhält die Werte als Ergebnis einer Abfrage.

JDBC-Treiberversion	getDatabaseProductErgebnis für Name ()	getDatabaseProductErgebnis für Version ()
2.1	Redshift	8.0.2
1.x	PostgreSQL	08.00.0002

In der folgenden Tabelle sind die DatabaseMetadata Informationen aufgeführt, die von der getTypeInfo Funktion für jede Version des JDBC-Treibers zurückgegeben werden.

JDBC-Treiberversion	getTypeInfo Ergebnis
2.1	Konsistent mit Redshift-Datentypen
1.x	Konsistent mit PostgreSQL-Datentypen

Erstellen von Initialisierungsdateien (.ini) für JDBC-Treiberversion 2.1

Indem Sie Initialisierungsdateien (.ini) für Amazon-Redshift-JDBC-Treiberversion 2.1 verwenden, können Sie Konfigurationsparameter auf Systemebene angeben. Beispielsweise können Parameter für die verbundene IdP-Authentifizierung für jede Anwendung variieren. Die .ini-Datei stellt einen gemeinsamen Speicherort für SQL-Clients bereit, um die erforderlichen Konfigurationsparameter abzurufen.

Sie können eine Initialisierungsdatei (.ini) für JDBC-Treiberversion 2.1 erstellen, die Konfigurationsoptionen für SQL-Clients enthält. Die Datei heißt standardmäßig `rsjdbc.ini`. Der JDBC-Treiberversion 2.1 sucht die .ini-Datei an den folgenden Speicherorten, die in ihrer Rangfolge aufgeführt sind:

- `IniFile`-Parameter in der Verbindungs-URL oder im Dialogfeld der Verbindungseigenschaft des SQL-Clients. Stellen Sie sicher, dass der Parameter `IniFile` den vollständigen Pfad der .ini-Datei einschließlich des Dateinamens enthält. Weitere Informationen zum Parameter `IniFile` erhalten Sie unter IniFile. Wenn der Parameter `IniFile` den Speicherort der .ini-Datei falsch angibt, wird ein Fehler angezeigt.
- Umgebungsvariablen wie AMAZON_REDSHIFT_JDBC_INI_FILE mit dem vollständigen Pfad einschließlich des Dateinamens. Sie können `rsjdbc.ini` verwenden oder einen Dateinamen angeben. Wenn die Umgebungsvariable AMAZON_REDSHIFT_JDBC_INI_FILE den Speicherort der .ini-Datei falsch angibt, wird ein Fehler angezeigt.
- Verzeichnis, in dem sich die JAR-Datei des Treibers befindet.
- Stammverzeichnis des Benutzers.
- Temporäres Verzeichnis des Systems.

Sie können die .ini-Datei in Abschnitte organisieren, zum Beispiel [DRIVER]. Jeder Abschnitt enthält Schlüssel-Wert-Paare, die verschiedene Verbindungsparameter angeben. Sie können mit dem Parameter `IniSection` einen Abschnitt in der .ini-Datei angeben. Weitere Informationen zum Parameter `IniSection` erhalten Sie unter IniSection.

Es folgt ein Beispiel für das .ini-Dateiformat mit Abschnitten für [DRIVER], [DEV], [QA] und [PROD]. Der Abschnitt [DRIVER] kann für jede Verbindung gelten.

```
[DRIVER]
key1=val1
key2=val2
```

```
[DEV]
key1=val1
key2=val2

[QA]
key1=val1
key2=val2

[PROD]
key1=val1
key2=val2
```

Die JDBC-Treiberversion 2.1 lädt Konfigurationsparameter von den folgenden Speicherorten, die in ihrer Rangfolge aufgeführt sind:

- Standardkonfigurationsparameter im Anwendungscode.
- Eigenschaften aus dem Abschnitt [DRIVER] der .ini-Datei, falls enthalten.
- Konfigurationsparameter für benutzerdefinierte Abschnitte, wenn die Option `IniSection` in der Verbindungs-URL oder im Dialogfeld der Verbindungseigenschaft des SQL-Clients angegeben wird.
- Eigenschaften aus dem Verbindungseigenschaftenobjekt, das im Aufruf `getConnection` angegeben wird.
- Konfigurationsparameter, die in der Verbindungs-URL angegeben werden.

Konfigurationsoptionen der JDBC-Treiberversion 2.1

Im Folgenden finden Sie Beschreibungen für die Optionen, die Sie für Version 2.1 des Amazon-Redshift-JDBC-Treibers angeben können. Bei den Konfigurationsoptionen wird die Groß-/Kleinschreibung nicht beachtet.

Sie können Konfigurationseigenschaften mithilfe der Verbindungs-URL festlegen. Weitere Informationen finden Sie unter Erstellen der Verbindungs-URL.

Themen

- AccessKeyID
- AllowDB UserOverride
- App_ID

- App_Name
- ApplicationName
- AuthProfile
- AutoCreate
- Client_ID
- Client_Secret
- ClusterID
- Komprimierung
- ConnectTimeout
- connectionTimezone
- databaseMetadataCurrentDbOnly
- DbUser
- DbGroups
- DBNAME
- defaultRowFetchGröße
- DisableIsValidQuery
- enableFetchRingPuffer
- enableMultiSqlSupport
- fetchRingBufferGröße
- ForceLowercase
- groupFederation
- HOST
- ICH BIN DisableCache
- IAMDuration
- Identity_Namespace
- IdP_Host
- IdP_Port
- IdP_Tenant
- IdP_Response_Timeout

- IniFile
- IniSection
- isServerless
- Login_URL
- loginTimeout
- loginToRp
- LogLevel
- LogPath
- OverrideSchemaPatternType
- Partner_SPID
- Passwort
- Plugin_Name
- PORT
- Preferred_Role
- Profil
- PWD
- QueryGroup
- readOnly
- Region
- reWriteBatchedFügt ein
- reWriteBatchedInsertsSize
- roleArn
- roleSessionName
- scope
- SecretAccessKey
- SessionToken
- serverlessAcctId
- serverlessWorkGroup
- socketFactory
- socketTimeout

- SSL
- SSL_Insecure
- SSLCert
- SSLFactory
- SSLKey
- SSLMode
- SSLPassword
- SSL RootCert
- StsEndpointUrl
- tcpKeepAlive
- Benutzerkennung (UID)
- Benutzer
- webIdentityToken

AccessKeyID

- Standardwert – Kein
- Datentyp – Zeichenfolge

Sie können diesen Parameter angeben, um den IAM-Zugriffsschlüssel für den Benutzer oder die Rolle einzugeben. Sie finden den Schlüssel normalerweise in einer vorhandenen Zeichenfolge oder einem vorhandenen Benutzerprofil. Wenn Sie diesen Parameter angeben, müssen Sie auch den Parameter `SecretAccessKey` angeben: Wenn die JDBC-URL übergeben wird, muss die AccessKey ID URL-codiert sein.

Dieser Parameter ist optional.

AllowDB UserOverride

- Standardwert – 0
- Datentyp – Zeichenfolge

Diese Option gibt an, ob der Treiber den Wert von `DbUser` aus der SAML-Assertion verwendet oder den Wert, der in der Verbindungseigenschaft `DbUser` in der Verbindungs-URL angegeben ist.

Dieser Parameter ist optional.

1

Der Treiber verwendet den Wert `DbUser` aus der SAML-Assertion.

Wenn die SAML-Assertion keinen Wert für `DBUser` angibt, verwendet der Treiber den Wert, der in der `DBUser`-Verbindungseigenschaft angegeben ist. Wenn die Verbindungseigenschaft auch keinen Wert angibt, verwendet der Treiber den Wert, der im Verbindungsprofil angegeben ist.

0

Der Treiber verwendet den `DBUser`-Wert, der in der`DBUser`-Verbindungseigenschaft angegeben ist.

Wenn die `DBUser`-Verbindungseigenschaft keinen Wert angibt, verwendet der Treiber den Wert, der im Verbindungsprofil angegeben ist. Wenn das Verbindungsprofil auch keinen Wert angibt, verwendet der Treiber den Wert aus der SAML-Assertion.

App_ID

- Standardwert – None
- Datentyp – Zeichenfolge

Die von Okta bereitgestellte eindeutige ID, die mit Ihrer Amazon-Redshift-Anwendung verknüpft ist.

Dieser Parameter ist erforderlich, wenn die Authentifizierung über den Okta-Service erfolgt.

App_Name

- Standardwert – None
- Datentyp – Zeichenfolge

Der Name der Okta-Anwendung, mit der Sie die Verbindung zu Amazon Redshift authentifizieren.

Dieser Parameter ist optional.

ApplicationName

- Standardwert – Null

- Datentyp – Zeichenfolge

Der Name der Anwendung, die zu Prüfungszwecken an Amazon Redshift übergeben wird.

Dieser Parameter ist optional.

AuthProfile

- Standardwert – None
- Datentyp – Zeichenfolge

Der Name des Authentifizierungsprofils, das für die Verbindung mit Amazon Redshift verwendet werden soll.

Dieser Parameter ist optional.

AutoCreate

- Standardwert – false
- Datentyp – boolesch

Diese Option gibt an, ob der Treiber dazu führt, dass ein neuer Benutzer erstellt wird, wenn der angegebene Benutzer nicht existiert.

Dieser Parameter ist optional.

true

Wenn der Benutzer, der durch `DBUser` oder eine eindeutige ID (UID) angegeben wird, nicht vorhanden ist, wird ein neuer Benutzer mit diesem Namen erstellt.

false

Der Treiber führt nicht dazu, dass neue Benutzer erstellt werden. Wenn der angegebene Benutzer nicht vorhanden ist, schlägt die Authentifizierung fehl.

Client_ID

- Standardwert – None
- Datentyp – Zeichenfolge

Die Client-ID, die beim Authentifizieren der Verbindung mit dem Azure-AD-Dienst verwendet werden soll.

Dieser Parameter ist erforderlich, wenn die Authentifizierung über den Azure-AD-Service erfolgt.

Client_Secret

- Standardwert – None
- Datentyp – Zeichenfolge

Das Client-Secret, das beim Authentifizieren der Verbindung mit dem Azure-AD-Dienst verwendet werden soll.

Dieser Parameter ist erforderlich, wenn die Authentifizierung über den Azure-AD-Service erfolgt.

ClusterID

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Name des Amazon-Redshift-Clusters, mit dem Sie eine Verbindung herstellen möchten. Der Treiber versucht, diesen Parameter vom angegebenen Host zu erkennen. Wenn Sie einen Network Load Balancer (NLB) verwenden und über IAM eine Verbindung herstellen, wird der Treiber ihn nicht erkennen, daher können Sie ihn unter Verwendung dieser Verbindungsoption einstellen.

Dieser Parameter ist optional.

Komprimierung

- Standardwert — aus
- Datentyp – Zeichenfolge

Die Komprimierungsmethode, die für die Wire-Protokollkommunikation zwischen dem Amazon-Redshift-Server und dem Client oder Treiber verwendet wird.

Dieser Parameter ist optional.

Sie können die folgenden Werte angeben:

- lz4

Legt für die Komprimierungsmethode, die für die Wire-Protokollkommunikation mit Amazon Redshift verwendet wird, lz4 fest.

- aus

  Für die Wire-Protokollkommunikation mit Amazon Redshift wird keine Komprimierungsmethode verwendet.

ConnectTimeout

- Standardwert – 10
- Datentyp – Ganzzahl

Der Timeout-Wert, der für Socket-Connect-Vorgänge verwendet werden soll. Wenn die zum Herstellen einer Amazon-Redshift-Verbindung erforderliche Zeit diesen Wert überschreitet, gilt die Verbindung als nicht verfügbar. Das Timeout wird in Sekunden angegeben. Ein Wert von 0 bedeutet, dass kein Timeout angegeben wird.

Dieser Parameter ist optional.

connectionTimezone

- Standardwert – LOKAL
- Datentyp – Zeichenfolge

Die Zeitzone auf Sitzungsebene.

Dieser Parameter ist optional.

Sie können die folgenden Werte angeben:

LOCAL

Konfiguriert für die Zeitzone auf Sitzungsebene die Zeitzone LOCAL JVM.

SERVER

Konfiguriert für die Zeitzone auf Sitzungsebene die Zeitzone, die für den Benutzer auf dem Amazon-Redshift-Server festgelegt wurde. Mit dem folgenden Befehl können Sie Zeitzonen auf Sitzungsebene für Benutzer konfigurieren:

```
ALTER USER
[...]
SET TIMEZONE TO [...];
```

databaseMetadataCurrentDbOnly

- Standardwert – true
- Datentyp – boolesch

Diese Option gibt an, ob die Metadaten-API Daten aus allen zugänglichen Datenbanken oder nur aus der verbundenen Datenbank abruft.

Dieser Parameter ist optional.

Sie können die folgenden Werte angeben:

true

Die Anwendung ruft Metadaten aus einer einzelnen Datenbank ab.

false

Die Anwendung ruft Metadaten aus allen zugänglichen Datenbanken ab.

DbUser

- Standardwert – None
- Datentyp – Zeichenfolge

Die Benutzer-ID, die mit Ihrem Amazon-Redshift-Konto verwendet werden soll. Sie können eine ID verwenden, die derzeit nicht existiert, wenn Sie die AutoCreate Eigenschaft aktiviert haben.

Dieser Parameter ist optional.

DbGroups

- Standardwert – PUBLIC
- Datentyp – Zeichenfolge

Eine durch Komma getrennte Liste vorhandener Datenbankgruppennamen, die `DBUser` für die aktuelle Sitzung verbindet.

Dieser Parameter ist optional.

DBNAME

- Standardwert – Null
- Datentyp – Zeichenfolge

Der Name der Datenbank, mit der eine Verbindung hergestellt werden soll. Mit dieser Option können Sie den Datenbanknamen in der JDBC-Verbindungs-URL angeben.

Dieser Parameter muss angegeben werden. Sie müssen den Datenbanknamen entweder in der Verbindungs-URL oder in den Verbindungseigenschaften der Clientanwendung angeben.

defaultRowFetchGröße

- Standardwert – 0
- Datentyp – Ganzzahl

Diese Option gibt einen Standardwert für an getFetchSize.

Dieser Parameter ist optional.

Sie können die folgenden Werte angeben:

0

Ruft alle Zeilen in einer einzigen Operation ab.

Positive Ganzzahl

Anzahl der Zeilen, die für jede Abruf-Iteration von aus der Datenbank abgerufen werden sollen. ResultSet

DisableIsValidQuery

- Standardwert – False
- Datentyp – boolesch

Diese Option gibt an, ob der Treiber eine neue Datenbankabfrage sendet, wenn die Methode Connection.isValid() verwendet wird, um zu bestimmen, ob die Datenbankverbindung aktiv ist.

Dieser Parameter ist optional.

true

Der Treiber sendet keine Abfrage, wenn mit .Connection.isValid() bestimmt wird, ob die Datenbankverbindung aktiv ist. Dies kann dazu führen, dass der Treiber die Datenbankverbindung fälschlicherweise als aktiv identifiziert, wenn der Datenbankserver unerwartet heruntergefahren wurde.

false

Der Treiber sendet eine Abfrage, wenn mit .Connection.isValid() bestimmt wird, ob die Datenbankverbindung aktiv ist.

enableFetchRingPuffer

- Standardwert – true
- Datentyp – boolesch

Diese Option gibt an, dass der Treiber Zeilen mit einem Ringpuffer in einem separaten Thread abruft. Der Parameter fetchRingBuffer Size gibt die Größe des Ringpuffers an.

Wenn eine Transaktion eine Anweisung erkennt, die mehrere durch Semikolons getrennte SQL-Befehle enthält, wird der Fetch-Ringpuffer für diese Transaktion auf False gesetzt. enableFetchRingDer Wert des Puffers ändert sich nicht.

Dieser Parameter ist optional.

enableMultiSqlSupport

- Standardwert – true
- Datentyp – boolesch

Diese Option gibt an, ob mehrere SQL-Befehle in einer Anweisung durch Semikolons getrennt verarbeitet werden sollen.

Dieser Parameter ist optional.

Sie können die folgenden Werte angeben:

true

Der Treiber verarbeitet mehrere SQL-Befehle, getrennt durch Semikolon, in einem Anweisungsobjekt.

false

Der Treiber gibt einen Fehler für mehrere SQL-Befehle in einer einzelnen Anweisung zurück.

fetchRingBufferGröße

- Standardwert – 1G
- Datentyp – Zeichenfolge

Diese Option gibt die Größe des Ringpuffers an, der beim Abrufen der Ergebnismenge verwendet wird. Sie können eine Größe in Byte angeben, z. B. 1K für 1 KB, 5000 für 5 000 Byte, 1M für 1 MB, 1G für 1 GB usw. Sie können auch einen Prozentsatz des Heap-Arbeitsspeichers angeben. Der Treiber stoppt das Abrufen von Zeilen, wenn das Limit erreicht ist. Der Abruf wird fortgesetzt, wenn die Anwendung Zeilen liest und Speicherplatz im Ringpuffer freigibt.

Dieser Parameter ist optional.

ForceLowercase

- Standardwert – false
- Datentyp – boolesch

Diese Option gibt an, ob der Treiber bei Verwendung der Single Sign-On-Authentifizierung alle Datenbankgruppen (DbGroups), die vom Identitätsanbieter an Amazon Redshift gesendet werden, in Kleinbuchstaben schreibt.

Dieser Parameter ist optional.

true

Der Treiber schreibt alle Datenbankgruppen in Kleinbuchstaben, die vom Identitätsanbieter gesendet werden.

false

Der Treiber ändert Datenbankgruppen nicht.

groupFederation

- Standardwert – false
- Datentyp – boolesch

Diese Option gibt an, ob Amazon-Redshift-IDP-Gruppen verwendet werden sollen. Dies wird von der V2-API unterstützt. GetClusterCredentials

Dieser Parameter ist optional.

true

Verwenden Sie Amazon Redshift-Identity-Provider (IDP)-Gruppen.

false

Verwenden Sie STS-API und GetClusterCredentials für den Benutzerverbund und geben Sie dies explizit DbGroups für die Verbindung an.

HOST

- Standardwert – Null
- Datentyp – Zeichenfolge

Der Hostname des Amazon-Redshift-Servers, mit dem eine Verbindung hergestellt werden soll. Mit dieser Option können Sie den Hostnamen in der JDBC-Verbindungs-URL angeben.

Dieser Parameter muss angegeben werden. Sie müssen den Hostnamen entweder in der Verbindungs-URL oder in den Verbindungseigenschaften der Clientanwendung angeben.

ICH BIN DisableCache

- Standardwert – false
- Datentyp – boolesch

Diese Option gibt an, ob die IAM-Anmeldeinformationen zwischengespeichert werden.

Dieser Parameter ist optional.

true

Die IAM-Anmeldeinformationen werden nicht zwischengespeichert.

false

Die IAM-Anmeldeinformationen werden zwischengespeichert. Dies verbessert die Leistung, wenn beispielsweise Anfragen an das API-Gateway gedrosselt werden.

IAMDuration

- Standardwert – 900
- Datentyp – Ganzzahl

Die Zeitdauer in Sekunden, bis die temporären IAM-Anmeldeinformationen ablaufen.

- Mindestwert – 900
- Maximaler Wert – 3,600

Dieser Parameter ist optional.

Identity_Namespace

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Identitätsnamespace, der bei der Authentifizierung mit dem verwendet werden soll. IdpTokenAuthPlugin Er hilft Redshift, zu bestimmen, welche IAM-Identity-Center-Instance verwendet werden soll.

Wenn nur eine IAM-Identity-Center-Instance vorhanden ist oder der standardmäßige Identitäts-Namespace festgelegt ist, ist dieser Parameter optional, andernfalls ist er erforderlich.

IdP_Host

- Standardwert – None

- Datentyp – Zeichenfolge

Der IdP-Host (Identitätsanbieter), den Sie zur Authentifizierung bei Amazon Redshift verwenden. Kann entweder in der Verbindungszeichenfolge oder in einem Profil angegeben werden.

Dieser Parameter ist optional.

IdP_Port

- Standardwert – None
- Datentyp – Zeichenfolge

Der vom IdP (Identitätsanbieter) verwendete Port. Sie können den Port entweder in der Verbindungszeichenfolge oder in einem Profil angeben. Der Standard-Port ist 5439. Erlauben Sie den Zugriff auf den ausgewählten Port, je nachdem, welchen Port Sie beim Erstellen, Ändern oder Migrieren des Clusters ausgewählt haben.

Dieser Parameter ist optional.

IdP_Tenant

- Standardwert – None
- Datentyp – Zeichenfolge

Die Azure-AD-Mandanten-ID für Ihre Amazon-Redshift-Anwendung.

Dieser Parameter ist erforderlich, wenn die Authentifizierung über den Azure-AD-Service erfolgt.

IdP_Response_Timeout

- Standardwert – 120
- Datentyp – Ganzzahl

Die Zeitspanne in Sekunden, die der Treiber auf die SAML-Antwort vom Identitätsanbieter wartet, wenn die SAML- oder Azure AD-Services über ein Browser-Plug-In verwendet werden.

Dieser Parameter ist optional.

IniFile

- Standardwert – None
- Datentyp – Zeichenfolge

Der vollständige Dateipfad der .ini-Datei einschließlich des Dateinamens. Zum Beispiel:

```
IniFile="C:\tools\rsjdbc.ini"
```

Informationen zur .ini-Datei finden Sie unter Erstellen von Initialisierungsdateien (.ini) für JDBC-Treiberversion 2.1.

Dieser Parameter ist optional.

IniSection

- Standardwert – None
- Datentyp – Zeichenfolge

Der Name eines Abschnitts in der .ini-Datei, der die Konfigurationsoptionen enthält. Informationen zur .ini-Datei finden Sie unter Erstellen von Initialisierungsdateien (.ini) für JDBC-Treiberversion 2.1.

Im folgenden Beispiel wird der Abschnitt [Prod] der .ini-Datei angegeben:

```
IniSection="Prod"
```

Dieser Parameter ist optional.

isServerless

- Standardwert – false
- Datentyp – boolesch

Diese Option gibt an, ob der Amazon-Redshift-Endpunkthost eine Serverless-Instance ist. Der Treiber versucht, diesen Parameter vom angegebenen Host zu erkennen. Wenn Sie einen Network Load Balancer (NLB) verwenden, wird der Treiber ihn nicht erkennen, also können Sie ihn hier einstellen.

Dieser Parameter ist optional.

true

Der Amazon-Redshift-Endpunkthost ist eine Serverless-Instance.

false

Der Amazon-Redshift-Endpunkthost ist ein bereitgestellter Cluster.

Login_URL

- Standardwert – None
- Datentyp – Zeichenfolge

Die URL für die Ressource auf der Website des Identitätsanbieters, wenn die SAML- oder Azure-AD-Services über ein Browser-Plug-In verwendet werden.

Dieser Parameter ist erforderlich, wenn die Authentifizierung über die SAML- oder Azure-AD-Services über ein Browser-Plug-In erfolgt.

loginTimeout

- Standardwert – 0
- Datentyp – Ganzzahl

Die Anzahl der Sekunden, die gewartet werden soll, bevor eine Zeitüberschreitung für einen Verbindungs- und Authentifizierungsversuch mit dem Server eintritt. Wenn es länger dauert, eine Verbindung mit dem Server herzustellen, als durch diesen Schwellenwert angegeben, wird die Verbindung abgebrochen.

Wenn diese Eigenschaft auf 0 festgelegt ist, treten keine Zeitüberschreitungen für Verbindungen ein.

Dieser Parameter ist optional.

loginToRp

- Standardwert – `urn:amazon:webservices`
- Datentyp – Zeichenfolge

Die Vertrauensstellung die Sie für den AD-FS-Authentifizierungstyp verwenden möchten.

Dieser Parameter ist optional.

LogLevel

- Standardwert – 0
- Datentyp – Ganzzahl

Verwenden Sie diese Eigenschaft, um die Protokollierung im Treiber zu aktivieren oder zu deaktivieren und den Grad an Details anzugeben, die in den Protokolldateien enthalten sein sollen.

Aktivieren Sie die Protokollierung nur lange genug, um ein Problem zu erfassen. Die Protokollierung reduziert die Leistung und kann eine große Menge an Datenträgerplatz verbrauchen.

Dieser Parameter ist optional.

Legen Sie den Parameter auf einen der folgenden Werte fest:

0

Deaktiviert die gesamte Protokollierung.

1

Aktiviert die Protokollierung auf der Ebene FATAL, die sehr schwerwiegende Fehlerereignisse protokolliert, die zu einem Absturz des Treibers führen.

2

Aktiviert die Protokollierung auf der Ebene ERROR, die Fehlerereignisse protokolliert, bei denen der Treiber weiter ausgeführt werden kann.

3

Aktivieren Sie die Protokollierung auf der Ebene WARNING, die Ereignisse protokolliert, die möglicherweise zu einem Fehler führen, wenn nicht unternommen wird.

4

Aktivieren Sie die Protokollierung auf der Ebene INFO, die allgemeine Informationen protokolliert, die den Fortschritt des Treibers beschreiben.

5

Aktivieren Sie die Protokollierung auf der Ebene DEBUG, die detaillierte Informationen protokolliert, die für das Debuggen des Treibers nützlich sind.

6

Aktivieren Sie die Protokollierung auf der Ebene TRACE, die alle Treiberaktivitäten protokolliert.

Wenn die Protokollierung aktiviert ist, erstellt der Treiber die folgenden Protokolldateien an dem Speicherort, der in der Eigenschaft `LogPath` angegeben ist.

- **`redshift_jdbc.log`** – Diese Datei protokolliert Treiberaktivitäten, die nicht für die Verbindung spezifisch sind.
- **`redshift_jdbc_connection_[Number].log`** – Datei für jede Verbindung mit der Datenbank, wobei `[Number]` eine Nummer zur Unterscheidung der Protokolldateien ist. Diese Datei protokolliert Treiberaktivitäten, die für die Verbindung spezifisch sind.

Wenn der LogPath Wert ungültig ist, sendet der Treiber die protokollierten Informationen an den Standardausgabestream,. `System.out`

LogPath

- Standardwert – Das aktuelle Arbeitsverzeichnis.
- Datentyp – Zeichenfolge

Der vollständige Pfad zu dem Ordner, in dem der Treiber Protokolldateien speichert, wenn die LogLevel DSI-Eigenschaft aktiviert ist.

Um sicherzustellen, dass die Verbindungs-URL mit allen JDBC-Anwendungen kompatibel ist, empfehlen wir, die umgekehrten Schrägstriche (\) in Ihrem Dateipfad mit einem zusätzlichen umgekehrten Schrägstrich zu escapen.

Dieser Parameter ist optional.

OverrideSchemaPatternType

- Standardwert – Null
- Datentyp – Ganzzahl

Diese Option gibt an, ob der Abfragetyp, der in getTables-Aufrufen verwendet wird, überschrieben werden soll.

0

Keine universelle Schemaabfrage

1

Abfrage von lokalen Schemata

2

Abfrage von externen Schemata

Dieser Parameter ist optional.

Partner_SPID

- Standardwert – None
- Datentyp – Zeichenfolge

Der Partner-SPID-Wert (Service Provider ID), der bei der Authentifizierung der Verbindung über den Dienst verwendet werden soll. PingFederate

Dieser Parameter ist optional.

Passwort

- Standardwert – Kein
- Datentyp – Zeichenfolge

Wenn Sie eine Verbindung mit IAM-Authentifizierung über einen IDP herstellen, ist dies das Kennwort für den IDP_Host-Server. Bei Verwendung der Standardauthentifizierung kann dies für das Amazon-Redshift-Datenbankkennwort anstelle von PWD verwendet werden.

Dieser Parameter ist optional.

Plugin_Name

- Standardwert – None
- Datentyp – Zeichenfolge

Der vollqualifizierte Klassenname zur Implementierung eines spezifischen Anmeldeinformationsanbieters.

Dieser Parameter ist optional.

Folgende Anbieteroptionen werden unterstützt:

- **`AdfsCredentialsProvider`**— Active Directory-Verbunddienst.
- **`AzureCredentialsProvider`**— Microsoft Azure Active Directory (AD) -Dienst.
- **`BasicJwtCredentialsProvider`**— Dienst für JSON-Web-Tokens (JWT).
- **`BasicSamlCredentialsProvider`** – SAML-Anmeldeinformationen (Security Assertion Markup Language), die Sie mit vielen SAML-Dienstanbietern verwenden können.
- **`BrowserAzureCredentialsProvider`**— Browser Microsoft Azure Active Directory (AD) -Dienst.
- **`BrowserAzureOAuth2CredentialsProvider`**— Browser Microsoft Azure Active Directory (AD) Service für native Authentifizierung.
- **`BrowserSamlCredentialsProvider`**— Browser-SAML für SAML-Dienste wie Okta, Ping oder ADFS.
- **`IdpTokenAuthPlugin`**— Ein Autorisierungs-Plugin, das ein Identity Center (iDC) -Token oder OpenID Connect (OIDC) JSON-basierte Identitätstoken (JWT) von jedem mit dem iDC verknüpften Web-Identitätsanbieter akzeptiert.
- **`OktaCredentialsProvider`**— Okta-Dienst.
- **`PingCredentialsProvider`**— PingFederate Bedienung.

PORT

- Standardwert – Null
- Datentyp – Ganzzahl

Der Port des Amazon-Redshift-Servers, zu dem eine Verbindung hergestellt werden soll. Mit dieser Option können Sie den Port in der JDBC-Verbindungs-URL angeben.

Dieser Parameter ist optional.

Preferred_Role

- Standardwert – None

- Datentyp – Zeichenfolge

IAM-Rolle, die Sie während der Verbindung mit Amazon Redshift übernehmen möchten.

Dieser Parameter ist optional.

Profil

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Name des Profils für die IAM-Authentifizierung. Dieses Profil enthält alle zusätzlichen Verbindungseigenschaften, die nicht in der Verbindungszeichenfolge angegeben sind.

Dieser Parameter ist optional.

PWD

- Standardwert – Kein
- Datentyp – Zeichenfolge

Das Kennwort, das dem Amazon-Redshift-Benutzernamen entspricht, den Sie mithilfe der Eigenschaften-UID angegeben haben.

Dieser Parameter ist optional.

QueryGroup

- Standardwert – Null
- Datentyp – Zeichenfolge

Diese Option weist eine Abfrage zur Laufzeit einer Warteschlange zu, indem Sie die Abfrage der entsprechenden Abfragegruppe zuweisen. Die Abfragegruppe wird für die Sitzung festgelegt. Alle Abfragen, die für die Verbindung ausgeführt werden, gehören zu dieser Abfragegruppe.

Dieser Parameter ist optional.

readOnly

- Standardwert – false

- Datentyp – boolesch

Diese Eigenschaft gibt an, ob sich der Treiber im schreibgeschützten Modus befindet.

Dieser Parameter ist optional.

true

Die Verbindung befindet sich im schreibgeschützten Modus und kann nicht in den Datenspeicher schreiben.

false

Die Verbindung befindet sich nicht im schreibgeschützten Modus und kann in den Datenspeicher schreiben.

Region

- Standardwert – Null
- Datentyp – Zeichenfolge

Diese Option gibt die AWS Region an, in der sich der Cluster befindet. Wenn Sie die StsEndPoint Option angeben, wird die Option Region ignoriert. Die Redshift-API-Operation `GetClusterCredentials` verwendet auch die Option „Region“.

Dieser Parameter ist optional.

reWriteBatchedFügt ein

- Standardwert – false
- Datentyp – boolesch

Diese Option ermöglicht die Optimierung, um kompatible INSERT-Anweisungen neu zu schreiben und zu kombinieren, die als Batch ausgeführt werden.

Dieser Parameter ist optional.

reWriteBatchedInsertsSize

- Standardwert – 128

- Datentyp – Ganzzahl

Diese Option ermöglicht die Optimierung, um kompatible INSERT-Anweisungen neu zu schreiben und zu kombinieren, die als Batch ausgeführt werden. Dieser Wert muss exponentiell um die Potenz von 2 erhöht werden.

Dieser Parameter ist optional.

roleArn

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Amazon-Ressourcenname (ARN) der Rolle. Stellen Sie sicher, dass Sie diesen Parameter angeben, wenn Sie ihn BasicJwtCredentialsProvider für die Option Plugin_Name angeben. Sie geben den ARN im folgenden Format an:

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

Dieser Parameter ist erforderlich, wenn Sie ihn BasicJwtCredentialsProvider für die Option Plugin_Name angeben.

roleSessionName

- Standardwert – jwt_redshift_session
- Datentyp – Zeichenfolge

Ein Bezeichner für die Sitzung der angenommenen Rolle. Normalerweise übergeben Sie den Namen oder den Bezeichner, der dem Benutzer Ihrer Anwendung zugeordnet ist. Die temporären Sicherheitsanmeldeinformationen, die Ihre Anwendung verwendet, sind diesem Benutzer zugeordnet. Sie können diesen Parameter angeben, wenn Sie ihn BasicJwtCredentialsProvider für die Option Plugin_Name angeben.

Dieser Parameter ist optional.

scope

- Standardwert – Kein
- Datentyp – Zeichenfolge

Eine durch Leerzeichen getrennte Liste von Bereichen, denen der Benutzer zustimmen kann. Sie geben diesen Parameter an, damit Ihre Microsoft-Azure-Anwendung die Zustimmung zu APIs einholen kann, die Sie aufrufen möchten. Sie können diesen Parameter angeben, wenn Sie BrowserAzure OAuth2 CredentialsProvider für die Option Plugin_Name angeben.

Dieser Parameter ist für das OAuth2-Plug-In erforderlich. BrowserAzure CredentialsProvider

SecretAccessKey

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der IAM-Zugriffsschlüssel für den Benutzer oder die Rolle. Wenn dies angegeben ist, muss auch die AccessKey ID angegeben werden. Wenn die JDBC-URL übergeben wird, SecretAccessKey muss sie URL-kodiert sein.

Dieser Parameter ist optional.

SessionToken

- Standardwert – None
- Datentyp – Zeichenfolge

Das temporäre IAM-Sitzungstoken, das der IAM-Rolle zugeordnet ist, die Sie zur Authentifizierung verwenden. Das temporäre IAM-Sitzungstoken muss URL-codiert sein, wenn es in der JDBC-URL übergeben wird.

Dieser Parameter ist optional.

serverlessAcctId

- Standardwert – Null
- Datentyp – Zeichenfolge

Die Konto-ID von Amazon Redshift Serverless. Der Treiber versucht, diesen Parameter vom angegebenen Host zu erkennen. Wenn Sie einen Network Load Balancer (NLB) verwenden, wird der Treiber ihn nicht erkennen, also können Sie ihn hier einstellen.

Dieser Parameter ist optional.

serverlessWorkGroup

- Standardwert – Null
- Datentyp – Zeichenfolge

Der Name der Amazon-Redshift-Serverless-Arbeitsgruppe. Der Treiber versucht, diesen Parameter vom angegebenen Host zu erkennen. Wenn Sie einen Network Load Balancer (NLB) verwenden, wird der Treiber ihn nicht erkennen, also können Sie ihn hier einstellen.

Dieser Parameter ist optional.

socketFactory

- Standardwert – Null
- Datentyp – Zeichenfolge

Diese Option gibt eine Socket-Factory für die Socket-Erstellung an.

Dieser Parameter ist optional.

socketTimeout

- Standardwert – 0
- Datentyp – Ganzzahl

Die Anzahl der Sekunden, die während Sockelleseoperationen gewartet werden soll, bevor eine Zeitüberschreitung eintritt. Wenn eine Operation länger dauert, als durch diesen Schwellenwert angegeben, wird die Verbindung geschlossen. Wenn diese Eigenschaft auf 0 festgelegt ist, treten keine Zeitüberschreitungen für die Verbindung ein.

Dieser Parameter ist optional.

SSL

- Standardwert – TRUE
- Datentyp – Zeichenfolge

Verwenden Sie diese Eigenschaft, um SSL für die Verbindung zu aktivieren oder zu deaktivieren.

Dieser Parameter ist optional.

Sie können die folgenden Werte angeben:

TRUE

Der Treiber stellt über SSL eine Verbindung mit dem Server her.

FALSE

Der Treiber stellt ohne SSL eine Verbindung mit dem Server her. Diese Option wird bei der IAM-Authentifizierung nicht unterstützt.

Alternativ können Sie die Eigenschaft konfigurieren. AuthMech

SSL_Insecure

- Standardwert – true
- Datentyp – Zeichenfolge

Diese Eigenschaft gibt an, ob das Serverzertifikat für IDP-Hosts überprüft werden soll.

Dieser Parameter ist optional.

Sie können die folgenden Werte angeben:

true

Der Treiber überprüft die Authentizität des IDP-Serverzertifikats nicht.

false

Der Treiber überprüft die Authentizität des IDP-Serverzertifikats.

SSLCert

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der vollständige Pfad einer .pem- oder .crt-Datei, die zusätzliche vertrauenswürdige CA-Zertifikate für die Verifizierung der Amazon-Redshift-Server-Instance bei Verwendung von SSL enthält.

Dieser Parameter ist erforderlich, wenn SSLKey festgelegt ist.

SSLFactory

- Standardwert – Kein
- Datentyp – Zeichenfolge

Die SSL-Factory, die verwendet werden soll, wenn eine Verbindung mit dem Server über TLS/SSL ohne Verwendung eines Serverzertifikats hergestellt wird.

SSLKey

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der vollständige Pfad der .der-Datei, die die PKCS8-Schlüsseldatei zum Überprüfen der in SSLCert angegebenen Zertifikate enthält.

Dieser Parameter ist erforderlich, wenn SSLCert festgelegt ist.

SSLMode

- Standardwert – verify-ca
- Datentyp – Zeichenfolge

Verwenden Sie diese Eigenschaft, um anzugeben, wie der Treiber Zertifikate validiert, wenn TLS/SSL aktiviert ist.

Dieser Parameter ist optional.

Sie können die folgenden Werte angeben:

verify-ca

Der Treiber stellt sicher, dass das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) stammt.

verify-full

Der Treiber überprüft, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle stammt und dass der Hostname im Zertifikat mit dem Hostnamen übereinstimmt, der in der Verbindungs-URL angegeben ist.

SSLPassword

- Standardwert – 0
- Datentyp – Zeichenfolge

Das Passwort für die verschlüsselte Schlüsseldatei, die in SSLKey angegeben wurde.

Dieser Parameter ist erforderlich, wenn SSLKey festgelegt ist und die Schlüsseldatei verschlüsselt ist.

SSL RootCert

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der vollständige Pfad einer .pem- oder .crt-Datei, die das Stamm-CA-Zertifikat für die Verifizierung der Amazon-Redshift-Serverinstanz bei Verwendung von SSL enthält.

StsEndpointUrl

- Standardwert – Null
- Datentyp – Zeichenfolge

Sie können einen Endpunkt AWS Security Token Service (AWS STS) angeben. Wenn Sie diese Option angeben, wird die Option „Region“ ignoriert. Sie können nur ein sicheres Protokoll (HTTPS) für diesen Endpunkt angeben.

tcpKeepAlive

- Standardwert – TRUE
- Datentyp – Zeichenfolge

Verwenden Sie diese Eigenschaft, um TCP-Keepalives zu aktivieren oder zu deaktivieren.

Dieser Parameter ist optional.

Sie können die folgenden Werte angeben:

TRUE

Der Treiber verwendet TCP-Keepalives, um ein Timeout für Verbindungen zu verhindern.

FALSE

Der Treiber verwendet keine TCP-Keepalives.

Benutzerkennung (UID)

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Datenbankbenutzername, der für den Datenbankzugriff verwendet wird.

Dieser Parameter muss angegeben werden.

Benutzer

- Standardwert – Kein
- Datentyp – Zeichenfolge

Wenn Sie eine Verbindung mit IAM-Authentifizierung über einen IDP herstellen, ist dies der Benutzername für den idp_host-Server. Bei Verwendung der Standardauthentifizierung kann dies für den Amazon-Redshift-Datenbankbenutzernamen verwendet werden.

Dieser Parameter ist optional.

webIdentityToken

- Standardwert – None
- Datentyp – Zeichenfolge

Das OAuth-2.1-Zugriffstoken oder OpenID-Connect-ID-Token, das vom Identitätsanbieter bereitgestellt wird. Ihre Anwendung muss dieses Token abrufen, indem Sie den Benutzer Ihrer

Anwendung bei einem Web-Identitätsanbieter authentifizieren. Stellen Sie sicher, dass Sie diesen Parameter angeben, wenn Sie ihn BasicJwtCredentialsProvider für die Option Plugin_Name angeben.

Dieser Parameter ist erforderlich, wenn Sie ihn BasicJwtCredentialsProvider für die Option Plugin_Name angeben.

Bisherige Versionen der JDBC-Treiberversion 2.1

Sie sollten eine frühere Version der Amazon-Redshift-JDBC-Treiberversion 2.1 nur dann herunterladen, wenn Ihr Tool eine spezifische Treiberversion benötigt.

Dies sind die vorherigen JDBC-4.2-kompatiblen JDBC-Treiber der Version 2.1:

- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.25/redshift-jdbc42-2.1.0.25.zip
  https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/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

Konfigurieren des Amazon-Redshift-Python-Konnektors

Mithilfe des Amazon Redshift Redshift-Konnektors für Python können Sie die Arbeit mit dem AWS SDK for Python (Boto3) sowie mit Pandas und Numerical Python () integrieren. NumPy Weitere Informationen zu Pandas finden Sie im Pandas-Repository. GitHub Weitere Informationen zu finden Sie im NumPy Repository. NumPy GitHub

Der Amazon-Redshift-Python-Konnektor stellt eine Open-Source-Lösung bereit. Sie können den Quellcode durchsuchen, Verbesserungen anfordern, Probleme melden und Beiträge bereitstellen.

Um den Amazon-Redshift-Python-Konnektor zu verwenden, stellen Sie sicher, dass Sie über Python-Version 3.6 oder höher verfügen. Weitere Informationen finden Sie in der Amazon-Redshift-Python-Treiber-Lizenzvereinbarung.

Der Amazon-Redshift-Python-Konnektor stellt Folgendes bereit:

- AWS Identity and Access Management (IAM) -Authentifizierung. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.
- Authentifizierung des Identitätsanbieters mit föderiertem API Der föderierte API-Zugriff wird beispielsweise für folgende Unternehmensidentitätsanbieter unterstützt:
  - Azure AD. Weitere Informationen finden Sie im AWS Big-Data-Blogbeitrag Federate Amazon Redshift access with Microsoft Azure AD Single Sign-On.
  - Active Directory Federation Services Weitere Informationen finden Sie im AWS Big-Data-Blogbeitrag Verbundzugriff auf Ihren Amazon Redshift Redshift-Cluster mit Active Directory Federation Services (AD FS): Teil 1.
  - Okta Weitere Informationen finden Sie im AWS Big-Data-Blogbeitrag Federate Amazon Redshift access with Okta as a identity provider.
  - PingFederate. Weitere Informationen finden Sie auf der PingFederate Website.
  - JumpCloud. Weitere Informationen finden Sie auf der JumpCloudWebsite.
- Amazon-Redshift-Datentypen.

Der Amazon-Redshift-Python-Konnektor implementiert die Python-Datenbank-API-Spezifikation 2.0. Weitere Informationen finden Sie unter PEP 249 – Python-Datenbank-API-Spezifikation v2.0 auf der Python-Website.

Themen

- Installieren des Amazon-Redshift-Python-Konnektors
- Konfigurationsoptionen für den Amazon-Redshift-Python-Konnektor
- Importieren des Python-Konnektors
- Integration des Python-Konnektors mit NumPy
- Integrieren des Python-Konnektors in Pandas
- Verwenden von Identitätsanbieter-Plugins
- Beispiele für die Verwendung des Amazon-Redshift-Python-Konnektors
- API-Referenz für den Amazon-Redshift-Python-Konnektor

Installieren des Amazon-Redshift-Python-Konnektors

Sie können eine der folgenden Methoden verwenden, um den Amazon-Redshift-Python-Konnektor zu installieren:

- Python-Paketindex (PyPi)
- Conda
- Das GitHub Repository klonen

Installieren des Python-Konnektors aus dem PyPi

Um den Python-Konnektor aus dem Python-Paketindex (PyPI) zu installieren, können Sie pip verwenden. Führen Sie dazu den folgenden Befehl aus.

```
>>> pip install redshift_connector
```

Sie können den Konnektor in einer virtuellen Umgebung installieren. Führen Sie dazu den folgenden Befehl aus.

```
>>> pip install redshift_connector
```

Optional können Sie Pandas und NumPy mit dem Connector installieren.

```
>>> pip install "redshift_connector[full]"
```

Weitere Informationen finden zu Pip finden Sie auf der Pip-Website.

Installieren des Python-Konnektors über Conda

Sie können den Python-Konnektor von Anaconda.org installieren.

```
>>>conda install -c conda-forge redshift_connector
```

Installation des Python-Konnektors durch Klonen des GitHub Repositorys von AWS

Um den Python-Konnektor aus der Quelle zu installieren, klonen Sie das GitHub Repository von AWS. Richten Sie nach der Installation von Python und virtualenv Ihre Umgebung ein und installieren Sie die erforderlichen Abhängigkeiten, indem Sie die folgenden Befehle ausführen.

```
$ 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
```

Konfigurationsoptionen für den Amazon-Redshift-Python-Konnektor

Im Folgenden finden Sie Beschreibungen für die Optionen, die Sie für den Amazon-Redshift-Python-Konnektor angeben können.

access_key_id

- Standardwert – Keine
- Datentyp – Zeichenfolge

Der Zugriffsschlüssel der IAM-Rolle bzw. des IAM-Benutzers, die/der für die IAM-Datenbankauthentifizierung konfiguriert wurde.

Dieser Parameter ist optional.

allow_db_user_override

- Standardwert – false

- Datentyp – boolesch

Wahr

Gibt an, dass der Konnektor den `DbUser`-Wert aus der SAML-Assertion (Security Assertion Markup Language) verwendet.

Falsch

Gibt an, dass der Wert im `DbUser`-Verbindungsparameter verwendet wird.

Dieser Parameter ist optional.

app_name

- Standardwert – Keiner
- Datentyp – Zeichenfolge

Der Name der Identitätsanbieter-Anwendung (IdP), die für die Authentifizierung verwendet wird.

Dieser Parameter ist optional.

auth_profile

- Standardwert – Keines
- Datentyp – Zeichenfolge

Der Name eines Amazon-Redshift-Authentifizierungsprofils mit Verbindungseigenschaften als JSON. Weitere Informationen zur Benennung von Verbindungsparametern finden Sie in der `RedshiftProperty`-Klasse. Die`RedshiftProperty`-Klasse speichert vom Endbenutzer bereitgestellte und ggf. während des IAM-Authentifizierungsprozesses generierte Verbindungsparameter (z. B. temporäre IAM-Anmeldeinformationen). Weitere Informationen finden Sie in der RedshiftProperty Klasse.

Dieser Parameter ist optional.

auto_create

- Standardwert – false
- Datentyp – boolesch

Ein Wert, der angibt, ob der Benutzer erstellt werden soll, wenn der Benutzer nicht existiert.

Dieser Parameter ist optional.

Client-ID

- Standardwert – Keiner
- Datentyp – Zeichenfolge

Die Client-ID von Azure IdP.

Dieser Parameter ist optional.

client_secret

- Standardwert – Keine
- Datentyp – Zeichenfolge

Das Client-Geheimnis von Azure IdP.

Dieser Parameter ist optional.

cluster_identifier

- Standardwert – Keine
- Datentyp – Zeichenfolge

Die Cluster-Kennung des Amazon-Redshift-Clusters.

Dieser Parameter ist optional.

credentials_provider

- Standardwert – Keine
- Datentyp – Zeichenfolge

Der IdP, der zur Authentifizierung bei Amazon Redshift verwendet wird. Die folgenden Werte sind gültig:

- `AdfsCredentialsProvider`
- `AzureCredentialsProvider`
- `BrowserAzureCredentialsProvider`
- `BrowserSamlCredentialsProvider`
- `IdpTokenAuthPlugin`— Ein Autorisierungs-Plugin, das ein Identity Center (iDC) -Token oder OpenID Connect (OIDC) JSON-basierte Identitätstoken (JWT) von jedem mit dem iDC verknüpften Web-Identitätsanbieter akzeptiert.
- `PingCredentialsProvider`
- `OktaCredentialsProvider`

Dieser Parameter ist optional.

Datenbank

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Name der Datenbank, mit der Sie sich verbinden möchten.

Dieser Parameter ist optional.

database_metadata_current_db_only

- Standardwert – true
- Datentyp – boolesch

Ein Wert, der angibt, ob eine Anwendung Datashare-Kataloge mit mehreren Datenbanken unterstützt. Der Standardwert True gibt an, dass die Anwendung aus Gründen der Abwärtskompatibilität keine Datashare-Kataloge mit mehreren Datenbanken unterstützt.

Dieser Parameter ist optional.

db_groups

- Standardwert – Keine
- Datentyp – Zeichenfolge

Eine durch Kommas getrennte Liste vorhandener Datenbankgruppennamen, die der Benutzer für die aktuelle Sitzung durch Joins angegeben hat. DbUser

Dieser Parameter ist optional.

db_user

- Standardwert – Keine
- Datentyp – Zeichenfolge

Die Benutzer-ID, die mit Amazon Redshift verwendet werden soll.

Dieser Parameter ist optional.

endpoint_url

- Standardwert – Keine
- Datentyp – Zeichenfolge

Die Amazon-Redshift-Endpunkt-URL Diese Option ist nur für den AWS internen Gebrauch bestimmt.

Dieser Parameter muss angegeben werden.

group_federation

- Standardwert – false
- Datentyp – boolesch

Diese Option gibt an, ob Amazon-Redshift-IDP-Gruppen verwendet werden sollen.

Dieser Parameter ist optional.

true

Verwenden Sie Amazon Redshift-Identity-Provider (IDP)-Gruppen.

false

Verwenden Sie die STS-API und GetClusterCredentials den Benutzerverbund und geben Sie db_groups für die Verbindung an.

Host

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Hostname des Amazon-Redshift-Clusters.

Dieser Parameter ist optional.

iam

- Standardwert – false
- Datentyp – boolesch

Die IAM-Authentifizierung ist aktiviert.

Dieser Parameter muss angegeben werden.

iam_disable_cache

- Standardwert – false
- Datentyp – boolesch

Diese Option gibt an, ob die IAM-Anmeldeinformationen zwischengespeichert werden. Die IAM-Anmeldeinformationen werden standardmäßig zwischengespeichert. Dies verbessert die Leistung, wenn Anfragen an das API-Gateway gedrosselt werden.

Dieser Parameter ist optional.

identity_namespace

- Standardwert — null
- Datentyp – Zeichenfolge

Der Identitäts-Namespace, der bei der Authentifizierung verwendet werden soll. IdpTokenAuthPlugin Es hilft Redshift bei der Entscheidung, welche Identity Center-Instanz verwendet werden soll.

Wenn nur eine Identity Center-Instanz vorhanden ist oder wenn der Standard-Identitätsnamespace festgelegt ist, ist dieser Parameter optional. Andernfalls ist er erforderlich.

idpPort

- Standardwert – 7890
- Datentyp – Ganzzahl

Der Listen Port, an den der IdP die SAML-Assertion sendet.

Dieser Parameter muss angegeben werden.

idp_response_timeout

- Standardwert – 120
- Datentyp – Ganzzahl

Das Timeout für das Abrufen der SAML-Assertion vom IdP.

Dieser Parameter muss angegeben werden.

idp_tenant

- Standardwert – Keine
- Datentyp – Zeichenfolge

Der IdP-Tenant.

Dieser Parameter ist optional.

listen_port

- Standardwert – 7890
- Datentyp – Ganzzahl

Der Listen Port, an den der IdP die SAML-Assertion sendet.

Dieser Parameter ist optional.

login_url

- Standardwert – Keine

- Datentyp – Zeichenfolge

Die Single-Sign-On-URL für den IdP.

Dieser Parameter ist optional.

max_prepared_statements

- Standardwert – 1000
- Datentyp – Ganzzahl

Die maximale Anzahl von vorbereiteten Anweisungen, die gleichzeitig geöffnet sein können.

Dieser Parameter muss angegeben werden.

numeric_to_float

- Standardwert – false
- Datentyp – boolesch

Diese Option gibt an, ob der Konnektor numerische Datentypwerte von decimal.Decimal in Float konvertiert. Standardmäßig erhält der Konnektor numerische Datentypwerte als decimal.Decimal und konvertiert sie nicht.

Wir empfehlen nicht, numeric_to_float für Anwendungsfälle zu aktivieren, die Genauigkeit erfordern, da die Ergebnisse ggf. gerundet werden.

Weitere Informationen zu decimal.Decimal und den Kompromissen im Hinblick auf decimal.Decimal und Float finden Sie unter decimal – Dezimale Festpunkt- und Gleitkomma-Arithmetik auf der Python-Website.

Dieser Parameter ist optional.

partner_sp_id

- Standardwert – Keine
- Datentyp – Zeichenfolge

Die Partner-SP-ID, die für die Authentifizierung mit Ping verwendet wird.

Dieser Parameter ist optional.

password

- Standardwert – Kein
- Datentyp – Zeichenfolge

Das Passwort, das für die Authentifizierung verwendet werden soll.

Dieser Parameter ist optional.

port

- Standardwert – 5 439
- Datentyp – Ganzzahl

Die Portnummer für den Amazon-Redshift-Cluster.

Dieser Parameter muss angegeben werden.

preferred_role

- Standardwert – Kein
- Datentyp – Zeichenfolge

Die für die aktuelle Verbindung bevorzugte IAM-Rolle.

Dieser Parameter ist optional.

principal_arn

- Standardwert – Keine
- Datentyp – Zeichenfolge

Der Amazon-Ressourcenname (ARN) des Benutzers oder der IAM-Rolle, für die Sie eine Richtlinie erstellen. Es wird empfohlen, eine Richtlinie an eine Rolle anzufügen und die Rolle Ihrem Benutzer für den Zugriff zuzuweisen.

Dieser Parameter ist optional.

profile

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Name eines Profils in einer AWS Anmeldeinformationsdatei, die AWS Anmeldeinformationen enthält.

Dieser Parameter ist optional.

provider_name

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Name des Anbieters für die systemeigene Authentifizierung von Redshift.

Dieser Parameter ist optional.

region

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der AWS-Region Ort, an dem sich der Cluster befindet.

Dieser Parameter ist optional.

role_arn

- Standardwert – Keine
- Datentyp – Zeichenfolge

Den Amazon-Ressourcennamen (ARN) der Rolle, die der Anrufer übernehmen soll. Dieser Parameter wird von dem Anbieter verwendet, der mit `JwtCredentialsProvider` angegeben ist.

Für den `JwtCredentialsProvider`-Anbieter ist dieser Parameter obligatorisch. Andernfalls ist dieser Parameter optional.

role_session_name

- Standardwert – jwt_redshift_session
- Datentyp – Zeichenfolge

Ein Bezeichner für die Sitzung der angenommenen Rolle. Normalerweise übergeben Sie den Namen oder den Bezeichner, der dem Benutzer Ihrer Anwendung zugeordnet ist. Die temporären Sicherheitsanmeldeinformationen, die Ihre Anwendung verwendet, sind diesem Benutzer zugeordnet. Dieser Parameter wird von dem Anbieter verwendet, der mit `JwtCredentialsProvider` angegeben ist.

Dieser Parameter ist optional.

scope

- Standardwert – Kein
- Datentyp – Zeichenfolge

Eine durch Leerzeichen getrennte Liste von Bereichen, denen der Benutzer zustimmen kann. Sie geben diesen Parameter an, damit Ihre Anwendung die Zustimmung zu APIs einholen kann, die Sie aufrufen möchten. Sie können diesen Parameter angeben, wenn Sie BrowserAzure OAuth2 CredentialsProvider für die Option Plugin_Name angeben.

Dieser Parameter ist für das OAuth2-Plug-In erforderlich. BrowserAzure CredentialsProvider

secret_access_key_id

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der geheime Zugriffsschlüssel der IAM-Rolle bzw. des IAM-Benutzers, die/der für die IAM-Datenbankauthentifizierung konfiguriert wurde.

Dieser Parameter ist optional.

session_token

- Standardwert – Keine

- Datentyp – Zeichenfolge

Der Zugriffsschlüssel der IAM-Rolle bzw. des IAM-Benutzers, die/der für die IAM-Datenbankauthentifizierung konfiguriert wurde. Dieser Parameter ist erforderlich, wenn temporäre AWS Anmeldeinformationen verwendet werden.

Dieser Parameter ist optional.

serverless_acct_id

- Standardwert – Kein
- Datentyp – Zeichenfolge

Die Konto-ID von Amazon Redshift Serverless.

Dieser Parameter ist optional.

serverless_work_group

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Name der Amazon-Redshift-Serverless-Arbeitsgruppe.

Dieser Parameter ist optional.

ssl

- Standardwert – true
- Datentyp – boolesch

Secure Sockets Layer (SSL) ist aktiviert.

Dieser Parameter muss angegeben werden.

ssl_insecure

- Standardwert – true
- Datentyp – boolesch

Ein Wert, der angibt, ob das IdP-Host-Serverzertifikat überprüft werden soll.

Dieser Parameter ist optional.

sslmode

- Standardwert – verify-ca
- Datentyp – Zeichenfolge

Die Sicherheit der Verbindung zu Amazon Redshift. Sie können einen der folgenden Werte angeben:

- verify-ca
- verify-full

Dieser Parameter muss angegeben werden.

timeout

- Standardwert – Kein
- Datentyp – Ganzzahl

Die Anzahl der Sekunden, die gewartet werden soll, bevor eine Zeitüberschreitung für einen Verbindungsversuch mit dem Server eintritt.

Dieser Parameter ist optional.

Token

- Standardwert — null
- Datentyp – Zeichenfolge

Das Identity Center (iDC) bereitgestellte Zugriffstoken oder ein OpenID Connect (IDC) JSON-basiertes Identitätstoken (JWT), das von einem Web-Identitätsanbieter bereitgestellt wird, der mit dem IDC verknüpft ist. Ihre Anwendung muss dieses Token generieren, indem sie den Benutzer Ihrer Anwendung beim IdC oder einem mit dem IdC verknüpften Web-Identitätsanbieter authentifiziert.

Dieser Parameter ist nur bei der Authentifizierung mit erforderlich. IdpTokenAuthPlugin

token_type

- Standardwert — null
- Datentyp – Zeichenfolge

Der Tokentyp, der in verwendet wird IdpTokenAuthPlugin.

Dieser Parameter ist nur bei der Authentifizierung mit IdpTokenAuthPlugin erforderlich.

Sie können die folgenden Werte angeben:

- `ACCESS_TOKEN`— Geben Sie diesen Wert an, wenn Sie ein von Identity Center (IdC) bereitgestelltes Zugriffstoken verwenden.
- `EXT_JWT`— Geben Sie diesen Wert an, wenn Sie ein OpenID Connect (OIDC) JSON-basiertes Identitätstoken (JWT) verwenden, das von einem externen Web-Identitätsanbieter bereitgestellt wird, der mit dem IdC verknüpft ist.

user

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Benutzername für die Autorisierung.

Dieser Parameter ist optional.

web_identity_token

- Standardwert – Kein
- Datentyp – Zeichenfolge

Das OAuth-2.0-Zugriffstoken oder OpenID-Connect-ID-Token, das vom Identitätsanbieter bereitgestellt wird. Stellen Sie sicher, dass Ihre Anwendung dieses Token abruft, indem Sie den Benutzer Ihrer Anwendung bei einem Web-Identitätsanbieter authentifizieren. Dieser Parameter wird von dem Anbieter verwendet, der mit `JwtCredentialsProvider` angegeben ist.

Für den `JwtCredentialsProvider`-Anbieter ist dieser Parameter obligatorisch. Andernfalls ist dieser Parameter optional.

Importieren des Python-Konnektors

Um den Python-Konnektor zu importieren, führen Sie den folgenden Befehl aus.

```
>>> import redshift_connector
```

Amazon Redshift importieren NumPy und eine Verbindung zu Amazon Redshift herstellen

Führen Sie die folgenden Befehle aus, um den Amazon Redshift Python-Konnektor und Numerical Python (NumPy) zu importieren.

```
import redshift_connector
import numpy
```

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Anmeldeinformationen eine Verbindung zu einem Amazon Redshift Redshift-Cluster herzustellen.

```
conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
 )
```

Integration des Python-Konnektors mit NumPy

Es folgt ein Beispiel für die Integration des Python-Konnektors mit 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)
```

Das Ergebnis sieht wie folgt aus.

```
[['One Hundred Years of Solitude' 'Gabriel García Márquez']
['A Brief History of Time' 'Stephen Hawking']]
```

Integrieren des Python-Konnektors in Pandas

Es folgt ein Beispiel für die Integration des Python-Konnektors in 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)
```

Verwenden von Identitätsanbieter-Plugins

Allgemeine Informationen zur Verwendung von Identitätsanbieter-Plug-ins finden Sie unter Optionen für die Bereitstellung von IAM-Anmeldeinformationen. Weitere Informationen zur Verwaltung von IAM-Identitäten, einschließlich bewährter Methoden für IAM-Rollen, finden Sie unter Identity and Access Management in Amazon Redshift.

Authentifizierung mit dem ADFS-Identitätsanbieter-Plug-In

Es folgt ein Beispiel für die Verwendung des Identitätsanbieter-Plug-Ins für den Active Directory Federation Service (ADFS), um einen Benutzer zu authentifizieren, der sich mit einer Amazon-Redshift-Datenbank verbindet.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='AdfsCredentialsProvider',
    user='brooke@myadfshostname.com',
    password='Hunter2',
    idp_host='myadfshostname.com'
)
```

Authentifizierung mit dem Azure-Identitätsanbieter-Plug-In

Es folgt ein Beispiel für die Authentifizierung mit dem Azure-Identitätsanbieter-Plug-In. Sie können wie folgt Werte für `client_id` und `client_secret` für eine Azure-Enterprise-Anwendung erstellen.

```
>>>  con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='AzureCredentialsProvider',
    user='brooke@myazure.org',
    password='Hunter2',
    idp_tenant='my_idp_tenant',
    client_id='my_client_id',
    client_secret='my_client_secret',
    preferred_role='arn:aws:iam:123:role/DataScientist'
)
```

Authentifizierung mit dem Azure-Browser-Identitätsanbieter-Plug-In

Es folgt ein Beispiel für die Verwendung des Azure-Browser-Identitätsanbieter-Plug-Ins zur Authentifizierung eines Benutzers, der sich mit einer Amazon-Redshift-Datenbank verbindet.

Die Multi-Faktor-Authentifizierung erfolgt im Browser, wo die Anmeldeinformationen vom Benutzer angegeben werden.

```
>>>con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='BrowserAzureCredentialsProvider',
    idp_tenant='my_idp_tenant',
    client_id='my_client_id',
)
```

Authentifizierung mit dem Okta-Identitätsanbieter-Plug-In

Es folgt ein Beispiel für die Authentifizierung mit dem Okta-Identitätsanbieter-Plug-In. Sie können die Werte für `idp_host`, `app_id` und `app_name` über die Okta-Anwendung erhalten.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='OktaCredentialsProvider',
    user='brooke@myazure.org',
    password='hunter2',
    idp_host='my_idp_host',
    app_id='my_first_appetizer',
    app_name='dinner_party'
)
```

Authentifizierung JumpCloud mithilfe eines generischen SAML-Browser-Identity-Provider-Plug-ins

Im Folgenden finden Sie ein Beispiel für die Verwendung JumpCloud mit einem generischen SAML-Browser-Identity-Provider-Plugin zur Authentifizierung.

Der Passwort-Parameter muss angegeben werden. Sie müssen diesen Parameter jedoch nicht eingeben, da die Multi-Faktor-Authentifizierung im Browser stattfindet.

```
>>> 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'
)
```

Beispiele für die Verwendung des Amazon-Redshift-Python-Konnektors

Im Folgenden finden Sie Beispiele zur Verwendung des Amazon-Redshift-Python-Konnektors. Um sie auszuführen, müssen Sie zuerst den Python-Konnektor installieren. Weitere Informationen zum Installieren des Python-Konnektors von Amazon Redshift finden Sie unter Installieren des Amazon-Redshift-Python-Konnektors. Weitere Informationen zu den Konfigurationsoptionen, die Sie mit dem Python-Konnektor verwenden können, finden Sie unter Konfigurationsoptionen für den Amazon-Redshift-Python-Konnektor.

Themen

- Mit Anmeldeinformationen eine Verbindung zu einem Amazon Redshift Redshift-Cluster herstellen und ihn abfragen AWS
- Aktivieren von Autocommit
- Konfiguration des Paramstyle-Werts für den Cursor
- Kopieren von Daten mit COPY aus einem Amazon-S3-Bucket und Verwenden von UNLOAD, um Daten in den Bucket zu schreiben

Mit Anmeldeinformationen eine Verbindung zu einem Amazon Redshift Redshift-Cluster herstellen und ihn abfragen AWS

Das folgende Beispiel zeigt Ihnen, wie Sie mithilfe Ihrer AWS Anmeldeinformationen eine Verbindung zu einem Amazon Redshift Redshift-Cluster herstellen, dann eine Tabelle abfragen und die Abfrageergebnisse abrufen.

```
#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'])
```

Aktivieren von Autocommit

Die Autocommit-Eigenschaft ist gemäß der Python-Datenbank-API-Spezifikation standardmäßig deaktiviert. Sie können die folgenden Befehle verwenden, um die autocommit-Eigenschaft der Verbindung nach dem Ausführen eines Rollback-Befehls zu aktivieren und sicherzustellen, dass sich keine Transaktion in Bearbeitung befindet.

```
#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
```

Konfiguration des Paramstyle-Werts für den Cursor

Der Paramstyle-Wert für einen Cursor kann über cursor.paramstyle geändert werden. Der verwendete Paramstyle-Standardwert ist `format`. Gültige Werte für den Parameter sind `qmark`, `numeric`, `named`, `format` und `pyformat`.

Im Folgenden finden Sie Beispiele für die Verwendung verschiedener Paramstyle-Werte, um Parameter an eine SQL-Beispielanweisung zu übergeben.

```
# 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"})
```

Kopieren von Daten mit COPY aus einem Amazon-S3-Bucket und Verwenden von UNLOAD, um Daten in den Bucket zu schreiben

Das folgende Beispiel zeigt, wie Daten aus einem Amazon-S3-Bucket in eine Tabelle kopiert und dann aus der Tabelle wieder in den Bucket entladen werden.

Eine Textdatei mit dem Namen `category_csv.txt` und den folgenden Daten wird in einen Amazon-S3-Bucket hochgeladen.

```
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"
```

Es folgt ein Beispiel für den Python-Code, der sich zuerst mit der Amazon-Redshift-Datenbank verbindet. Anschließend wird eine Tabelle `category` erstellt und die CSV-Daten werden aus dem S3 Bucket in die Tabelle kopiert.

```
#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'])
```

Wenn Sie den Wert für `autocommit` nicht auf „true“ gesetzt haben, führen Sie mit `conn.commit()` einen Commit durch, nachdem Sie die `execute()`-Anweisungen ausgeführt haben.

Die Daten werden in die Datei `unloaded_category_csv.text0000_part00` im S3-Bucket mit folgendem Inhalt entladen:

```
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"
```

API-Referenz für den Amazon-Redshift-Python-Konnektor

Im Folgenden finden Sie eine Beschreibung der API-Operationen des Amazon-Redshift-Python-Konnektors.

redshift_connector

Im Folgenden finden Sie eine Beschreibung der `redshift_connector` API-Operation.

`connect(user, database, password[, port, …])`

Stellt eine Verbindung zu einem Amazon-Redshift-Cluster her. Diese Funktion validiert Benutzereingaben, authentifiziert sich optional mit einem Identitätsanbieter-Plug-In und erstellt dann ein Verbindungsobjekt.

`apilevel`

Die unterstützte DBAPI-Ebene, derzeit „2.0".

`paramstyle`, `str(object='') -> str str(bytes_or_buffer[, encoding[, errors]]) -> str`

Der global zu verwendende Datenbank-API-Parameterstil.

Verbindung

Im Folgenden finden Sie eine Beschreibung der Verbindungs-API-Operationen für den Amazon-Redshift-Python-Konnektor.

`__init__(user, password, database[, host, …])`

Initialisiert ein rohes Verbindungsobjekt.

`cursor`

Erstellt ein Cursor-Objekt, das an diese Verbindung gebunden ist.

`commit`

Führt einen Commit der aktuellen Datenbanktransaktion aus.

`rollback`

Rollt die aktuelle Datenbanktransaktion zurück.

`close`

Schließt die Datenbankverbindung.

`execute(cursor, operation, vals)`

Führt den angegebenen SQL-Befehl aus. Sie können die Parameter als Sequenz oder als Mapping angeben, abhängig vom Wert von `redshift_connector.paramstyle`.

`run(sql[, stream])`

Führt den angegebenen SQL-Befehl aus. Optional können Sie einen Stream zur Verwendung mit dem Befehl COPY bereitstellen.

`xid(format_id, global_transaction_id, …)`

Erstellen Sie eine Transaktions-ID. Nur der `global_transaction_id`-Parameter wird in Postgres verwendet. format_id und branch_qualifier werden nicht in Postgres verwendet. Der `global_transaction_id` kann jeder String-Bezeichner sein, der von Postgres unterstützt wird und ein Tupel zurückgibt (`format_id`, `global_transaction_id`, `branch_qualifier`).

`tpc_begin(xid)`

Startet eine TPC-Transaktion mit einer Transaktions-ID `xid` bestehend aus einer Format-ID, einer globalen Transaktions-ID und einem Branch Qualifier.

`tpc_prepare`

Führt die erste Phase einer mit .tpc_begin gestarteten Transaktion aus.

`tpc_commit([xid])`

Wenn es ohne Argumente aufgerufen wird, führt .tpc_commit einen Commit für eine TPC-Transaktion aus, die zuvor mit .tpc_prepare() vorbereitet wurde.

`tpc_rollback([xid])`

Wenn es ohne Argumente aufgerufen wird, rollt .tpc_rollback eine TPC-Transaktion zurück.

`tpc_recover`

Gibt eine Liste ausstehender Transaktions-IDs zurück, die für die Verwendung mit .tpc_commit(xid) oder .tpc_rollback(xid) geeignet sind.

Cursor

Im Folgenden finden Sie eine Beschreibung der Cursor-API-Operation.

`__init__(connection[, paramstyle])`

Initialisiert ein rohes Cursor-Objekt.

`insert_data_bulk(filename, table_name, parameter_indices, column_names, delimiter, batch_size)`

Führt eine Massen-INSERT-Anweisung aus.

`execute(operation[, args, stream, …])`

Führt einen Datenbankvorgang aus.

`executemany(operation, param_sets)`

Bereitet einen Datenbankvorgang vor und führt ihn dann für alle bereitgestellten Parametersequenzen oder Mappings aus.

`fetchone`

Ruft die nächste Zeile eines Abfrageergebnissatzes ab.

`fetchmany([num])`

Ruft die nächste Reihe von Zeilen eines Abfrageergebnisses ab.

`fetchall`

Ruft alle verbleibenden Zeilen eines Abfrageergebnisses ab.

`close`

Schließt den Cursor jetzt.

`__iter__`

Ein Cursorobjekt kann iteriert werden, um die Zeilen aus einer Abfrage abzurufen.

`fetch_dataframe([num])`

Gibt einen Datenrahmen der letzten Abfrageergebnisse zurück.

`write_dataframe(df, table)`

Schreibt denselben Strukturdatenrahmen in eine Amazon-Redshift-Datenbank.

`fetch_numpy_array([num])`

Gibt ein NumPy Array der letzten Abfrageergebnisse zurück.

`get_catalogs`

Amazon Redshift unterstützt nicht mehrere Kataloge über eine einzige Verbindung. Amazon Redshift gibt nur den aktuellen Katalog zurück.

`get_tables([catalog, schema_pattern, …])`

Gibt die eindeutigen öffentlichen Tabellen zurück, die innerhalb des Systems benutzerdefiniert sind.

`get_columns([catalog, schema_pattern, …])`

Gibt eine Liste aller Spalten in einer bestimmten Tabelle einer Amazon-Redshift-Datenbank zurück.

AdfsCredentialsProvider Plugin

Im Folgenden finden Sie die Syntax für den AdfsCredentialsProvider Plugin-API-Vorgang für den Amazon Redshift Python-Konnektor.

```
redshift_connector.plugin.AdfsCredentialsProvider()
```

AzureCredentialsProvider Plugin

Im Folgenden finden Sie die Syntax für den AzureCredentialsProvider Plugin-API-Vorgang für den Amazon Redshift Python-Konnektor.

```
redshift_connector.plugin.AzureCredentialsProvider()
```

BrowserAzureCredentialsProvider Plugin

Im Folgenden finden Sie die Syntax für den BrowserAzureCredentialsProvider Plugin-API-Vorgang für den Amazon Redshift Python-Konnektor.

```
redshift_connector.plugin.BrowserAzureCredentialsProvider()
```

BrowserSamlCredentialsProvider Plugin

Im Folgenden finden Sie die Syntax für den BrowserSamlCredentialsProvider Plugin-API-Vorgang für den Amazon Redshift Python-Konnektor.

```
redshift_connector.plugin.BrowserSamlCredentialsProvider()
```

OktaCredentialsProvider Plugin

Im Folgenden finden Sie die Syntax für den OktaCredentialsProvider Plugin-API-Vorgang für den Amazon Redshift Python-Konnektor.

```
redshift_connector.plugin.OktaCredentialsProvider()
```

PingCredentialsProvider Plugin

Im Folgenden finden Sie die Syntax für den PingCredentialsProvider Plugin-API-Vorgang für den Amazon Redshift Python-Konnektor.

```
redshift_connector.plugin.PingCredentialsProvider()
```

SamlCredentialsProvider Plugin

Im Folgenden finden Sie die Syntax für den SamlCredentialsProvider Plugin-API-Vorgang für den Amazon Redshift Python-Konnektor.

```
redshift_connector.plugin.SamlCredentialsProvider()
```

Amazon-Redshift-Integration für Apache Spark

Apache Spark ist ein verteiltes Verarbeitungs-Framework und Programmiermodell, mit dem Sie Machine Learning, Stream-Verarbeitung oder Graph-Analysen durchführen können. Ähnlich wie Apache Hadoop ist Spark ein verteiltes Open-Source-Verarbeitungssystem, das häufig für große Workloads verwendet wird. Spark verfügt über eine optimierte Engine zur Ausführung gerichteter

azyklischer Graphen und speichert Daten aktiv im In-Memory-Cache. Dies kann die Leistung steigern, insbesondere bei bestimmten Algorithmen und interaktiven Abfragen.

Mit dieser Integration erhalten Sie einen Spark-Connector, mit dem Sie Apache-Spark-Anwendungen erstellen können, die Daten in Amazon Redshift und Amazon Redshift Serverless lesen und schreiben. Diese Anwendungen gehen keine Kompromisse bei der Anwendungsleistung oder der transaktionalen Konsistenz der Daten ein. Diese Integration ist automatisch in Amazon EMR und AWS Glue enthalten, sodass Sie sofort Apache-Spark-Aufträge ausführen können, die im Rahmen Ihrer Datenerfassungs- und Transformationspipelines auf Daten zugreifen und diese in Amazon Redshift laden.

Derzeit können Sie mit dieser Integration die Versionen 3.3.0, 3.3.1, 3.3.2 und 3.4.0 von Spark verwenden.

Diese Integration bietet Folgendes:

- AWS Identity and Access Management (IAM)-Authentifizierung. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.
- Prädikat- und Abfrage-Pushdown zur Verbesserung der Leistung.
- Amazon-Redshift-Datentypen.
- Konnektivität mit Amazon Redshift und Amazon Redshift Serverless.

Überlegungen und Einschränkungen bei der Verwendung des Spark-Connectors

- Die Tempdir-URI verweist auf einen Amazon-S3-Speicherort. Dieses temporäre Verzeichnis wird nicht automatisch bereinigt und kann zusätzliche Kosten verursachen. Wir empfehlen, die Lebenszyklusrichtlinien für Amazon S3 im Benutzerhandbuch für Amazon Simple Storage Service zu verwenden, um die Aufbewahrungsregeln für den Amazon-S3-Bucket zu definieren.
- Standardmäßig funktionieren Kopien zwischen Amazon S3 und Redshift nicht, wenn sich der S3-Bucket und der Redshift-Cluster in unterschiedlichen AWS-Regionen befinden. Um separate AWS-Regionen zu verwenden, setzen Sie den Parameter `tempdir_region` auf die Region des S3-Buckets, der für `tempdir` verwendet wird.
- Regionsübergreifende Schreibvorgänge zwischen S3 und Redshift beim Schreiben von Parquet-Daten mit dem `tempformat`-Parameter.
- Wir empfehlen die Verwendung der serverseitigen Amazon-S3-Verschlüsselung, um die verwendeten Amazon-S3-Buckets zu verschlüsseln.
- Wir empfehlen, den öffentlichen Zugriff auf Amazon-S3-Buckets zu blockieren.

- Wir empfehlen, den Amazon-Redshift-Cluster nicht öffentlich zugänglich zu machen.
- Wir empfehlen, die Amazon-Redshift-Auditprotokollierung zu aktivieren.
- Wir empfehlen, die Amazon-Redshift-Verschlüsselung im Ruhezustand zu aktivieren.
- Wir empfehlen, SSL für die JDBC-Verbindung von Spark auf Amazon EMR zu Amazon Redshift zu aktivieren.
- Wir empfehlen, eine IAM-Rolle mit dem Parameter `aws_iam_role` für den Amazon-Redshift-Authentifizierungsparameter zu übergeben.

Authentifizierung mit dem Spark-Connector

Das folgende Diagramm beschreibt die Authentifizierung zwischen Amazon S3, Amazon Redshift, dem Spark-Treiber und Spark-Executors.

Authentifizierung zwischen Redshift und Spark

Sie können den von Amazon Redshift bereitgestellten JDBC-Treiber Version 2 verwenden, um durch die Angabe von Anmeldeinformationen mit dem Spark-Connector eine Verbindung mit Amazon Redshift herzustellen. Wenn Sie IAM verwenden möchten, konfigurieren Sie Ihre JDBC-URL so, dass die IAM-Authentifizierung verwendet wird. Wenn Sie von Amazon EMR oder AWS Glue aus eine Verbindung mit einem Redshift-Cluster herstellen möchten, stellen Sie sicher, dass Ihre IAM-Rolle über die erforderlichen Berechtigungen zum Abrufen von temporären IAM-Anmeldeinformationen verfügt. In der folgenden Liste werden alle Berechtigungen beschrieben, die Ihre IAM-Rolle benötigt, um Anmeldeinformationen abzurufen und Amazon-S3-Operationen auszuführen.

- Redshift:GetClusterCredentials (für bereitgestellte Redshift-Cluster)
- Redshift:DescribeClusters (für bereitgestellte Redshift-Cluster)
- Redshift:GetWorkgroup (für Arbeitsgruppen in Amazon Redshift Serverless)
- Redshift:GetCredentials (für Arbeitsgruppen in Amazon Redshift Serverless)
- s3:ListBucket
- s3:GetBucket
- s3:GetObject
- s3:PutObject
- s3:GetBucketLifecycleConfiguration

Weitere Informationen zu GetClusterCredentials finden Sie unter Ressourcenbasierte Richtlinien für „GetClusterCredentials“.

Sie müssen außerdem sicherstellen, dass Amazon Redshift die IAM-Rolle während `COPY`- und `UNLOAD`-Operationen übernehmen kann.

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

Wenn Sie den aktuellen JDBC-Treiber verwenden, verwaltet der Treiber die Umstellung von einem selbstsignierten Amazon-Redshift-Zertifikat auf ein ACM-Zertifikat automatisch. Sie müssen jedoch die SSL-Optionen für die JDBC-URL angeben.

Im Folgenden finden Sie ein Beispiel dafür, wie Sie die JDBC-Treiber-URL und `aws_iam_role` angeben, um eine Verbindung mit Amazon Redshift herstellen.

```
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()
```

Authentifizierung zwischen Amazon S3 und Spark

Wenn Sie eine IAM-Rolle für die Authentifizierung zwischen Spark und Amazon S3 verwenden, nutzen Sie eine der folgenden Methoden:

- Das AWS SDK für Java versucht automatisch, AWS-Anmeldeinformationen zu finden, indem es die standardmäßige Anbieterkette für Anmeldeinformationen verwendet, die von der Klasse

DefaultAWSCredentialsProviderChain implementiert wird. Weitere Informationen finden Sie unter Verwenden der standardmäßigen Anbieterkette von Anmeldeinformationen.

- Sie können AWS-Schlüssel über die Hadoop-Konfigurationseigenschaften angeben. Wenn Ihre `tempdir`-Konfiguration beispielsweise auf ein `s3n://`-Dateisystem verweist, legen Sie die Eigenschaften `fs.s3n.awsAccessKeyId` und `fs.s3n.awsSecretAccessKey` in einer Hadoop-XML-Konfigurationsdatei fest oder rufen Sie `sc.hadoopConfiguration.set()` auf, um die globale Hadoop-Konfiguration von Spark zu ändern.

Wenn Sie beispielsweise das s3n-Dateisystem verwenden, fügen Sie Folgendes hinzu:

```
sc.hadoopConfiguration.set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3n.awsSecretAccessKey", "YOUR_SECRET_ACCESS_KEY")
```

Fügen Sie für das s3a-Dateisystem Folgendes hinzu:

```
sc.hadoopConfiguration.set("fs.s3a.access.key", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3a.secret.key", "YOUR_SECRET_ACCESS_KEY")
```

Wenn Sie Python verwenden, verwenden Sie die folgenden Operationen:

```
sc._jsc.hadoopConfiguration().set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc._jsc.hadoopConfiguration().set("fs.s3n.awsSecretAccessKey",
 "YOUR_SECRET_ACCESS_KEY")
```

- Codieren Sie die Authentifizierungsschlüssel in der `tempdir`-URL. Beispielsweise codiert die URI `s3n://ACCESSKEY:SECRETKEY@bucket/path/to/temp/dir` das Schlüsselpaar (`ACCESSKEY`, `SECRETKEY`).

Authentifizierung zwischen Redshift und Amazon S3

Wenn Sie die Befehle COPY und UNLOAD in der Abfrage verwenden, müssen Sie Amazon S3 außerdem Zugriff auf Amazon Redshift gewähren, um Abfragen in Ihrem Namen auszuführen. Autorisieren Sie dazu zunächst Amazon Redshift, auf andere AWS-Services zuzugreifen, und autorisieren Sie dann die COPY- und die UNLOAD-Operation mithilfe von IAM-Rollen.

Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Integration in AWS Secrets Manager

Sie können Ihren Redshift-Benutzernamen und Ihr Passwort aus einem gespeicherten Secret in AWS Secrets Manager abrufen. Wenn Sie Redshift-Anmeldeinformationen automatisch bereitstellen möchten, verwenden Sie den `secret.id`-Parameter. Weitere Informationen zum Erstellen eines Secrets für Redshift-Anmeldeinformationen Sie unter Erstellen einesAWS Secrets Manager-Datenbank-Secrets.

GroupID	ArtifactID	Unterstützte Revision(en)	Beschreibung
com.amazonaws.secretsmanager	aws-secretsmanager-jdbc	1.0.12	Mit der AWS Secrets Manager SQL Connection Library for Java können Java-Entwickler mithilfe von Secrets, die in AWS Secrets Manager gespeichert sind, auf einfache Weise eine Verbindung mit SQL-Datenbanken herstellen.

> **Note**
>
> Danksagung: Diese Dokumentation enthält Beispielcode und Sprache, die von der Apache Software Foundation entwickelt wurden und unter der Apache-2.0-Lizenz lizenziert sind.

Leistungsverbesserungen mit Pushdown

Der Spark-Connector wendet automatisch Prädikat- und Abfrage-Pushdown an, um die Leistung zu optimieren. Diese Unterstützung bedeutet, dass der Spark-Connector, wenn Sie eine unterstützte Funktion in der Abfrage verwenden, diese Funktion in eine SQL-Abfrage umwandelt und die Abfrage in Amazon Redshift ausführt. Durch diese Optimierung werden weniger Daten abgerufen, sodass

Apache Spark weniger Daten verarbeiten und eine bessere Leistung erzielen kann. Standardmäßig ist Pushdown automatisch aktiviert. Zum Deaktivieren muss `autopushdown` auf „false“ festgelegt werden.

```
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()
```

Die folgenden Funktionen werden mit Pushdown unterstützt. Wenn Sie eine Funktion verwenden, die nicht in dieser Liste enthalten ist, führt der Spark-Connector die Funktion in Spark anstatt in Amazon Redshift aus, was dazu führt, dass die Leistung nicht optimiert ist. Eine vollständige Liste der Funktionen in Spark finden Sie unter Built-in Functions (Eingebaute Funktionen).

- Aggregationsfunktionen
  - avg
  - count
  - max
  - Min.
  - sum
  - stddev_samp
  - stddev_pop
  - var_samp
  - var_pop
- Boolesche Operatoren
  - in
  - isnull
  - isnotnull
  - enthält
  - endswith
  - startswith

- Logische Operatoren
  - und
  - oder
  - nicht (oder !)
- Mathematische Funktionen
  - +
  - -
  - *
  - /
  - - (unär)
  - abs
  - acos
  - asin
  - atan
  - ceil
  - cos
  - exp
  - floor
  - greatest
  - least
  - log10
  - pi
  - pow
  - round
  - sin
  - sqrt
  - tan
- Verschiedene Funktionen
  - cast
  - COALESCE

  - Dezimalwert
  - if
  - in
- Relationale Operatoren
  - !=
  - =
  - >
  - >=
  - <
  - <=
- Zeichenfolgenfunktionen
  - ascii
  - lpad
  - rpad
  - translate
  - upper
  - lower
  - length
  - trim
  - ltrim
  - rtrim
  - like
  - substring
  - concat
- Funktionen für Datum/Uhrzeit
  - add_months
  - date
  - date_add
  - date_sub
  - date_trunc

  - timestamp
  - trunc
- Mathematische Operationen
  - CheckOverflow
  - PromotePrecision
- Relationale Operationen
  - Aliase (zum Beispiel AS)
  - CaseWhen
  - Distinct
  - InSet
  - Verknüpfungen und Cross-Joins
  - Einschränkungen
  - Unions, union all
  - ScalarSubquery
  - Sorts (aufsteigend und absteigend)
  - UnscaledValue

Andere Konfigurationsoptionen

Ändern der maximalen Größe von Zeichenfolgespalten

Während des Erstellens von Tabellen erstellt Redshift Zeichenfolgespalten als Textspalten, die als VARCHAR(256) gespeichert werden. Wenn Sie Spalten benötigen, die größere Größen unterstützen, können Sie die maximale Länge von Zeichenfolgespalten mithilfe von maxlength angeben. Nachstehend finden Sie ein Beispiel zum Angeben von `maxlength`.

```
columnLengthMap.foreach { case (colName, length) =>
  val metadata = new MetadataBuilder().putLong("maxlength", length).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

Festlegen eines Spaltentyps

Verwenden Sie das Feld `redshift_type`, um einen Spaltentyp festzulegen.

```
columnTypeMap.foreach { case (colName, colType) =>
  val metadata = new MetadataBuilder().putString("redshift_type", colType).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

Festlegen einer Kompressionskodierung für eine Spalte

Verwenden Sie das Kodierungsfeld, um eine spezifische Kompressionskodierung für eine Spalte zu verwenden. Eine vollständige Liste der unterstützten Kompressionskodierungen finden Sie unter Kompressionskodierungen.

Angeben einer Beschreibung für eine Spalte

Verwenden Sie das Feld `description`, um eine Beschreibung anzugeben.

Authentifizierung zwischen Redshift und Amazon S3

Standardmäßig wird das Ergebnis im Parquet-Format in Amazon S3 entladen. Geben Sie folgende Option an, um das Ergebnis als Textdatei mit Pipe-Trennzeichen zu entladen.

```
.option("unload_s3_format", "TEXT")
```

Pushdown-Anweisungen träge ausführen

Parameter	Erforderlich	Standard	Beschreibung
spark.datasource.redshift.community.autopushdown.lazyMode	Nein	Wahr	Gibt an, ob der Connector Pushdown-Anweisungen in Redshift träge ausführen soll. Wenn der Wert true ist, ruft der Spark-Connector alle zugehörigen Modelle und Informationen ab, bevor die Abfrage ausgeführt wird, was

Parameter	Erforderlich	Standard	Beschreibung
			in der Regel zu einer besseren Leistung führt. Wenn der Wert false ist, führt der Spark-Connector Pushdown-Anweisungen sofort im Spark-Treiber-Hauptthread aus und wird ausdrucks übergreifend serialisiert.

Connector-Parameter

Die Parameterzuordnung oder `OPTIONS` in Spark SQL unterstützt die folgenden Einstellungen.

Parameter	Erforderlich	Standard	Beschreibung
dbtable	Ja, wenn keine Abfrage angegeben ist	–	Die Tabelle, die in Redshift erstellt oder aus der gelesen werden soll. Dieser Parameter ist erforderlich, wenn Sie Daten in Redshift speichern.
query	Ja, wenn dbtable nicht angegeben ist	–	Die Abfrage, aus der in Redshift gelesen werden soll.
user	Nein	–	Der Redshift-Benutzername. Muss

Parameter	Erforderlich	Standard	Beschreibung
			mit dem Passwort-Parameter verwendet werden. Gilt nur, wenn der Benutzer und das Passwort keine Parameter in der URL sind. Wenn beide verwendet werden, tritt ein Fehler auf.
password	Nein	–	Das Redshift-Passwort. Muss mit dem Benutzer-Parameter verwendet werden. Gilt nur, wenn der Benutzer und das Passwort keine Parameter in der URL sind. Wenn beide verwendet werden, tritt ein Fehler auf.

Parameter	Erforderlich	Standard	Beschreibung
URL	Nein	–	EINE JDBC-URL. Das Format ist jdbc:subprotocol://host:port/database?user=username&password=password. „Subprotocol“ kann postgresql oder Redshift sein, je nachdem, welchen JDBC-Treiber Sie geladen haben. Beachten Sie, dass sich ein Redshift-kompatibler Treiber im Klassenpfad befinden und dieser URL entsprechen muss. „Host“ und „Port“ sollten auf den Redshift-Hauptknoten verweisen. Sie müssen also Sicherheitsgruppen und/oder VPC konfigurieren, um den Zugriff von Ihrer Treiberanwendung aus zu ermöglichen.

Parameter	Erforderlich	Standard	Beschreibung
			„Database“ ist der Name der Redshift-Datenbank. „User“ und „Password“ sind Anmeldeinformationen für den Zugriff auf die Datenbank, die in diese URL für JDBC eingebettet sein müssen, und der Datenbankbenutzer muss über die erforderlichen Berechtigungen für den Zugriff auf die Tabelle verfügen.
aws_iam_role	Nur wenn IAM-Rollen verwendet werden, um COPY/UNLOAD-Operationen in Redshift zu autorisieren	–	Vollständig spezifizierter ARN der IAM-Rolle, die dem Redshift-Cluster zugeordnet ist

Parameter	Erforderlich	Standard	Beschreibung
forward_spark_s3_credentials	Nein	Falsch	Gibt an, ob diese Bibliothek automatisch die Anmeldeinformationen erkennen soll, die Spark für die Verbindung mit Amazon S3 verwendet, und ob diese Anmeldeinformationen über den JDBC-Treiber an Redshift weitergeleitet werden sollen. Diese Anmeldeinformationen werden als Teil der JDBC-Abfrage gesendet. Daher empfehlen wir, bei Verwendung dieser Option die SSL-Verschlüsselung mit JDBC-Verbindung zu aktivieren.
temporary_aws_access_key_id	Nein	–	AWS-Zugriffsschlüssel. Muss über Schreibberechtigungen für den S3-Bucket verfügen.
temporary_aws_secret_access_key	Nein	–	Geheimer AWS-Zugriffsschlüssel, der dem Zugriffsschlüssel entspricht

Parameter	Erforderlich	Standard	Beschreibung
temporary_aws_session_token	Nein	–	AWS-Sitzungstoken, das dem bereitgestellten Zugriffsschlüssel entspricht
tempdir	Nein	–	Ein beschreibbarer Speicherort in Amazon S3. Wird zum Entladen von Daten beim Lesen und zum Laden von Avro-Daten in Redshift beim Schreiben verwendet. Wenn Sie eine Redshift-Datenquelle für Spark als Teil einer regulären ETL-Pipeline verwenden, kann es nützlich sein, eine Lebenszyklus-Richtlinie für einen Bucket festzulegen und diesen als temporären Speicherort für diese Daten zu verwenden.

Parameter	Erforderlich	Standard	Beschreibung
jdbcdriver	Nein	Wird durch das Unterprotokoll der JDBC-URL bestimmt	Der Klassenname des zu verwenden den JDBC-Treibers. Diese Klasse muss sich im Klassenpf ad befinden. In den meisten Fällen sollte die Angabe dieser Option nicht erforderlich sein, da der entsprechende Treiber-Klassennam e automatisch durch das Unterprotokoll der JDBC-URL bestimmt werden sollte.
diststyle	Nein	Even	Der Redshift-Verteilungsstil, der beim Erstellen einer Tabelle verwendet werden soll. Gültige Optionen sind EVEN, KEY oder ALL. Wenn Sie KEY verwenden , müssen Sie auch einen Verteilun gsschlüssel mit der Option distkey festlegen.

Parameter	Erforderlich	Standard	Beschreibung
distkey	Nein, es sei denn, Sie verwenden DISTSTYLE_KEY	–	Der Name einer Tabellenspalte, die beim Erstellen einer Tabelle als Verteilungsschlüssel verwendet werden soll.
sortkeyspec	Nein	–	Eine vollständige Redshift-Definition für Sortierschlüssel.
include_column_list	Nein	Falsch	Gibt an, ob diese Bibliothek die Spalten automatisch aus dem Schema extrahieren und sie gemäß den Optionen für die Zuweisung von Spalten dem Befehl COPY hinzufügen soll.

Parameter	Erforderlich	Standard	Beschreibung
description	Nein	–	Eine Beschreibung der Tabelle. Die Beschreibung wird mit dem Befehl SQL COMMENT festgelegt und in den meisten Abfragetools angezeigt. Sehen Sie sich die `description` -Metadaten an, um Beschreibungen für einzelne Spalten festzulegen.

Parameter	Erforderlich	Standard	Beschreibung
preactions	Nein	–	Eine durch Semikolons getrennte Liste von SQL-Befehlen, die vor dem Laden des COPY-Befehls ausgeführt werden müssen. Es kann nützlich sein, DELETE-Befehle oder ähnliches auszuführen, bevor neue Daten geladen werden. Wenn der Befehl %s enthält, wird der Tabellenname vor der Laufzeit formatiert (falls Sie eine Staging-Tabelle verwenden). Schlägt dieser Befehl fehl, wird er als Ausnahme behandelt. Wenn Sie eine Staging-Tabelle verwenden, werden die Änderungen rückgängig gemacht und die Backup-Tabelle wiederhergestellt, falls „preactions“ fehlschlägt.

Parameter	Erforderlich	Standard	Beschreibung
extracopyoptions	Nein	–	Eine Liste zusätzlicher Optionen, die beim Laden von Daten an den Redshift-Befehl COPY angehängt werden können (z. B. `TRUNCATECOLUMNS` oder `MAXERROR n`). Eine vollständige Liste der verfügbaren Parameter finden Sie unter Optionale Parameter. Beachten Sie Folgendes: Da diese Optionen an das Ende des Befehls `COPY` angehängt werden, können nur Optionen verwendet werden, die am Ende des Befehls Sinn ergeben. Das sollte die meisten möglichen Anwendungsfälle abdecken.

Parameter	Erforderlich	Standard	Beschreibung
sse_kms_key	Nein	–	Die AWS KMS-Schlüssel-ID, die während der Redshift-Operation UNLOAD anstelle der AWS-Standardverschlüsselung für die serverseitige Verschlüsselung in S3 verwendet werden soll. Die IAM-Rolle von Redshift muss Zugriff auf den KMS-Schlüssel haben, um damit schreiben zu können, und die IAM-Rolle von Spark muss Zugriff auf den Schlüssel für Leseoperationen haben. Das Lesen der verschlüsselten Daten erfordert keine Änderungen (AWS übernimmt dies), solange die IAM-Rolle von Spark über den richtigen Zugriff verfügt.

Parameter	Erforderlich	Standard	Beschreibung
tempformat	Nein	AVRO	Das Format, in dem temporäre Dateien in Amazon S3 gespeichert werden, wenn in Redshift geschrieben wird. Gültige Werte sind AVRO, CSV und CSV GZIP (komprimierte Größe).
csvnullstring (experimentell)	Nein	Null	Der Zeichenfolgenwert, der bei Verwendung von CSV als „tempformat“ für Nullen geschrieben werden soll. Dies sollte ein Wert sein, der in Ihren tatsächlichen Daten nicht vorkommt.

Parameter	Erforderlich	Standard	Beschreibung
autopushdown	Nein	Wahr	Gibt an, ob Prädikat- und Abfrage-P ushdown angewende t werden soll, indem die logischen Spark-Pläne für SQL-Opera tionen erfasst und analysiert werden. Die Operationen werden in eine SQL-Abfrage übersetzt und dann in Redshift ausgeführt, um die Leistung zu verbessern.

Parameter	Erforderlich	Standard	Beschreibung
autopushdown.s3_result_cache	Nein	Falsch	Speichern Sie die SQL-Abfrage im Cache, um Daten aus der Amazon-S3-Pfadzuweisung im Speicher zu entladen, sodass dieselbe Abfrage nicht erneut in derselben Spark-Sitzung ausgeführt werden muss. Wird nur unterstützt, wenn „autopushdown“ aktiviert ist. Wir empfehlen, diesen Parameter nicht zu verwenden, wenn Lese- und Schreiboperationen kombiniert werden, da zwischengespeicherte Ergebnisse möglicherweise veraltete Informationen enthalten.

Parameter	Erforderlich	Standard	Beschreibung
unload_s3_format	Nein	Parquet	Das Format, mit dem Abfrageergebnisse entladen werden sollen. Gültige Optionen sind Parquet und Text, bei dem die Abfrageergebnisse im Textformat mit Pipe-Trennzeichen entladen werden.
extraunloadoptions	Nein	–	Zusätzliche Optionen, die an den Redshift-Befehl UNLOAD angehängt werden können. Es ist nicht garantiert, dass alle Optionen funktionieren, da einige Optionen mit anderen im Connector festgelegten Optionen im Konflikt stehen könnten.
copydelay	Nein	30000	Die Verzögerung (in ms) zwischen Wiederholungsversuchen für Redshift-COPY-Operationen.

Parameter	Erforderlich	Standard	Beschreibung
copyretrycount	Nein	2	Die Anzahl der erneuten Versuche von Redshift-COPY-Operationen

Parameter	Erforderlich	Standard	Beschreibung
tempdir_region	Nein	–	Die AWS-Region, in der sich `tempdir` befindet. Die Einstellung dieser Option verbesser t die Leistung des Connectors bei Interaktionen mit `tempdir` und gibt diesen Wert während der Lese- und Schreibvorgänge des Connector automatisch als Teil der COPY- und UNLOAD-Op erationen an. Diese Einstellung wird in folgenden Situationen empfohlen: 1) Wenn der Connector außerhalb von AWS ausgeführ t wird, da die automatische Regionserkennung fehlschlägt und sich negativ auf die Leistung des Connectors auswirkt.

Parameter	Erforderlich	Standard	Beschreibung
			2) Wenn `tempdir` sich in einer anderen Region als der Redshift-Cluster befindet, da durch die Verwendung dieser Einstellung die Notwendigkeit entfällt, die Region mit dem `extracopy options` - und `extraunlo adoptions` - Parameter manuell zu versorgen. `tempdir` kann sich bei der Verwendun g nicht in einer anderen Region als der Redshift-Cluster befinden, wenn `PARQUET` als `tempformat` verwendet wird, auch wenn dabei dieser Parameter verwendet wird. 3) Wenn der Connector in einer anderen Region als `tempdir` ausgeführ t wird, da dies die Zugriffsleistung des

Parameter	Erforderlich	Standard	Beschreibung
			Connectors von `tempdir` verbessert.
secret.id	Nein	–	Der Name oder der ARN Ihres Secrets, der in AWS Secrets Manager gespeicherte ist. Sie können diesen Parameter verwenden, um automatisch Redshift-Anmeldeinformationen bereitzustellen, aber nur, wenn der Benutzer, das Passwort und die `DbUser`-Anmeldeinformationen nicht an die JDBC-URL oder als andere Optionen übergeben werden.

Parameter	Erforderlich	Standard	Beschreibung
secret.region	Nein	–	Die primäre AWS-Region, z. B. USA Ost (Nord-Virginia), in der nach dem `secret.id` -Wert gesucht werden soll. Wenn Sie diese Region nicht angeben, versucht der Connector, die Standardmäßige Kette der Anbieter von Anmeldeinformationen zu verwenden, um die Region der `secret.id` aufzulösen. In einigen Fällen, z. B. wenn Sie den Connector außerhalb eines verwenden, kann der Connector die Region nicht finden. Diese Einstellung wird in folgenden Situationen empfohlen: 1) Wenn der Connector außerhalb von AWS ausgeführt wird, da die automatische

Parameter	Erforderlich	Standard	Beschreibung
			Regionserkennung fehlschlägt und die Authentifizierung mit Redshift verhindert wird Wenn der Connector in einer anderen Region als `secret.id` ausgeführt wird, da dies die Zugriffsleistung des Connector vom Secret verbessert.
secret.vpcEndpointUrl	Nein	–	Die PrivateLink-DNS-Endpunkt-URL für AWS Secrets Manager, wenn die standardmäßige Kette für Anbieter der Anmeldeinformationen überschrieben wird.
secret.vpcEndpoint Region	Nein	–	Die PrivateLink-DNS-Endpunktregion für AWS Secrets Manager, wenn die standardmäßige Kette für Anbieter der Anmeldeinformationen überschrieben wird.

Parameter	Erforderlich	Standard	Beschreibung
jdbc.*	Nein	–	Zusätzliche Parameter, die an den zugrunde liegenden JDBC-Treiber übergeben werden, wobei der Platzhalter der Name des JDBC-Parameters ist, z. B. jdbc.ssl. Beachten Sie, dass das `jdbc.`-Präfix entfernt wird, bevor es an den JDBC-Treiber übergeben wird. Alle möglichen Optionen für den Redshift-JDBC-Treiber finden Sie unter Konfigurationsoptionen der JDBC-Treiberversion 2.1.

Parameter	Erforderlich	Standard	Beschreibung
Bezeichnung	Nein	" "	Ein Bezeichner, der in den Abfragegruppensatz aufgenommen werden soll, wenn Abfragen mit dem Connector ausgeführt werden. Darf maximal 100 Zeichen enthalten, und alle Zeichen müssen `unicodeIdentifierParts` entsprechen. Wenn Ihre Kennung mehr als 100 Zeichen enthält, wird der Überschuss entfernt. Wenn Sie eine Abfrage mit dem Connector ausführen, wird die Abfragegruppe als Zeichenfolge im JSON-Format festgelegt, z. B. `{"spark-redshift-connector":{"svc":"","ver":"5.1.0-amzn-1-spark_3.3","op":"Read","lbl":""}}`)

Parameter	Erforderlich	Standard	Beschreibung
			. Diese Option ersetzt den Wert des `lbl`-Schlüssels.

> **Note**
>
> Danksagung: Diese Dokumentation enthält Beispielcode und Sprache, die von der Apache Software Foundation entwickelt wurden und unter der Apache-2.0-Lizenz lizenziert sind.

Unterstützte Datentypen

Die folgenden Datentypen in Amazon Redshift werden im Spark-Connector unterstützt. Eine vollständige Liste der unterstützten Datentypen in Amazon Redshift finden Sie unter Datentypen. Wenn ein Datentyp nicht in der folgenden Tabelle enthalten ist, wird er im Spark-Connector nicht unterstützt.

Datentyp	Aliasnamen
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

Datentyp	Aliasnamen
DATUM	
TIMESTAMP	Zeitstempel ohne Zeitzone
TIMESTAMPTZ	Timestamp with time zone
SUPER	
TIME	Time without time zone
TIMETZ	Time with time zone
VARBYTE	VARBINARY, BINARY VARYING

Komplexe Datentypen

Sie können den Spark-Connector verwenden, um komplexe Spark-Datentypen zu lesen und zu schreiben, z. B. `ArrayType`, `MapType` und `StructType` zu und von Redshift SUPER-Datentypspalten. Wenn Sie während eines Lesevorgangs ein Schema angeben, werden in Spark die Daten in der Spalte in die entsprechenden komplexen Typen konvertiert, einschließlich aller verschachtelten Typen. Wenn darüber hinaus `autopushdown` aktiviert ist, wird die Projektion von verschachtelten Attributen, Map-Werten und Array-Indizes nach Redshift verschoben, sodass die gesamte verschachtelte Datenstruktur nicht mehr entladen werden muss, wenn nur auf einen Teil der Daten zugegriffen wird.

Wenn Sie DataFrames aus dem Connector schreiben, wird eine beliebige Spalte vom Typ `MapType` (unter Verwendung von `StringType`), `StructType` oder `ArrayType` in eine Redshift-SUPER-Datentypspalte geschrieben. Beim Schreiben dieser verschachtelten Datenstrukturen muss der `tempformat`-Parameter vom Typ `CSV`, `CSV GZIP` oder `PARQUET` sein. Die Verwendung von `AVRO` löst eine Ausnahme aus. Das Schreiben einer `MapType`-Datenstruktur, die einen anderen Schlüsseltyp als `StringType`hat, verursacht auch eine Ausnahme.

StructType

Das folgende Beispiel zeigt, wie eine Tabelle mit einem SUPER-Datentyp erstellt wird, der eine Struktur enthält

```
create table contains_super (a super);
```

Anschließend können Sie den Connector wie im folgenden Beispiel verwenden, um ein `StringType`-Feld `hello` aus der SUPER-Spalte `a` in der Tabelle mit einem Schema abzufragen.

```
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")
```

Das folgende Beispiel zeigt, wie eine Struktur in die Spalte `a` geschrieben wird.

```
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

Wenn Sie lieber `MapType` verwenden, um Ihre Daten darzustellen, dann können Sie eine `MapType`-Datenstruktur in Ihrem Schema verwenden und den Wert abrufen, der dem Schlüssel in der Map entspricht. Beachten Sie, dass alle Schlüssel in Ihrer `MapType`-Datenstruktur vom Typ Zeichenfolge und alle Werte vom gleichen Typ sein müssen, z. B. int.

Das folgende Beispiel zeigt, wie der Wert des Schlüssels `hello` in der Spalte`a` abgerufen wird.

```
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

Wenn die Spalte ein Array statt einer Struktur enthält, können Sie den Connector verwenden, um das erste Element im Array abzufragen.

```
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]")
```

Einschränkungen

Die Verwendung komplexer Datentypen mit dem Spark-Connector hat die folgenden Einschränkungen:

- Alle verschachtelten Strukturfeldnamen und Map-Schlüssel müssen in Kleinbuchstaben geschrieben werden. Wenn Sie komplexe Feldnamen mit Großbuchstaben abfragen, können Sie versuchen, das Schema wegzulassen und die `from_json`-Spark-Funktion zur lokalen Konvertierung der zurückgegebenen Zeichenfolge als Problemumgehung zu verwenden.
- Alle Map-Felder, die bei Lese- oder Schreiboperationen verwendet werden, dürfen nur `StringType`-Schlüssel haben.
- Es werden nur die Tempformat-Werte `CSV`, `CSV GZIP` und `PARQUET` für das Schreiben komplexer Typen nach Redshift unterstützt. Der Versuch `AVRO` zu verwenden, löst eine Ausnahme aus.

Konfigurieren einer Verbindung für ODBC-Treiberversion 2.x für Amazon Redshift

Für zahlreiche SQL-Client-Tools und Anwendungen von Drittanbietern können Sie eine ODBC-Verbindung verwenden, um Ihren Amazon-Redshift-Cluster zu verbinden. Wenn Ihr Client-Tool JDBC unterstützt, können Sie aufgrund der einfachen Konfiguration, die JDBC bietet, diesen Verbindungstyp anstelle von ODBC verwenden. Wenn Ihr Client-Tool JDBC jedoch nicht unterstützt, können Sie die Schritte in diesem Abschnitt befolgen, um eine ODBC-Verbindung auf Ihrem Client-Computer oder Ihrer Amazon-EC2-Instance einzurichten.

Amazon Redshift bietet 64-Bit-ODBC-Treiber für Linux- und Windows-Betriebssysteme; die 32-Bit-ODBC-Treiber werden eingestellt. Derzeit wird macOS X nicht unterstützt. Weitere Updates für die 32-Bit-ODBC-Treiber werden nicht veröffentlicht, außer für dringende Sicherheitspatches. Informationen zum Herunterladen und Installieren von ODBC-Treibern für macOS X und 32-Bit-Betriebssysteme finden Sie unter Konfigurieren einer ODBC-Verbindung.

Aktuelle Informationen zu ODBC-Treiberänderungen finden Sie im Änderungsprotokoll.

Themen

- Abrufen der ODBC-URL
- Installieren und Konfigurieren des Amazon-Redshift-ODBC-Treibers unter Microsoft Windows
- Installieren und Konfigurieren des Amazon-Redshift-ODBC-Treibers unter Linux

- Konfigurieren der Authentifizierung
- Konvertieren von Datentypen
- Konfigurieren von ODBC-Treiberoptionen
- Frühere ODBC-Treiberversionen

Abrufen der ODBC-URL

Amazon Redshift zeigt die ODBC-URL für Ihren Cluster in der Amazon-Redshift-Konsole an. Diese URL enthält die erforderlichen Informationen, um die Verbindung zwischen Ihrem Client-Computer und der Datenbank herzustellen.

Eine ODBC-URL hat folgenden Format:

```
Driver={driver}; Server=endpoint_host; Database=database_name; UID=user_name;
 PWD=password; Port=port_number
```

Die Felder des vorhergehenden Formats haben die folgenden Werte:

ODBC-URL-Feldwerte

Feld	Value (Wert)
Driver	Der Name des zu verwendenden 64-Bit-ODBC-Treibers: Amazon Redshift ODBC Driver (x64) (Amazon-Redshift-ODBC-Treiber (x64))
Server	Der Endpunkt-Host des Amazon-Redshift-Clusters.
Database	Die Datenbank, die Sie für Ihren Cluster erstellt haben.
UID	Der Benutzername eines Datenbankbenutzerkontos, das die Berechtigung für die Verbindung mit der Datenbank besitzt. Obwohl es sich bei diesem Wert um eine Berechtigung auf Datenbankebene und nicht um eine Berechtigung auf Clusterebene handelt, können Sie das Redshift-Admin-Benutzerkonto verwenden, das Sie beim Starten des Clusters eingerichtet haben.
PWD	Das Passwort für das Datenbankbenutzerkonto, um die Verbindung mit der Datenbank herzustellen.

Feld	Value (Wert)
Port	Die Portnummer, die Sie beim Starten des Clusters angegeben haben. Wenn Sie eine Firewall haben, stellen Sie sicher, dass dieser Port geöffnet ist, sodass Sie ihn verwenden können.

Im Folgenden finden Sie ein Beispiel für eine ODBC-URL:

```
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
```

Informationen darüber, wo Sie die ODBC-URL finden können, finden Sie unter Suchen Ihrer Cluster-Verbindungszeichenfolge.

Installieren und Konfigurieren des Amazon-Redshift-ODBC-Treibers unter Microsoft Windows

Systemanforderungen

Sie müssen den Amazon-Redshift-ODBC-Treiber auf Client-Computern installieren, die auf ein Amazon-Redshift-Data-Warehouse zugreifen. Für jeden Computer, auf dem Sie den Treiber installieren, gelten die folgenden Mindestanforderungen:

- Administratorrechte auf dem Computer.
- Der Computer erfüllt die folgenden Systemanforderungen:
  - Eines der folgenden Betriebssysteme:
    - Windows 10 oder 8.1.
    - Windows Server 2019, 2016 oder 2012.
  - 100 MB verfügbarer Speicherplatz.
  - Visual C++ Redistributable für Visual Studio 2015 für 64-Bit-Windows installiert. Sie können das Installationspaket unter Download von Visual C++ Redistributable für Visual Studio 2022 auf der Microsoft-Website herunterladen.

Installieren des Amazon-Redshift-ODBC-Treibers

Gehen Sie wie folgt vor, um den Amazon-Redshift-ODBC-Treiber für Windows-Betriebssysteme herunterzuladen und zu installieren. Verwenden Sie nur dann einen anderen Treiber, wenn Sie eine Drittanbieteranwendung ausführen, die für die Verwendung mit Amazon Redshift zertifiziert ist, und diese Anwendung diesen speziellen Treiber erfordert.

So laden Sie den ODBC-Treiber herunter und installieren ihn:

1. Laden Sie den folgenden Treiber herunter: 64-Bit-ODBC-Treiberversion 2.1.0.0 2.1.0.0

   Der Name für diesen Treiber lautet Amazon-Redshift ODBC Driver (x64) (Amazon-Redshift-ODBC-Treiber (x64)).

   > **Note**
   >
   > 32-Bit-ODBC-Treiber werden eingestellt. Es werden außer dringenden Sicherheitspatches keine weiteren Updates veröffentlicht. Informationen zum Herunterladen und Installieren von ODBC-Treibern für 32-Bit-Betriebssysteme finden Sie unter Installieren und Konfigurieren des Amazon-Redshift-ODBC-Treibers unter Microsoft Windows.

2. Überprüfen Sie die Amazon-Redshift-ODBC-Treiberversion 2.x-Lizenz.
3. Doppelklicken Sie auf die .msi-Datei und befolgen Sie dann die Schritte im Assistenten, um den Treiber zu installieren.

Erstellen eines System-DSN-Eintrags für eine ODBC-Verbindung

Nachdem Sie den ODBC-Treiber heruntergeladen und installiert haben, fügen Sie dem Clientcomputer oder der Amazon-EC2-Instance einen Datenquellennamen (Data Source Name, DSN) hinzu. SQL-Client-Tools können diese Datenquelle verwenden, um eine Verbindung zur Amazon-Redshift-Datenbank herzustellen.

Sie sollten anstelle eines Benutzer-DSN einen System-DSN erstellen. Einige Anwendungen laden die Daten unter Verwendung eines anderen Datenbankbenutzerkontos und sind möglicherweise nicht in der Lage, Benutzer-DSNs zu erkennen, die unter einem anderen Datenbankbenutzerkonto erstellt wurden.

> **Note**
>
> Für die Authentifizierung mit AWS Identity and Access Management (IAM-) Anmeldeinformationen oder Identitätsanbietern (IdP) sind zusätzliche Schritte erforderlich. Weitere Informationen finden Sie unter Konfigurieren einer JDBC- oder ODBC-Verbindung zur Verwendung von IAM-Anmeldeinformationen.

So erstellen Sie einen System-DSN-Eintrag für eine ODBC-Verbindung:

1. Geben Sie im Start-Menü „ODBC-Datenquellen“ ein. Wählen Sie ODBC Data Sources (ODBC-Datenquellen).

   Stellen Sie sicher, dass Sie einen ODBC-Datenquellenadministrator mit derselben Bitness wie die Clientanwendung auswählen, über die Sie die Verbindung mit Amazon Redshift herstellen.
2. Wählen Sie im ODBC Data Source Administrator (ODBC-Datenquellen-Administrator) die Registerkarte Driver (Treiber) und suchen Sie den folgenden Treiberordner: Amazon Redshift ODBC Driver (x64) (Amazon-Redshift-ODBC-Treiber (x64)).
3. Wählen Sie die Registerkarte System-DSN aus, um den Treiber für alle Benutzer auf dem Computer zu konfigurieren, oder die Registerkarte Benutzer-DSN, um den Treiber nur für Ihr Datenbankbenutzerkonto zu konfigurieren.
4. Wählen Sie Add (Hinzufügen) aus. Das Fenster Create New Data Source (Neue Datenquelle erstellen) wird geöffnet.
5. Wählen Sie den Amazon Redshift ODBC driver (x64) (Amazon-Redshift-ODBC-Treiber (x64)) und wählen Sie dann Finish (Fertigstellen). Das Fenster Amazon Redshift ODBC Driver DSN Setup (DSN-Einrichtung des Amazon-Redshift-ODBC-Treibers) wird geöffnet.
6. Geben Sie im Abschnitt Connection Settings (Verbindungseinstellungen) die folgenden Informationen ein:

   Datenquellenname

   Geben Sie einen Namen für die Datenquelle ein. Wenn Sie beispielsweise den Anweisungen unter Erste Schritte mit Amazon Redshift gefolgt sind, können Sie `exampleclusterdsn` eingeben, um sich den Cluster leichter zu merken, den Sie mit diesem DSN verknüpfen.

   Server

Geben Sie den Endpunkt-Host für Ihren Amazon-Redshift-Cluster an. Sie finden diese Informationen in der Amazon-Redshift-Konsole auf der Seite mit den Cluster-Details. Weitere Informationen finden Sie unter Konfigurieren von Verbindungen in Amazon Redshift.

Port

Geben Sie die Portnummer ein, die von der Datenbank verwendet wird. Erlauben Sie den Zugriff auf den ausgewählten Port, je nachdem, welchen Port Sie beim Erstellen, Ändern oder Migrieren des Clusters ausgewählt haben.

Datenbank

Geben Sie den Namen der Amazon-Redshift-Datenbank ein. Wenn Sie den Cluster gestartet haben, ohne einen Datenbanknamen anzugeben, geben Sie ein `dev`. Verwenden Sie andernfalls den Namen, den Sie während des Startvorgangs ausgewählt haben. Wenn Sie den Anweisungen unter Erste Schritte mit Amazon Redshift gefolgt sind, geben Sie `dev` ein.

7. Geben Sie im Abschnitt Authentication (Authentifizierung) die Konfigurationsoptionen zum Konfigurieren der Standard- oder IAM-Authentifizierung an.
8. Wählen Sie SSL Options (SSL-Optionen) und geben Sie einen Wert für Folgendes an:

   Authentifizierungsmodus

   Wählen Sie einen Modus für den Umgang mit Secure Sockets Layer (SSL) aus. In einer Testumgebung können Sie verwenden `prefer`. Für Produktionsumgebungen und dann, wenn ein sicherer Datenaustausch erforderlich ist, verwenden Sie jedoch `verify-ca` oder `verify-full`.
9. Geben Sie auf der Registerkarte Proxy eine beliebige Proxy-Verbindungseinstellung an.
10. Geben Sie auf der Registerkarte Cursor Optionen an, wie Abfrageergebnisse an Ihr SQL-Client-Tool oder Ihre Anwendung zurückgegeben werden.
11. Geben Sie unter Erweiterte Optionen Werte für `logLevel`, `logPathcompression`, und andere Optionen an.
12. Wählen Sie Test aus. Wenn der Client-Computer eine Verbindung zur Amazon-Redshift-Datenbank herstellen kann, wird die folgende Meldung angezeigt: Connection successful (Verbindung erfolgreich). Wenn der Client-Computer keine Verbindung zur Datenbank herstellen kann, können Sie mögliche Probleme beheben, indem Sie eine Protokolldatei erstellen und sich an den AWS Support wenden. Informationen zum Generieren von Protokollen finden Sie unter (LINK).
13. Wählen Sie OK aus.

Installieren und Konfigurieren des Amazon-Redshift-ODBC-Treibers unter Linux

Systemanforderungen

Sie müssen den Amazon-Redshift-ODBC-Treiber auf Client-Computern installieren, die auf ein Amazon-Redshift-Data-Warehouse zugreifen. Für jeden Computer, auf dem Sie den Treiber installieren, gelten die folgenden Mindestanforderungen:

- Root-Zugriff auf den Computer.
- Eine der folgenden Verteilungen:
  - Red Hat® Enterprise Linux® (RHEL) 8 oder höher
  - CentOS 8 oder höher.
- 150 MB verfügbarer Speicherplatz.
- unixODBC 2.2.14 oder höher.
- glibc 2.26 oder höher.

Installieren des Amazon-Redshift-ODBC-Treibers

So laden Sie die Amazon-Redshift-ODBC-Treiberversion 2.x für Linux herunter und installieren sie:

1. Laden Sie den folgenden Treiber herunter: 64-Bit-RPM-Treiberversion 2.1.0.0 2.1.0.0

   > **Note**
   >
   > 32-Bit-ODBC-Treiber werden eingestellt. Es werden außer dringenden Sicherheitspatches keine weiteren Updates veröffentlicht.

2. Navigieren Sie zu dem Verzeichnis, in das Sie das Paket heruntergeladen haben, und führen Sie einen der folgenden Befehle aus. Verwenden Sie den Befehl, der Ihrer Linux-Distribution entspricht.

   Führen Sie auf RHEL- und CentOS-Betriebssystemen den folgenden Befehl aus:

   ```
   yum --nogpgcheck localinstall RPMFileName
   ```

   Ersetzen Sie `RPMFileName` durch den Dateinamen des RPM-Pakets. Im folgenden Beispiel wird beispielsweise die Installation des 64-Bit-Treibers gezeigt:

```
yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-2.x.xx.xxxx.x86_64.rpm
```

Verwenden eines ODBC-Treibermanagers zum Konfigurieren des ODBC-Treibers unter Linux

Unter Linux verwenden Sie einen ODBC-Treibermanager, um die ODBC-Verbindungseinstellungen zu konfigurieren. ODBC-Treibermanager verwenden Konfigurationsdateien, um ODBC-Datenquellen und -Treiber zu definieren und zu konfigurieren. Der ODBC-Treibermanager, den Sie verwenden, ist vom verwendeten Betriebssystem abhängig.

Konfigurieren des ODBC-Treibers mit dem unixODBC-Treibermanager

Die folgenden Dateien sind erforderlich, um den Amazon-Redshift-ODBC-Treiber zu konfigurieren:

- `amazon.redshiftodbc.ini`
- `odbc.ini`
- `odbcinst.ini`

Wenn Sie am Standardspeicherort installiert haben, befindet sich die `amazon.redshiftodbc.ini`-Konfigurationsdatei in `/opt/amazon/redshiftodbcx64`.

Außerdem finden Sie unter `/opt/amazon/redshiftodbcx64` die Beispieldateien `odbc.ini` und `odbcinst.ini`. Sie können diese Dateien als Beispiele für die Konfiguration des Amazon-Redshift-ODBC-Treibers und des Datenquellennamens (DSN) verwenden.

Die Verwendung des Installationsverzeichnisses für den Amazon-Redshift-ODBC-Treiber für die Konfigurationsdateien wird nicht empfohlen. Die Beispieldateien im installierten Verzeichnis dienen nur Beispielzwecken. Wenn Sie den Amazon-Redshift-ODBC-Treiber zu einem späteren Zeitpunkt neu installieren oder auf eine neuere Version aktualisieren, wird das Installationsverzeichnis überschrieben. Sie verlieren alle Änderungen, die Sie möglicherweise an Dateien im Installationsverzeichnis vorgenommen haben.

Um dies zu vermeiden, kopieren Sie die `amazon.redshiftodbc.ini`-Datei in ein anderes Verzeichnis als das Installationsverzeichnis. Wenn Sie diese Datei in das Stammverzeichnis des Benutzers kopieren, fügen Sie am Anfang der Datei einen Punkt (.) hinzu, um die Datei zu verbergen.

Verwenden Sie für die `odbc.ini`- und `odbcinst.ini`-Dateien entweder die Konfigurationsdateien im Basisverzeichnis des Benutzers, oder erstellen Sie neue Versionen in einem anderen Verzeichnis. Standardmäßig sollte Ihr Linux-Betriebssystem eine `odbc.ini`-Datei und eine `odbcinst.ini`-Datei im Home-Verzeichnis des Benutzers haben (`/home/$USER` oder `~/.`). Bei diesen Standarddateien handelt es sich um versteckte Dateien, die durch den Punkt (.) vor jedem Dateinamen angezeigt werden. Diese Dateien werden nur angezeigt, wenn Sie das `-a`-Flag zum Auflisten des Verzeichnisinhalts verwenden.

Unabhängig davon, welche Option Sie für die `odbc.ini`- und `odbcinst.ini`-Dateien wählen, ändern Sie die Dateien, um Treiber- und DSN-Konfigurationsinformationen hinzuzufügen. Wenn Sie neue Dateien erstellen, müssen Sie auch Umgebungsvariablen festlegen, um anzugeben, wo diese Konfigurationsdateien gespeichert sind.

Standardmäßig sind ODBC-Treibermanager so konfiguriert, dass sie versteckte Versionen der `odbc.ini`- und `odbcinst.ini`-Konfigurationsdateien (mit den Namen `.odbc.ini` und `.odbcinst.ini`) verwenden, die sich im Home-Verzeichnis befinden. Sie sind auch so konfiguriert, dass sie die `amazon.redshiftodbc.ini`-Datei im Installationsverzeichnis des Treibers verwenden. Wenn Sie diese Konfigurationsdateien an anderer Stelle speichern, legen Sie die folgenden Umgebungsvariablen fest, damit der Treibermanager die Dateien finden kann.

Wenn Sie unixODBC verwenden, gehen Sie wie folgt vor:

- Legen Sie `ODBCINI` auf den vollständigen Pfad und Dateinamen der `odbc.ini`-Datei fest.
- Legen Sie `ODBCSYSINI` auf den vollständigen Pfad des Verzeichnisses fest, das die `odbcinst.ini`-Datei enthält.
- Legen Sie `AMAZONREDSHIFTODBCINI` auf den vollständigen Pfad und Dateinamen der `amazon.redshiftodbc.ini`-Datei fest.

Im Folgenden finden Sie ein Beispiel für die Einstellung der obigen Werte:

```
export ODBCINI=/usr/local/odbc/odbc.ini
export ODBCSYSINI=/usr/local/odbc
export AMAZONREDSHIFTODBCINI=/etc/amazon.redshiftodbc.ini
```

Konfigurieren einer Verbindung mit einem Datenquellennamen (DSN) unter Linux

Wenn Sie eine Verbindung zu Ihrem Datenspeicher über einen Datenquellennamen (DSN) herstellen, konfigurieren Sie die `odbc.ini`-Datei, um Datenquellennamen (DSNs) zu definieren.

Legen Sie die Eigenschaften in der `odbc.ini`-Datei fest, um einen DSN zu erstellen, der die Verbindungsinformationen für den Datenspeicher angibt.

Verwenden Sie auf Linux-Betriebssystemen das folgende Format:

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file
Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

Das folgende Beispiel zeigt die Konfiguration für `odbc.ini` mit dem 64-Bit-ODBC-Treiber auf Linux-Betriebssystemen.

```
[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
```

Konfigurieren einer Verbindung ohne DSN unter Linux

Um eine Verbindung mit dem Datenspeicher über eine Verbindung herzustellen, die nicht über einen DSN verfügt, definieren Sie den Treiber in der `odbcinst.ini`-Datei. Geben Sie dann eine DSN-lose Verbindungszeichenfolge in Ihrer Anwendung an.

Verwenden Sie auf Linux-Betriebssystemen das folgende Format:

```
[ODBC Drivers]
```

```
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

Das folgende Beispiel zeigt die Konfiguration für `odbcinst.ini` mit dem 64-Bit-ODBC-Treiber auf Linux-Betriebssystemen.

```
[ODBC Drivers]
Amazon Redshift ODBC Driver (x64)=Installed

[Amazon Redshift ODBC Driver (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.so
```

Konfigurieren der Authentifizierung

Um Daten vor unbefugtem Zugriff zu schützen, erfordern Amazon-Redshift-Datenspeicher, dass alle Verbindungen mit Benutzeranmeldeinformationen authentifiziert werden.

Die folgende Tabelle veranschaulicht die erforderlichen und optionalen Verbindungsoptionen für jede Authentifizierungsmethode, die verwendet werden kann, um eine Verbindung mit der Amazon-Redshift-ODBC-Treiberversion 2.x herzustellen:

Erforderliche ODBC-Authentifizierungsmethode und optionale Verbindungsoptionen

Authentifizierungsmethode	Erforderlich	Optional
Standard	• Host • Port • Datenbank • Benutzerkennung (UID) • Passwort	

Authentifizierungsmethode	Erforderlich	Optional
IAM-Profil	• Host • Port • Datenbank • IAM • Profil	• ClusterID • Region • AutoCreate • EndpointURL • StsEndpointURL • InstanceProfile **Note** ClusterID (Cluster-ID) und Region müssen in Host festgelegt werden, wenn sie nicht separat festgelegt werden.

Authentifizierungsmethode	Erforderlich	Optional
IAM-Anmeldeinformationen	• Host • Port • Datenbank • IAM • AccessKeyID • SecretAccessKey	• ClusterID • Region • AutoCreate • EndpointURL • StsEndpointURL • SessionToken • Benutzerkennung (UID) **Note** ClusterID (Cluster-ID) und Region müssen in Host festgelegt werden, wenn sie nicht separat festgelegt werden.

Authentifizierungsmethode	Erforderlich	Optional
AD FS	• Host • Port • Datenbank • IAM • plugin_name • Benutzerkennung (UID) • Passwort • IdP_Host • IdP_Port	• ClusterID • Region • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • loginToRp • SSL_Insecure **Note** ClusterID (Cluster-ID) und Region müssen in Host festgelegt werden, wenn sie nicht separat festgelegt werden.

Authentifizierungsmethode	Erforderlich	Optional
Azure AD	• Host • Port • Datenbank • IAM • plugin_name • Benutzerkennung (UID) • Passwort • IdP_Tenant • Client_ID • Client_Secret	• ClusterID • Region • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter **Note** ClusterID (Cluster-ID) und Region müssen in Host festgelegt werden, wenn sie nicht separat festgelegt werden.
JWT	• Host • Port • Datenbank • IAM • plugin_name • web_identity_token	• provider_name

Authentifizierungsmethode	Erforderlich	Optional
Okta	• Host • Port • Datenbank • IAM • plugin_name • Benutzerkennung (UID) • Passwort • IdP_Host • App_Name • App_ID	• ClusterID • Region • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role **Note** ClusterID (Cluster-ID) und Region müssen in Host festgelegt werden, wenn sie nicht separat festgelegt werden.

Authentifizierungsmethode	Erforderlich	Optional
Ping Federate	• Host • Port • Datenbank • IAM • plugin_name • Benutzerkennung (UID) • Passwort • IdP_Host • IdP_Port	• ClusterID • Region • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • SSL_Insecure • partner_spid **Note** ClusterID (Cluster-ID) und Region müssen in Host festgelegt werden, wenn sie nicht separat festgelegt werden.

Authentifizierungsmethode	Erforderlich	Optional
Azure AD Browser	• Host • Port • Datenbank • IAM • plugin_name • IdP_Tenant • Client_ID • Benutzerkennung (UID)	• ClusterID • Region • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter • IdP_Response_Timeout • listen_port **Note** ClusterID (Cluster-ID) und Region müssen in Host festgelegt werden, wenn sie nicht separat festgelegt werden.

Authentifizierungsmethode	Erforderlich	Optional
SAML Browser	• Host • Port • Datenbank • IAM • plugin_name • login_url • Benutzerkennung (UID)	• ClusterID • Region • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter • IdP_Response_Timeout • listen_port **Note** ClusterID (Cluster-ID) und Region müssen in Host festgelegt werden, wenn sie nicht separat festgelegt werden.
Auth-Profil	• Host • Port • Datenbank • AccessKeyID • SecretAccessKey	

Authentifizierungsmethode	Erforderlich	Optional
Azure AD OAUTH2 Browser	• Host • Port • Datenbank • IAM • plugin_name • IdP_Tenant • Client_ID • Benutzerkennung (UID)	• ClusterID • Region • EndpointUrl • IdP_Response_Timeout • listen_port • scope • provider_name **Note** ClusterID (Cluster-ID) und Region müssen in Host festgelegt werden, wenn sie nicht separat festgelegt werden.

Verwenden eines Services für externe Anmeldeinformationen

Neben der integrierten Unterstützung für AD FS, Azure AD und Okta bietet die Windows-Version des Amazon-Redshift-ODBC-Treibers auch Unterstützung für andere Anmeldeinformationen-Services. Der Treiber kann Verbindungen mit jedem SAML-basierten Anmeldeinformationsanbieter-Plugin Ihrer Wahl authentifizieren.

So konfigurieren Sie einen Service für externe Anmeldeinformationen unter Windows:

1. Erstellen Sie ein IAM-Profil, das das Plug-in des Anmeldeinformationsanbieters und andere Authentifizierungsparameter nach Bedarf angibt. Das Profil muss ASCII-kodiert sein und das folgende Schlüssel-Wert-Paar enthalten, wobei `PluginPath` der vollständige Pfad zur Plugin-Anwendung ist:

```
plugin_name = PluginPath
```

Zum Beispiel:

```
plugin_name = C:\Users\kjson\myapp\CredServiceApp.exe
```

Informationen zum Erstellen eines Profils finden Sie unter Verwenden eines Konfigurationsprofils im Verwaltungshandbuch zum Amazon-Redshift-Cluster.

2. Konfigurieren Sie den Treiber für die Verwendung dieses Profils. Der Treiber erkennt und verwendet die im Profil angegebenen Authentifizierungseinstellungen.

Konvertieren von Datentypen

Die Amazon-Redshift-ODBC-Treiberversion 2.x unterstützt viele gängige Datenformate und konvertiert zwischen Amazon-Redshift- und SQL-Datentypen.

In der folgenden Tabelle sind die unterstützten Datentyp-Mappings aufgeführt.

Amazon-Redshift-Typ	SQL-Typ
BIGINT	SQL_BIGINT
BOOLEAN	SQL_BIT
CHAR	SQL_CHAR
DATUM	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

Amazon-Redshift-Typ	SQL-Typ
SUPER	SQL_LONGVARCHAR
TEXT	SQL_LONGVARCHAR
TIME	SQL_TYPE_TIME
TIMETZ	SQL_TYPE_TIME
TIMESTAMP (ZEITSTEMPEL)	SQL_TYPE_ TIMESTAMP
TIMESTAMPTZ	SQL_TYPE_ TIMESTAMP
VARBYTE	SQL_LONGVARBINARY
VARCHAR	SQL_VARCHAR

Konfigurieren von ODBC-Treiberoptionen

Sie können Treiberkonfigurationsoptionen verwenden, um das Verhalten des Amazon-Redshift-ODBC-Treibers zu steuern. Bei den Treiberoptionen wird die Groß-/Kleinschreibung nicht beachtet.

Unter Microsoft Windows legen Sie die Treiberoptionen in der Regel fest, wenn Sie einen Datenquellennamen (Data Source Name, DSN) konfigurieren. Sie können auch Treiberoptionen in der Verbindungszeichenfolge einstellen, wenn Sie eine programmgesteuerte Verbindung herstellen oder Registrierungsschlüssel in hinzufügen oder ändern `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\`*`your_DSN`*. Weitere Informationen zur Konfiguration eines DSN finden Sie unter Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows.

Unter Linux legen Sie Treiberkonfigurationsoptionen in Ihren `odbc.ini`- und `amazon.redshiftodbc.ini`-Dateien fest, wie in Verwenden Sie einen ODBC-Treibermanager, um den Treiber unter Linux und macOS X zu konfigurieren beschrieben. In einer `amazon.redshiftodbc.ini`-Datei eingestellte Konfigurationsoptionen gelten für alle Verbindungen. Konfigurationsoptionen, die in einer `odbc.ini`-Datei festgelegt wurden, gelten hingegen jeweils nur für eine bestimmte Verbindung. In `odbc.ini` eingestellte Konfigurationsoptionen haben Vorrang vor Konfigurationsoptionen, die in `amazon.redshiftodbc.ini` festgelegt sind.

Im Folgenden finden Sie Beschreibungen für die Optionen, die Sie für den Amazon-Redshift-ODBC-Treiber der Version 2.x angeben können:

AccessKeyAUSWEIS

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der IAM-Zugriffsschlüssel für den Benutzer oder die Rolle. Wenn Sie diesen Parameter festlegen, müssen Sie auch angeben SecretAccessKey.

Dieser Parameter ist optional.

app_id

- Standardwert – None
- Datentyp – Zeichenfolge

Die von Okta bereitgestellte eindeutige ID, die mit Ihrer Amazon-Redshift-Anwendung verknüpft ist.

Dieser Parameter ist optional.

app_name

- Standardwert – None
- Datentyp – Zeichenfolge

Der Name der Okta-Anwendung, mit der Sie die Verbindung zu Amazon Redshift authentifizieren.

Dieser Parameter ist optional.

AuthProfile

- Standardwert – None
- Datentyp – Zeichenfolge

Das zum Verwalten der Verbindungseinstellungen verwendete Authentifizierungsprofil. Wenn Sie diesen Parameter festlegen, müssen Sie auch AccessKeyID und festlegen SecretAccessKey.

Dieser Parameter ist optional.

AuthType

- Standardwert – Standard
- Datentyp – Zeichenfolge

Diese Option gibt den Authentifizierungsmodus an, den der Treiber verwendet, wenn Sie einen DSN mithilfe des Dialogfelds DSN-Einrichtung des Amazon-Redshift-ODBC-Treibers konfigurieren:

- Standard: Standardauthentifizierung mit Ihrem Amazon-Redshift-Benutzernamen und -Passwort.
- AWS Profil: IAM-Authentifizierung mithilfe eines Profils.
- AWS IAM-Anmeldeinformationen: IAM-Authentifizierung mit IAM-Anmeldeinformationen.
- Identitätsanbieter: AD FS: IAM-Authentifizierung mithilfe von Active-Directory-Federation-Services (AD FS).
- Identity Provider: Auth Plugin: Ein Autorisierungs-Plugin, das ein Identity Center (IdC) -Token oder OpenID Connect (OIDC) JSON-basierte Identitätstoken (JWT) von jedem mit dem IdC verknüpften Web-Identitätsanbieter akzeptiert.
- Identitätsanbieter: Azure AD: IAM-Authentifizierung mithilfe eines Azure-AD-Portals.
- Identitätsanbieter: JWT: IAM-Authentifizierung mithilfe eines JSON-Web-Tokens (JWT).
- Identitätsanbieter: Okta: IAM-Authentifizierung mithilfe von Okta.
- Identitätsanbieter: PingFederate IAM-Authentifizierung mithilfe von. PingFederate

Diese Option ist nur verfügbar, wenn Sie einen DSN über das Dialogfeld DSN-Einrichtung des Amazon-Redshift-ODBC-Treibers im Windows-Treiber konfigurieren. Wenn Sie eine Verbindung mithilfe einer Verbindungszeichenfolge oder auf einem Nicht-Windows-Computer konfigurieren, bestimmt der Treiber anhand Ihrer angegebenen Anmeldeinformationen automatisch, ob die Standard-, AWS Profil- oder AWS IAM-Authentifizierung verwendet werden soll. Um einen Identitätsanbieter zu verwenden, müssen Sie die Eigenschaft plugin_name (Plugin_Name) festlegen.

Dieser Parameter muss angegeben werden.

AutoCreate

- Standardwert – 0
- Datentyp – boolesch

Ein boolescher Wert, der angibt, ob der Treiber einen neuen Benutzer erstellt, wenn der angegebene Benutzer nicht existiert.

- 1 | TRUE: Wenn der durch die UID angegebene Benutzer nicht existiert, erstellt der Treiber einen neuen Benutzer.
- 0 | FALSE: Der Treiber erstellt keinen neuen Benutzer. Wenn der angegebene Benutzer nicht existiert, schlägt die Authentifizierung fehl.

Dieser Parameter ist optional.

CaFile

- Standardwert – None
- Datentyp – Zeichenfolge

Der Dateipfad zur CA-Zertifikatsdatei, die für einige Formen der IAM-Authentifizierung verwendet wird.

Dieser Parameter ist nur unter Linux verfügbar.

Dieser Parameter ist optional.

Client-ID

- Standardwert – None
- Datentyp – Zeichenfolge

Die Client-ID, die Ihrer Amazon-Redshift-Anwendung in Azure AD zugeordnet ist.

Dieser Parameter ist erforderlich, wenn die Authentifizierung über den Azure-AD-Service erfolgt.

client_ secret

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der geheime Schlüssel, der Ihrer Amazon-Redshift-Anwendung in Azure AD zugeordnet ist.

Dieser Parameter ist erforderlich, wenn die Authentifizierung über den Azure-AD-Service erfolgt.

ClusterId

- Standardwert – None
- Datentyp – Zeichenfolge

Der Name des Amazon-Redshift-Clusters, zu dem Sie eine Verbindung herstellen möchten. Es wird bei der IAM-Authentifizierung verwendet. Die Cluster-ID ist im Parameter-Server nicht angegeben.

Dieser Parameter ist optional.

Kompression

- Standardwert — aus
- Datentyp – Zeichenfolge

Die Komprimierungsmethode, die für die Wire-Protokollkommunikation zwischen dem Amazon-Redshift-Server und dem Client oder Treiber verwendet wird.

Sie können die folgenden Werte angeben:

- lz4: Legt die für die Wire-Protokoll-Kommunikation mit Amazon Redshift verwendete Komprimierungsmethode auf fest. `lz4`
- zstd: Legt die für die Wire-Protokoll-Kommunikation mit Amazon Redshift verwendete Komprimierungsmethode auf fest. `zstd`
- aus: Verwendet keine Komprimierung für die Wire-Protokoll-Kommunikation mit Amazon Redshift.

Dieser Parameter ist optional.

Datenbank

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Name der Amazon-Redshift-Datenbank, auf die Sie zugreifen möchten.

Dieser Parameter muss angegeben werden.

DatabaseMetadataCurrentDbOnly

- Standardwert – 1
- Datentyp – boolesch

Ein boolescher Wert, der angibt, ob der Treiber Metadaten aus mehreren Datenbanken und Clustern zurückgibt.

- 1 | TRUE: Der Treiber gibt nur Metadaten aus der aktuellen Datenbank zurück.
- 0 | FALSE. Der Treiber gibt Metadaten über mehrere Amazon-Redshift-Datenbanken und -Cluster zurück.

Dieser Parameter ist optional.

dbgroups_filter

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der reguläre Ausdruck, den Sie angeben können DbGroups , um diejenigen herauszufiltern, die von der SAML-Antwort an Amazon Redshift empfangen werden, wenn Sie die Authentifizierungstypen Azure, Browser Azure und Browser SAML verwenden.

Dieser Parameter ist optional.

Treiber

- Standardwert – Amazon-Redshift-ODBC-Treiber (x64)
- Datentyp – Zeichenfolge

Der Name des Treibers. Der einzige unterstützte Wert ist Amazon Redshift ODBC Driver (x64) (Amazon-Redshift-ODBC-Treiber (x64)).

Dieser Parameter ist erforderlich, wenn Sie DSN nicht festlegen.

DSN

- Standardwert – Kein

- Datentyp – Zeichenfolge

Der Name der Treiber-Datenquelle. Die Anwendung spezifiziert den DSN in der SQL-API. DriverConnect

Dieser Parameter ist erforderlich, wenn Sie den Driver (Treiber) nicht festlegen.

EndpointUrl

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der übergeordnete Endpunkt, der für die Kommunikation mit dem Amazon-Redshift-Coral-Service für die IAM-Authentifizierung verwendet wird.

Dieser Parameter ist optional.

ForceLowercase

- Standardwert – 0
- Datentyp – boolesch

Ein boolescher Wert, der angibt, ob der Treiber bei Verwendung der Single Sign-On-Authentifizierung alle vom Identitätsanbieter an Amazon Redshift in Kleinbuchstaben DbGroups gesendet wird.

- 1 | TRUE: Der Treiber schreibt alles, was vom Identitätsanbieter gesendet wird DbGroups , in Kleinbuchstaben.
- 0 | FALSE: Der Treiber ändert DbGroups sich nicht.

Dieser Parameter ist optional.

group_federation

- Standardwert – 0
- Datentyp – boolesch

Ein boolescher Wert, der angibt, ob die `getClusterCredentialsWithIAM` API zum Abrufen temporärer Clusteranmeldeinformationen in bereitgestellten Clustern verwendet wird. Mit dieser

Option können IAM-Benutzer Redshift-Datenbankrollen in bereitgestellten Clustern integrieren. Beachten Sie, dass diese Option nicht für Redshift Serverless-Namespaces gilt.

- 1 | TRUE: Der Treiber verwendet die `getClusterCredentialsWithIAM` API, um temporäre Cluster-Anmeldeinformationen in bereitgestellten Clustern abzurufen.
- 0 | FALSE: Der Treiber verwendet die `getClusterCredentials` Standard-API zum Abrufen temporärer Clusteranmeldeinformationen in bereitgestellten Clustern.

Dieser Parameter ist optional.

https_proxy_host

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Hostname oder die IP-Adresse des Proxy-Servers, über den Sie IAM-Authentifizierungsprozesse leiten möchten.

Dieser Parameter ist optional.

https_proxy_password

- Standardwert – Kein
- Datentyp – Zeichenfolge

Das Passwort, mit dem Sie auf den Proxy-Server zugreifen. Es wird für die IAM-Authentifizierung verwendet.

Dieser Parameter ist optional.

https_proxy_port

- Standardwert – Kein
- Datentyp – Ganzzahl

Die Nummer des Ports, den der Proxy-Server verwendet, um auf Client-Verbindungen zu warten. Es wird für die IAM-Authentifizierung verwendet.

Dieser Parameter ist optional.

https_proxy_username

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Benutzername, den Sie für den Zugriff auf den Proxy-Server verwenden. Es wird für die IAM-Authentifizierung verwendet.

Dieser Parameter ist optional.

IAM

- Standardwert – 0
- Datentyp – boolesch

Ein boolescher Wert, der angibt, ob der Treiber eine IAM-Authentifizierungsmethode verwendet, um die Verbindung zu authentifizieren.

- 1 | TRUE: Der Treiber verwendet eine der IAM-Authentifizierungsmethoden (unter Verwendung eines Zugriffsschlüssels und eines geheimen Schlüsselpaars oder eines Profils oder eines Anmeldeinformationen-Services).
- 0 | FALSE. Der Treiber verwendet die Standardauthentifizierung (unter Verwendung Ihres Datenbankbenutzernamens und Passworts).

Dieser Parameter ist optional.

identity_namespace

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Identitäts-Namespace, der bei der Authentifizierung verwendet werden soll. IdpTokenAuthPlugin Er hilft Redshift, zu bestimmen, welche IAM-Identity-Center-Instance verwendet werden soll.

Wenn nur eine IAM-Identity-Center-Instance vorhanden ist oder der standardmäßige Identitäts-Namespace festgelegt ist, ist dieser Parameter optional, andernfalls ist er erforderlich.

idp_host

- Standardwert – None
- Datentyp – Zeichenfolge

Der IdP-Host (Identitätsanbieter), den Sie zur Authentifizierung bei Amazon Redshift verwenden.

Dieser Parameter ist optional.

idp_port

- Standardwert – None
- Datentyp – Ganzzahl

Der IdP-Port (Identitätsanbieter), den Sie zur Authentifizierung bei Amazon Redshift verwenden. Erlauben Sie den Zugriff auf den ausgewählten Port, je nachdem, welchen Port Sie beim Erstellen, Ändern oder Migrieren des Clusters ausgewählt haben.

Dieser Parameter ist optional.

idp_response_timeout

- Standardwert – 120
- Datentyp – Ganzzahl

Die Anzahl der Sekunden, die der Treiber auf die SAML-Antwort vom Identitätsanbieter wartet, wenn SAML- oder Azure-AD-Services über ein Browser-Plugin verwendet werden.

Dieser Parameter ist optional.

idp_tenant

- Standardwert – None
- Datentyp – Zeichenfolge

Die Azure-AD-Mandanten-ID, die mit Ihrer Amazon-Redshift-Anwendung verbunden ist.

Dieser Parameter ist erforderlich, wenn die Authentifizierung über den Azure-AD-Service erfolgt.

idp_use_https_proxy

- Standardwert – 0
- Datentyp – boolesch

Ein boolescher Wert, der angibt, ob der Treiber die Authentifizierungsprozesse für Identitätsanbieter (IdP) über einen Proxy-Server weiterleitet.

- 1 | TRUE: Der Treiber leitet IdP-Authentifizierungsprozesse über einen Proxy-Server weiter.
- 0 | FALSE. Der Treiber leitet IdP-Authentifizierungsprozesse nicht über einen Proxy-Server weiter.

Dieser Parameter ist optional.

InstanceProfile

- Standardwert – 0
- Datentyp – boolesch

Ein boolescher Wert, der angibt, ob der Treiber das Amazon-EC2-Instance-Profil verwendet, wenn er für die Verwendung eines Profils zur Authentifizierung konfiguriert ist.

- 1 | TRUE: Der Treiber verwendet das Amazon-EC2-Instance-Profil.
- 0 | FALSE. Der Treiber verwendet stattdessen das verkettete Rollenprofil, das durch die Option Profilname (Profile (Profil)) angegeben wird.

Dieser Parameter ist optional.

KeepAlive

- Standardwert – 1
- Datentyp – boolesch

Ein boolescher Wert, der angibt, ob der Treiber TCP-Keepalives verwendet, um ein Timeout von Verbindungen zu verhindern.

- 1 | TRUE: Der Treiber verwendet TCP-Keepalives, um ein Timeout von Verbindungen zu verhindern.

- 0 | FALSE. Der Treiber verwendet keine TCP-Keepalives.

Dieser Parameter ist optional.

KeepAliveCount

- Standardwert – 0
- Datentyp – Ganzzahl

Die Anzahl der TCP-Keepalive-Pakete, die verloren gehen dürfen, bevor die Verbindung als abgebrochen betrachtet wird. Wenn dieser Parameter auf 0 gesetzt ist, verwendet der Treiber die Systemvorgabe für diese Einstellung.

Dieser Parameter ist optional.

KeepAliveInterval

- Standardwert – 0
- Datentyp – Ganzzahl

Die Anzahl der Sekunden zwischen den einzelnen TCP-Keepalive-Übertragungen. Wenn dieser Parameter auf 0 gesetzt ist, verwendet der Treiber die Systemvorgabe für diese Einstellung.

Dieser Parameter ist optional.

KeepAliveTime

- Standardwert – 0
- Datentyp – Ganzzahl

Die Anzahl der Inaktivitätsekunden, bevor der Treiber ein TCP-Keepalive-Paket sendet. Wenn dieser Parameter auf 0 gesetzt ist, verwendet der Treiber die Systemvorgabe für diese Einstellung.

Dieser Parameter ist optional.

listen_port

- Standardwert – 7 890
- Datentyp – Ganzzahl

Der Port, den der Treiber verwendet, um die SAML-Antwort vom Identitätsanbieter zu empfangen, wenn SAML- oder Azure-AD-Services über ein Browser-Plugin verwendet werden..

Dieser Parameter ist optional.

login_url

- Standardwert – None
- Datentyp – Zeichenfolge

Die URL für die Ressource auf der Website des Identitätsanbieters, wenn das generische Browser-SAML-Plugin verwendet wird.

Dieser Parameter ist erforderlich, wenn die Authentifizierung über die SAML- oder Azure-AD-Services über ein Browser-Plug-In erfolgt.

loginToRp

- Standardwert – urn:amazon:webservices
- Datentyp – Zeichenfolge

Die Vertrauensstellung die Sie für den AD-FS-Authentifizierungstyp verwenden möchten.

Diese Zeichenfolge ist optional.

LogLevel

- Standardwert – 0
- Datentyp – Ganzzahl

Verwenden Sie diese Eigenschaft, um die Protokollierung im Treiber zu aktivieren oder zu deaktivieren und den Umfang der in den Protokolldateien enthaltenen Details festzulegen. Wir empfehlen, die Protokollierung nur lange genug zu aktivieren, um ein Problem zu erfassen, da die Protokollierung die Leistung verringert und eine große Menge an Speicherplatz beanspruchen kann.

Legen Sie die Eigenschaft auf einen der folgenden Werte fest:

- 0: OFF. Deaktiviert die gesamte Protokollierung.

- 1: ERROR. Protokolliert Fehlerereignisse, die möglicherweise dazu führen, dass der Treiber weiter ausgeführt wird, aber einen Fehler erzeugt.
- 2: API_CALL. Protokolliert ODBC-API-Funktionsaufrufe mit Funktionsargumentwerten.
- 3: INFO. Protokolliert allgemeine Informationen, die den Fortschritt des Treibers beschreiben.
- 4: MSG_PROTOCOL. Protokolliert detaillierte Informationen über das Nachrichtenprotokoll des Treibers.
- 5: DEBUG. Protokolliert alle Treiberaktivitäten
- 6: DEBUG_APPEND. Führen Sie anhängende Protokolle für alle Treiberaktivitäten.

Wenn die Protokollierung aktiviert ist, erstellt der Treiber die folgenden Protokolldateien an dem Speicherort, den Sie in der LogPathEigenschaft angeben:

- EINE `redshift_odbc.log.1`-Datei, die die Treiberaktivität protokolliert, die während des Handshakes einer Verbindung stattfindet.
- Eine `redshift_odbc.log`-Datei für alle Treiberaktivitäten, nachdem eine Verbindung zur Datenbank hergestellt wurde.

Dieser Parameter ist optional.

LogPath

- Standardwert – Das betriebssystemspezifische TEMP-Verzeichnis
- Datentyp – Zeichenfolge

Der vollständige Pfad zu dem Ordner, in dem der Treiber Protokolldateien speichert, wenn er höher als 0 LogLevelist.

Dieser Parameter ist optional.

Min_TLS

- Standardwert – der Mindestwert.
- Datentyp – Zeichenfolge

Die Mindestversion von TLS/SSL, die der Treiber dem Datenspeicher für die Verschlüsselung von Verbindungen zulässt. Wenn beispielsweise TLS 1.3 angegeben ist, kann TLS 1.2 nicht zum Verschlüsseln von Verbindungen verwendet werden.

Min_TLS akzeptiert die folgenden Werte:

- 1.2: Die Verbindung muss mindestens TLS 1.2 verwenden. Dies ist die TLS-Mindestversion, die für Amazon-Redshift-Verbindungen erforderlich ist.
- 1.3: Die Verbindung muss mindestens TLS 1.3 verwenden. Wir empfehlen TLS 1.3.

Dieser Parameter ist optional.

partner_spid

- Standardwert – None
- Datentyp – Zeichenfolge

Der SPID-Wert (Service Provider ID) des Partners, der bei der Authentifizierung der Verbindung mithilfe des PingFederate Dienstes verwendet werden soll.

Dieser Parameter ist optional.

Passwort | PWS

- Standardwert – Kein
- Datentyp – Zeichenfolge

Das Passwort, das dem Datenbankbenutzernamen entspricht, den Sie im Feld „Benutzer“ (UID|User (Benutzer)|LogonID) angegeben haben.

Dieser Parameter ist optional.

plugin_name

- Standardwert – None
- Datentyp – Zeichenfolge

Der Plug-in-Name des Anmeldeinformationsanbieters, den Sie für die Authentifizierung verwenden möchten.

Folgende Werte werden unterstützt:

- `ADFS`: Verwenden Sie Active-Directory-Verbund-Services für die Authentifizierung.
- `AzureAD`: Verwenden Sie den Microsoft Azure Active Directory (AD)-Service für die Authentifizierung.
- `BrowserAzureAD`: Verwenden Sie zur Authentifizierung ein Browser-Plugin für den Microsoft Azure Active Directory (AD)-Service.
- `BrowserSAML`: Verwenden Sie zur Authentifizierung ein Browser-Plugin für SAML-Services wie Okta oder Ping.
- `IdpTokenAuthPlugin`: Ein Autorisierungs-Plugin, das ein Identity Center (iDC) -Token oder OpenID Connect (OIDC) JSON-basierte Identitätstoken (JWT) von jedem mit dem iDC verknüpften Web-Identitätsanbieter akzeptiert.
- `JWT`: Verwenden Sie ein JSON-Web-Token (JWT) für die Authentifizierung.
- `Ping`: Verwenden Sie den Dienst zur Authentifizierung. PingFederate
- `Okta`: Verwenden Sie den Okta-Service zur Authentifizierung.

Dieser Parameter ist optional.

Port | PortNumber

- Standardwert – 5 439
- Datentyp – Ganzzahl

Die Nummer des TCP-Ports, den der Amazon-Redshift-Server verwendet, um auf Client-Verbindungen zu warten.

Dieser Parameter ist optional.

preferred_role

- Standardwert – None
- Datentyp – Zeichenfolge

Die Rolle, die Sie während der Verbindung zu Amazon Redshift übernehmen möchten. Es wird für die IAM-Authentifizierung verwendet.

Dieser Parameter ist optional.

Profil

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Name des AWS Benutzerprofils, das für die Authentifizierung bei Amazon Redshift verwendet wird.

- Wenn der Parameter Use Instance Profile (die InstanceProfileEigenschaft) auf 1 | TRUE gesetzt ist, hat diese Einstellung Vorrang und der Treiber verwendet stattdessen das Amazon EC2 EC2-Instance-Profil.
- Der Standardspeicherort für die Datei mit den Anmeldeinformationen, die Profile enthält, ist `~/.aws/Credentials`. Die Umgebungsvariable `AWS_SHARED_CREDENTIALS_FILE` kann verwendet werden, um auf eine andere Anmeldeinformationsdatei zu verweisen.

Dieser Parameter ist optional.

provider_name

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Authentifizierungsanbieter, der vom Benutzer mithilfe der CREATE IDENTITY PROVIDER-Abfrage erstellt wurde. Es wird bei der nativen Amazon-Redshift-Authentifizierung verwendet.

Dieser Parameter ist optional.

ProxyHost

- Standardwert – None
- Datentyp – Zeichenfolge

Der Hostname oder die IP-Adresse des Proxy-Servers, über den Sie eine Verbindung herstellen möchten.

Dieser Parameter ist optional.

ProxyPort

- Standardwert – None
- Datentyp – Ganzzahl

Die Nummer des Ports, den der Proxy-Server verwendet, um auf Client-Verbindungen zu warten.

Dieser Parameter ist optional.

ProxyPwd

- Standardwert – None
- Datentyp – Zeichenfolge

Das Passwort, mit dem Sie auf den Proxy-Server zugreifen.

Dieser Parameter ist optional.

ProxyUid

- Standardwert – None
- Datentyp – Zeichenfolge

Der Benutzername, den Sie für den Zugriff auf den Proxy-Server verwenden.

Dieser Parameter ist optional.

ReadOnly

- Standardwert – 0
- Datentyp – boolesch

Ein boolescher Wert, der angibt, ob sich der Treiber im schreibgeschützten Modus befindet.

- 1 | TRUE: Die Verbindung befindet sich im schreibgeschützten Modus und kann nicht in den Datenspeicher schreiben..
- 0 | FALSE: Die Verbindung befindet sich nicht im schreibgeschützten Modus und kann in den Datenspeicher schreiben.

Dieser Parameter ist optional.

region

- Standardwert – Kein
- Datentyp – Zeichenfolge

Die AWS Region, in der sich Ihr Cluster befindet.

Dieser Parameter ist optional.

SecretAccessKey

- Standardwert – None
- Datentyp – Zeichenfolge

Der geheime IAM-Schlüssel für den Benutzer oder die Rolle. Wenn Sie diesen Parameter festlegen, müssen Sie auch die AccessKeyID festlegen.

Dieser Parameter ist optional.

SessionToken

- Standardwert – None
- Datentyp – Zeichenfolge

Das temporäre IAM-Sitzungstoken, das der IAM-Rolle zugeordnet ist, die Sie zur Authentifizierung verwenden.

Dieser Parameter ist optional.

Server | HostName | Host

- Standardwert – Kein

- Datentyp – Zeichenfolge

Der Endpunktserver, zu dem eine Verbindung hergestellt werden soll.

Dieser Parameter muss angegeben werden.

ssl_insecure

- Standardwert – 0
- Datentyp – boolesch

Ein boolescher Wert, der angibt, ob der Treiber die Authentizität des IdP-Serverzertifikats überprüft.

- 1 | TRUE: Der Treiber prüft die Authentizität des IdP-Server-Zertifikats nicht.
- 0 | FALSE: Der Treiber überprüft die Authentizität des IdP-Server-Zertifikats

Dieser Parameter ist optional.

SSLMode

- Standardwert – `verify-ca`
- Datentyp – Zeichenfolge

Der Verifizierungsmodus für das SSL-Zertifikat, der beim Herstellen einer Verbindung mit Amazon Redshift verwendet werden soll. Die folgenden Werte sind möglich:

- `verify-full`: Verbinden Sie sich nur mithilfe von SSL, einer vertrauenswürdigen Zertifizierungsstelle und einem Servernamen, der mit dem Zertifikat übereinstimmt.
- `verify-ca`: Verbinden Sie sich nur mithilfe von SSL und einer vertrauenswürdigen Zertifizierungsstelle.
- `require`: Verbinden Sie sich nur mithilfe von SSL.
- `prefer`: Verbinden Sie sich nur mithilfe von SSL, falls verfügbar. Andernfalls stellen Sie eine Verbindung her, ohne SSL zu verwenden.
- `allow`: Stellen Sie standardmäßig eine Verbindung her, ohne SSL zu verwenden. Wenn der Server SSL-Verbindungen erfordert, verwenden Sie SSL.
- `disable`: Verbinden ohne Verwendung von SSL.

Dieser Parameter ist optional.

StsConnectionTimeout

- Standardwert – 0
- Datentyp – Ganzzahl

Die maximale Wartezeit für IAM-Verbindungen in Sekunden. Wenn der Wert auf 0 gesetzt oder nicht angegeben ist, wartet der Treiber 60 Sekunden auf jeden AWS STS Anruf.

Dieser Parameter ist optional.

StsEndpointUrl

- Standardwert – None
- Datentyp – Zeichenfolge

Diese Option gibt den übergeordneten Endpunkt an, der für die Kommunikation mit AWS Security Token Service ()AWS STS verwendet wird.

Dieser Parameter ist optional.

Benutzer-ID | Benutzer | Anmelde-ID

- Standardwert – Kein
- Datentyp – Zeichenfolge

Der Benutzername, den Sie für den Zugriff auf den Amazon-Redshift-Server verwenden.

Dieser Parameter ist erforderlich, wenn Sie die Datenbankauthentifizierung verwenden.

web_identity_token

- Standardwert – Kein
- Datentyp – Zeichenfolge

Das vom Identitätsanbieter bereitgestellte OAUTH-Token. Es wird im JWT-Plugin verwendet.

Dieser Parameter ist erforderlich, wenn Sie den Parameter plugin_name auf setzen. BasicJwtCredentialsProvider

Frühere ODBC-Treiberversionen

Laden Sie eine frühere Version der Amazon-Redshift-ODBC-Treiberversion 2.x nur dann herunter, wenn Ihr Tool eine spezifische Version des Treibers benötigt.

Verwenden früherer ODBC-Treiberversionen für Microsoft Windows

Nachfolgend finden Sie die früheren Versionen von Amazon-Redshift-ODBC-Treiberversion 2.x für Microsoft Windows:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/ AmazonRedshift ODBC64-2.0.1.0.msi Verwenden Sie
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/ AmazonRedshift ODBC64-2.0.0.11.msi Verwenden Sie in
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/ AmazonRedshift ODBC64-2.0.0.9.msi Verwenden Sie in der
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/ AmazonRedshift ODBC64-2.0.0.8.msi Verwenden Sie in der
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/ AmazonRedshift ODBC64-2.0.0.7.msi Verwenden Sie in der
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/ AmazonRedshift ODBC64-2.0.0.6.msi Verwenden Sie in der
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/ AmazonRedshift ODBC64-2.0.0.5.msi Verwenden Sie in der
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/ AmazonRedshift ODBC64-2.0.0.3.msi Verwenden Sie in
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/ AmazonRedshift ODBC64-2.0.0.1.msi Verwenden Sie in der

Verwenden früherer ODBC-Treiberversionen für Linux

Nachfolgend finden Sie die früheren Versionen von Amazon-Redshift-ODBC-Treiberversion 2.x für Linux:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/ AmazonRedshift ODBC-64-Bit-2.0.1.0.x86_64.rpm Verwenden Sie in
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/ ODBC-64-Bit-2.0.0.11.x86_64.rpm Verwenden Sie in der Region China den folgenden Link. AmazonRedshift AWS
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/ AmazonRedshift ODBC-64-Bit-2.0.0.9.x86_64.rpm Verwenden Sie
- 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 Verwenden Sie
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/ AmazonRedshift ODBC-64-Bit-2.0.0.1.x86_64.rpm Verwenden Sie

Konfigurierung einer ODBC-Verbindung

Für zahlreiche SQL-Client-Tools und Anwendungen von Drittanbietern können Sie eine ODBC-Verbindung verwenden, um Ihren Amazon-Redshift-Cluster zu verbinden. Hierzu müssen Sie die Verbindung auf Ihrem Clientcomputer oder in Ihrer Amazon-EC2-Instance einrichten. Wenn Ihr Client-Tool JDBC unterstützt, sollten Sie aufgrund der einfachen Konfigurierbarkeit von JDBC diese Verbindungsart anstelle von ODBC verwenden. Wenn Ihr Client-Tool JDBC nicht unterstützt, folgen Sie den Schritten in diesem Abschnitt, um eine ODBC-Verbindung zu konfigurieren.

Amazon Redshift stellt 64-Bit-ODBC-Treiber für Linux-, Windows- und macOS X-Betriebssysteme bereit. Die 32-Bit-ODBC-Treiber werden eingestellt. Es werden außer dringenden Sicherheitspatches keine weiteren Updates veröffentlicht.

Aktuelle Informationen zur ODBC-Treiberfunktionalität und zu den Voraussetzungen finden Sie unter Versionshinweise für Amazon-Redshift-ODBC-Treiber.

Informationen zur Installation und Konfigurierung von Amazon-Redshift-ODBC-Treibern finden Sie im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

Wenn Sie eine ODBC-Verbindung verwenden möchten, führen Sie die folgenden Schritte aus.

Themen

- Abrufen der ODBC-URL für Ihren Cluster
- Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows
- Installieren des Amazon-Redshift-ODBC-Treibers unter Linux
- Installieren des Amazon-Redshift-ODBC-Treibers unter macOS X
- Verwenden Sie einen ODBC-Treibermanager, um den Treiber unter Linux und macOS X zu konfigurieren
- Konfigurieren von ODBC-Treiberoptionen
- Frühere ODBC-Treiberversionen

Abrufen der ODBC-URL für Ihren Cluster

Amazon Redshift zeigt die ODBC-URL für Ihren Cluster in der Amazon-Redshift-Konsole an. Diese URL enthält die für die Einrichtung der Verbindung zwischen Ihrem Clientcomputer und der Datenbank benötigten Informationen.

Eine ODBC-URL hat das folgende Format:

```
Driver={driver};Server=endpoint;Database=database_name;UID=user_name;PWD=passwor
```

Die Felder des im Vorhergehenden gezeigten Formats haben die folgenden Werte.

Feld	Wert
`Driver`	Name des 64-Bit-ODBC-Treibers, der verwendet werden soll: Amazon Redshift (x64). Name des 32-Bit-ODBC-Treibers, der verwendet werden soll: Amazon Redshift (x86).
`Server`	Der Endpunkt für den Amazon-Redshift-Cluster.
`Database`	Die Datenbank, die Sie für Ihren Cluster erstellt haben.

Feld	Wert
`UID`	Der Benutzername eines Benutzerkontos, das die Berechtigung für die Verbindung mit der Datenbank besitzt. Dieser Wert ist eine Datenbank berechtigung, keine Amazon-Redshift-Berechtigung. Sie können jedoch das Administratorkonto verwenden, das Sie beim Starten des Clusters eingerichtet haben.
`PWD`	Das Passwort für das Benutzerkonto, um die Verbindung mit der Datenbank herzustellen.
`Port`	Die Portnummer, die Sie beim Starten des Clusters angegeben haben. Wenn Sie eine Firewall haben, stellen Sie sicher, dass dieser Port geöffnet ist, sodass Sie ihn verwenden können.

Die Felder in den vorherigen Tabellen können die folgenden Sonderzeichen enthalten:

```
[]{}(),;?*=!@
```

Wenn Sie diese Sonderzeichen verwenden, müssen Sie den Wert in geschweifte Klammern setzen. So wird beispielsweise der Passwortwert `Your;password123` in einer Verbindungszeichenfolge als `PWD={Your;password123};` dargestellt.

Da `Field=value`-Paare durch ein Semikolon getrennt sind, wird die Kombination von `}` und `;` mit beliebig vielen Leerzeichen dazwischen als Ende eines `Field={value};`-Paares betrachtet. Wir empfehlen Ihnen, die Folge `};` in Ihren Feldwerten zu vermeiden. Wenn Sie als Passwortwert beispielsweise `PWD={This is a passwor} ;d};` festlegen, lautet Ihr Passwort `This is a passwor} ;` und die URL würde einen Fehler ausgeben.

Im Folgenden finden Sie ein Beispiel für eine ODBC-URL.

```
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
```

Informationen darüber, wie Sie Ihre ODBC-Verbindung herstellen können, finden Sie unter Suche der Zeichenfolge für die Verbindung mit dem Cluster.

Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows

Systemanforderungen

Sie installieren den Amazon-Redshift-ODBC-Treiber auf Client-Computern, indem Sie auf ein Amazon-Redshift-Data-Warehouse zugreifen. Jeder Computer, auf dem Sie den Treiber installieren, muss bestimmte Mindestsystemanforderungen erfüllen. Informationen zu den Mindestsystemanforderungen finden Sie im Handbuch für die Installation und Konfiguration des Amazon-Redshift-ODBC-Connectors.

Installieren des Amazon-Redshift-Treibers auf Windows-Betriebssystemen

Gehen Sie wie folgt vor, um die Amazon-Redshift-ODBC-Treiber für Windows-Betriebssysteme herunterzuladen. Verwenden Sie nur dann einen anderen Treiber als die hier aufgelisteten, wenn Sie eine Drittanbieteranwendung ausführen, die für die Verwendung mit Amazon Redshift zertifiziert ist und einen spezifischen Treiber erfordert.

So installieren Sie den ODBC-Treiber

1. Laden Sie einen der folgenden Treiber herunter, abhängig von der Systemarchitektur Ihres SQL-Client-Tools oder Ihrer Anwendung:

   - 64-Bit-ODBC-Treiberversion 1.5.9 1.5.9.

     Der Name dieses Treibers ist Amazon Redshift (x64).
   - 32-Bit-ODBC-Treiberversion 1.4.52 folgenden Link: 32-Bit-ODBC-Treiberversion 1.4.52

     Der Name dieses Treibers ist Amazon Redshift (x86). Die 32-Bit-ODBC-Treiber werden eingestellt. Es werden außer dringenden Sicherheitspatches keine weiteren Updates veröffentlicht.

   > **Note**
   >
   > Laden Sie das MSI-Paket herunter, das der Systemarchitektur Ihres SQL-Client-Tools oder Ihrer Anwendung entspricht. Wenn Ihr SQL-Client-Tool beispielsweise 64-Bit ist, installieren Sie den 64-Bit-Treiber.

Laden Sie anschließend den Lizenzvertrag für Amazon-Redshift-ODBC- und -JDBC-Treiber herunter und prüfen Sie ihn.

2. Doppelklicken Sie auf die MSI-Datei und folgen Sie anschließend den Schritten des Assistenten, um den Treiber zu installieren.

Erstellen eines System-DSN-Eintrags für eine ODBC-Verbindung in Microsoft Windows

Nachdem Sie den ODBC-Treiber heruntergeladen und installiert haben, fügen Sie dem Clientcomputer oder der Amazon-EC2-Instance einen Datenquellennamen (Data Source Name, DSN) hinzu. SQL-Client-Tools verwenden diese Datenquelle, um eine Verbindung mit der Amazon-Redshift-Datenbank herzustellen.

Sie sollten anstelle eines Benutzer-DSN einen System-DSN erstellen. Einige Anwendungen laden die Daten über ein anderes Benutzerkonto. Diese Anwendungen können unter Umständen keine Benutzer-DSNs erkennen, die unter einem anderen Benutzerkonto erstellt wurden.

> **Note**
>
> Für die Authentifizierung mit AWS Identity and Access Management (IAM-) Anmeldeinformationen oder Identity Provider-Anmeldeinformationen (IdP) sind zusätzliche Schritte erforderlich. Weitere Informationen finden Sie unter Konfigurieren einer JDBC- oder ODBC-Verbindung zur Verwendung von IAM-Anmeldeinformationen.

Informationen zum Erstellen eines System-DSN-Eintrags finden Sie im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

So erstellen Sie einen System-DSN-Eintrag für eine ODBC-Verbindung unter Windows

1. Öffnen Sie im Menü Start (Start) die Option ODBC Data Sources (ODBC-Datenquellen).

   Stellen Sie sicher, dass Sie einen ODBC-Datenquellenadministrator mit derselben Bitness wie die Clientanwendung auswählen, über die Sie die Verbindung mit Amazon Redshift herstellen.

2. Wählen Sie im Data Source Administrator (ODBC-Datenquellenadministrator) die Registerkarte Driver (Treiber) und suchen Sie den Treiberordner:

   - Amazon-Redshift-ODBC-Treiber (64-Bit)

- Amazon-Redshift-ODBC-Treiber (32-Bit)

3. Wählen Sie die Registerkarte System DSN (System-DSN) aus, um den Treiber für alle Benutzer auf dem Computer zu konfigurieren, oder die Registerkarte User DSN (Benutzer-DSN), um den Treiber nur für Ihr Benutzerkonto zu konfigurieren.
4. Wählen Sie Add (Hinzufügen) aus. Das Fenster Create New Data Source (Neue Datenquelle erstellen) wird geöffnet.
5. Wählen Sie den Amazon-Redshift-ODBC-Treiber und dann Finish (Beenden) aus. Das Fenster Amazon Redshift ODBC Driver DSN Setup (DSN-Einrichtung des Amazon-Redshift-ODBC-Treibers) wird geöffnet.
6. Geben Sie unter Connection Settings (Verbindungseinstellungen) die folgenden Informationen ein:

   Datenquellenname

   Geben Sie einen Namen für die Datenquelle ein. Sie können jeden gewünschten Namen verwenden, um die Datenquelle später zu identifizieren, nachdem Sie die Verbindung mit Cluster hergestellt haben. Wenn Sie beispielsweise den Anweisungen unter Erste Schritte mit Amazon Redshift gefolgt sind, können Sie `exampleclusterdsn` eingeben, um sich den Cluster leichter zu merken, den Sie mit diesem DSN verknüpfen.

   Server

   Geben Sie den Endpunkt für Ihren Amazon-Redshift-Cluster an. Sie finden diese Informationen in der Amazon-Redshift-Konsole auf der Seite mit den Cluster-Details. Weitere Informationen finden Sie unter Konfigurieren von Verbindungen in Amazon Redshift.

   Port

   Geben Sie die Portnummer ein, die von der Datenbank verwendet wird. Verwenden Sie den Port, für dessen Verwendung der Cluster konfiguriert wurde, als er gestartet oder geändert wurde.

   Datenbank

   Geben Sie den Namen der Amazon-Redshift-Datenbank ein. Wenn Sie den Cluster gestartet haben, ohne einen Datenbanknamen anzugeben, geben Sie ein *dev*. Verwenden Sie andernfalls den Namen, den Sie während des Startvorgangs ausgewählt haben. Wenn Sie den Anweisungen unter Erste Schritte mit Amazon Redshift gefolgt sind, geben Sie *dev* ein.

7. Geben Sie unter Authentication (Authentifizierung) die Konfigurationsoptionen an, um die Standard- oder IAM-Authentifizierung zu konfigurieren. Informationen zu Authentifizierungsoptionen finden Sie unter „Konfigurieren der Authentifizierung unter Windows“ im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Konnektors.
8. Geben Sie unter SSL Settings (SSL-Einstellungen) einen Wert für folgende Einstellungen an:

   SSL-Authentifizierung

   Wählen Sie einen Modus für den Umgang mit Secure Sockets Layer (SSL) aus. In einer Testumgebung können Sie verwenden `prefer`. Für Produktionsumgebungen und dann, wenn ein sicherer Datenaustausch erforderlich ist, verwenden Sie jedoch `verify-ca` oder `verify-full`. Weitere Informationen zur Verwendung von SSL unter Windows finden Sie unter „Konfigurieren der SSL-Verifizierung unter Windows“ im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.
9. Geben Sie unter Additional options (Zusätzliche Optionen) Optionen dazu an, wie Abfrageergebnisse an das SQL-Clienttool oder die SQL-Anwendung zurückgegeben werden. Weitere Informationen finden Sie unter „Konfigurieren von zusätzlichen Optionen unter Windows“ im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.
10. Geben Sie unter Logging Options (Protokollierungsoptionen) Werte für die Protokollierungsoption an: Weitere Informationen finden Sie unter „Konfigurieren von Protokollierungsoptionen unter Windows“ im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

    Wählen Sie dann OK aus.
11. Geben Sie unter Data Type Options (Datentypoptionen) Werte für Datentypen an. Weitere Informationen finden Sie unter „Konfigurieren von Datentypoptionen unter Windows“ im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

    Wählen Sie dann OK aus.
12. Wählen Sie Test aus. Wenn der Client-Computer eine Verbindung mit der Amazon-Redshift-Datenbank herstellen kann, wird Ihnen die folgende Meldung angezeigt: Connection successful (Verbindung erfolgreich).

    Wenn der Client-Computer keine Verbindung mit der Datenbank herstellen kann, können Sie mögliche Fehler beheben. Weitere Informationen finden Sie unter Beheben von Problemen mit Verbindungen in Amazon Redshift.

13. Konfigurieren Sie TCP-Keepalives unter Windows, um ein Timeout für Verbindungen zu verhindern. Informationen zum Konfigurieren von TCP-Keepalives unter Windows finden Sie im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.
14. Konfigurieren Sie die Protokollierung, um die Fehlerbehebung zu erleichtern. Informationen zum Konfigurieren der Protokollierung unter Windows finden Sie im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

Installieren des Amazon-Redshift-ODBC-Treibers unter Linux

Systemanforderungen

Sie installieren den Amazon-Redshift-ODBC-Treiber auf Client-Computern, indem Sie auf ein Amazon-Redshift-Data-Warehouse zugreifen. Jeder Computer, auf dem Sie den Treiber installieren, muss bestimmte Mindestsystemanforderungen erfüllen. Informationen zu den Mindestsystemanforderungen finden Sie im Handbuch für die Installation und Konfiguration des Amazon-Redshift-ODBC-Connectors.

Installieren des Amazon-Redshift-Treibers auf Linux-Betriebssystemen

Führen Sie die in diesem Abschnitt beschriebenen Schritte aus, um die Amazon-Redshift-ODBC-Treiber für eine unterstützte Linux-Distribution herunterzuladen und zu installieren. Der Installationsvorgang installiert die Treiberdateien in den folgenden Verzeichnissen:

- `/opt/amazon/redshiftodbc/lib/64` (für den 64-Bit-Treiber)
- `/opt/amazon/redshiftodbc/ErrorMessages`
- `/opt/amazon/redshiftodbc/Setup`
- `/opt/amazon/redshiftodbc/lib/32` (für den 32-Bit-Treiber)

So installieren Sie den Amazon-Redshift-ODBC-Treibers

1. Laden Sie einen der folgenden Treiber herunter, abhängig von der Systemarchitektur Ihres SQL-Client-Tools oder Ihrer Anwendung:

   - 64-Bit-RPM-Treiberversion 1.5.9 1.5.9.
   - 64-Bit-Debian-Treiberversion 1.5.9 1.5.9.
   - 32-Bit-RPM-Treiberversion 1.4.52 1.4.52
   - 32-Bit-Debian-Treiberversion 1.4.52 1.4.52

Der Name für beide Treiber ist Amazon-Redshift-ODBC-Treiber. Die 32-Bit-ODBC-Treiber werden eingestellt. Es werden außer dringenden Sicherheitspatches keine weiteren Updates veröffentlicht.

> **Note**
>
> Laden Sie das Paket herunter, das der Systemarchitektur Ihres SQL-Client-Tools oder Ihrer Anwendung entspricht. Wenn Ihr Client-Tool beispielsweise 64-Bit ist, installieren Sie einen 64-Bit-Treiber.

Laden Sie anschließend den Lizenzvertrag für Amazon-Redshift-ODBC- und -JDBC-Treiber herunter und prüfen Sie ihn.

2. Navigieren Sie zu dem Verzeichnis, in das Sie das Paket heruntergeladen haben, und führen Sie einen der folgenden Befehle aus. Verwenden Sie den Befehl, der Ihrer Linux-Distribution entspricht.

   - Führen Sie auf den Betriebssystemen RHEL und CentOS den folgenden Befehl aus.

     ```
     yum --nogpgcheck localinstall RPMFileName
     ```

     Ersetzen Sie *RPMFileName* durch den Dateinamen des RPM-Pakets. Im folgenden Beispiel wird die Installation des 64-Bit-Treibers gezeigt:

     ```
     yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-1.x.xx.xxxx-x.x86_64.rpm
     ```

   - Führen Sie auf SLES den folgenden Befehl aus:

     ```
     zypper install RPMFileName
     ```

     Ersetzen Sie *RPMFileName* durch den Dateinamen des RPM-Pakets. Im folgenden Beispiel wird die Installation des 64-Bit-Treibers gezeigt:

     ```
     zypper install AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.rpm
     ```

   - Führen Sie unter Debian den folgenden Befehl aus.

```
sudo apt install ./DEBFileName.deb
```

Ersetzen Sie *DEBFileName.deb* durch den Dateinamen des Debian-Pakets. Im folgenden Beispiel wird die Installation des 64-Bit-Treibers gezeigt:

```
sudo apt install ./AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.deb
```

> **Important**
>
> Wenn Sie die Installation der Treiber abgeschlossen haben, konfigurieren Sie sie für die Verwendung auf Ihrem System. Weitere Informationen zum Konfigurieren von Treibern finden Sie unter Verwenden Sie einen ODBC-Treibermanager, um den Treiber unter Linux und macOS X zu konfigurieren.

Installieren des Amazon-Redshift-ODBC-Treibers unter macOS X

Systemanforderungen

Sie installieren den Treiber auf Client-Computern, indem Sie auf ein Amazon-Redshift-Data-Warehouse zugreifen. Jeder Computer, auf dem Sie den Treiber installieren, muss bestimmte Mindestsystemanforderungen erfüllen. Informationen zu den Mindestsystemanforderungen finden Sie im Handbuch für die Installation und Konfiguration des Amazon-Redshift-ODBC-Connectors.

Installieren des Amazon-Redshift-ODBC-Treibers unter macOS X

Folgen Sie den Schritten in diesem Abschnitt, um den Amazon-Redshift-ODBC-Treiber unter einer unterstützten Version von macOS X herunterzuladen und zu installieren. Der Installationsvorgang installiert die Treiberdateien in den folgenden Verzeichnissen:

- `/opt/amazon/redshift/lib/universal`
- `/opt/amazon/redshift/ErrorMessages`
- `/opt/amazon/redshift/Setup`

So installieren Sie den Amazon-Redshift-ODBC-Treiber unter macOS X

1. Wenn Ihr macOS-X-System Intel-Architektur verwendet, laden Sie die macOS-X-Intel-Treiberversion 1.5.9 herunter. Wenn Ihr System ARM-Architektur verwendet, laden Sie die macOS-X-ARM-Treiberversion 1.5.9 herunter. In beiden Fällen lautet der Name dieses Treibers Amazon-Redshift-ODBC-Treiber.

   Laden Sie anschließend den Lizenzvertrag für Amazon-Redshift-ODBC- und -JDBC-Treiber herunter und prüfen Sie ihn.
2. Doppelklicken Sie auf AmazonRedshiftODBC.dmg, um das Disk-Image zu mounten.
3. Doppelklicken Sie auf AmazonRedshiftODBC.pkg, um das Installationsprogramm auszuführen.
4. Befolgen Sie die Schritte im Installationsprogramm, um die Treiberinstallation abzuschließen. Sie müssen den Bestimmungen des Lizenzvertrags zustimmen, um die Installation durchzuführen.

> **Important**
>
> Wenn Sie die Installation des Treibers abgeschlossen haben, konfigurieren Sie ihn für die Verwendung auf Ihrem System. Weitere Informationen zum Konfigurieren von Treibern finden Sie unter Verwenden Sie einen ODBC-Treibermanager, um den Treiber unter Linux und macOS X zu konfigurieren.

Verwenden Sie einen ODBC-Treibermanager, um den Treiber unter Linux und macOS X zu konfigurieren

Verwenden Sie für Linux- und macOS X-Betriebssysteme verwenden Sie einen ODBC-Treibermanager, um die ODBC-Verbindungseinstellungen zu konfigurieren. ODBC-Treibermanager verwenden Konfigurationsdateien, um ODBC-Datenquellen und -Treiber zu definieren und zu konfigurieren. Der ODBC-Treibermanager, den Sie verwenden, ist vom verwendeten Betriebssystem abhängig:

- unixODBC-Treibermanager (für Linux-Betriebssysteme)
- iODBC-Treiber-Manager (für macOS-X-Betriebssystem)

Weitere Informationen zu den ODBC-Treibermanagern, die für die Konfigurierung der Amazon-Redshift-ODBC-Treiber unterstützt werden, finden Sie unter Systemanforderungen für Linux-Betriebssysteme und Systemanforderungen für macOS-X-Betriebssysteme. Siehe auch „Angeben

von ODBC-Treibermanagern auf Nicht-Windows-Computern“ im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

Für die Konfiguration des Amazon-Redshift-ODBC-Treibers sind drei Dateien erforderlich: `amazon.redshiftodbc.ini`, `odbc.ini` und `odbcinst.ini`.

Wenn Sie die Installation am Standardspeicherort ausgeführt haben, befindet sich die `amazon.redshiftodbc.ini`-Konfigurationsdatei in einem der folgenden Verzeichnisse:

- `/opt/amazon/redshiftodbc/lib/64` (für den 64-Bit-Treiber unter Linux-Betriebssystemen)
- `/opt/amazon/redshiftodbc/lib/32` (für den 32-Bit-Treiber unter Linux-Betriebssystemen)
- `/opt/amazon/redshift/lib` (für den Treiber unter macOS X)

Zusätzlich gibt es unter `/opt/amazon/redshiftodbc/Setup` auf Linux oder /opt/amazon/redshift/Setup unter macOS X `odbc.ini`- und `odbcinst.ini`-Beispieldateien. Sie können diese Dateien als Beispiele für die Konfiguration des Amazon-Redshift-ODBC-Treibers und des Datenquellennamens (DSN) verwenden.

Die Verwendung des Installationsverzeichnisses für den Amazon-Redshift-ODBC-Treiber für die Konfigurationsdateien wird nicht empfohlen. Die Beispieldateien im `Setup`-Verzeichnis dienen lediglich Beispielzwecken. Wenn Sie den Amazon-Redshift-ODBC-Treiber zu einem späteren Zeitpunkt neu installieren oder auf eine neuere Version aktualisieren, wird das Installationsverzeichnis überschrieben. Sie verlieren dann alle Änderungen, die Sie möglicherweise an diesen Dateien vorgenommen haben.

Um dies zu vermeiden, kopieren Sie die `amazon.redshiftodbc.ini`-Datei in ein anderes Verzeichnis als das Installationsverzeichnis. Wenn Sie diese Datei in das Stammverzeichnis des Benutzers kopieren, fügen Sie am Anfang der Datei einen Punkt (.) hinzu, um die Datei zu verbergen.

Verwenden Sie für die `odbc.ini`- und `odbcinst.ini`-Dateien entweder die Konfigurationsdateien im Basisverzeichnis des Benutzers, oder erstellen Sie neue Versionen in einem anderen Verzeichnis. Standardmäßig sollte Ihr Linux- oder macOS X-Betriebssystem eine `odbc.ini`-Datei und eine `odbcinst.ini`-Datei im Home-Verzeichnis des Benutzers (`/home/$USER` oder `~/`) haben. Bei diesen Standarddateien handelt es sich um versteckte Dateien, die durch den Punkt (.) vor jedem Dateinamen angezeigt werden. Diese Dateien werden nur angezeigt, wenn Sie das `-a`-Flag zum Auflisten des Verzeichnisinhalts verwenden.

Unabhängig davon, welche Option Sie für die `odbc.ini`- und `odbcinst.ini`-Dateien wählen, ändern Sie die Dateien, um Treiber- und DSN-Konfigurationsinformationen hinzuzufügen. Wenn Sie

neue Dateien erstellen, müssen Sie auch Umgebungsvariablen festlegen, um anzugeben, wo diese Konfigurationsdateien gespeichert sind.

Standardmäßig sind ODBC-Treibermanager so konfiguriert, dass sie versteckte Versionen der `odbc.ini`- und `odbcinst.ini`-Konfigurationsdateien (mit den Namen `odbc.ini` und.`odbcinst.ini`) im Home-Verzeichnis verwenden. Sie sind auch so konfiguriert, dass die `amazon.redshiftodbc.ini`-Datei im `/lib`-Unterordner des Treiberinstallationsverzeichnisses verwendet wird. Wenn Sie diese Konfigurationsdateien an anderer Stelle speichern, legen Sie die folgenden Umgebungsvariablen fest, damit der Treibermanager die Dateien finden kann. Weitere Informationen finden Sie unter „Festlegen der Speicherorte der Treiberkonfigurationsdateien“ im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

Erstellen eines Datenquellennamens unter Linux- und macOS X-Betriebssystemen

Wenn Sie eine Verbindung mit dem Datenspeicher über einen Datenquellennamen (DSN) herstellen, konfigurieren Sie die `odbc.ini`-Datei für die Definition von DSNs. Legen Sie die Eigenschaften in der `odbc.ini`-Datei fest, um einen DSN zu erstellen, der die Verbindungsinformationen für den Datenspeicher angibt.

Informationen zur Konfiguration der `odbc.ini` Datei finden Sie unter „Erstellen eines Datenquellennamens auf einem Nicht-Windows-Computer“ im Installations- und Konfigurationsleitfaden für den Amazon Redshift ODBC Connector. Connector Installations- und Konfigurationshandbuch

Verwenden Sie das folgende Format auf Linux-Betriebssystemen.

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file

Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

Im folgenden Beispiel wird die Konfiguration von odbc.ini mit dem 64-Bit-ODBC-Treiber auf Linux-Betriebssystemen gezeigt.

```
[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
```

Im folgenden Beispiel wird die Konfiguration von odbc.ini mit dem 32-Bit-ODBC-Treiber auf Linux-Betriebssystemen gezeigt.

```
[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
```

Verwenden Sie das folgende Format auf macOS X-Betriebssystemen.

```
[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
```

Im folgenden Beispiel wird die Konfiguration für `odbc.ini` auf macOS X-Betriebssystemen gezeigt:

```
[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
```

Konfigurieren einer Verbindung ohne DSN unter Linux- und macOS X-Betriebssystemen

Um eine Verbindung mit dem Datenspeicher über eine Verbindung herzustellen, die nicht über einen DSN verfügt, definieren Sie den Treiber in der `odbcinst.ini`-Datei. Geben Sie dann eine DSN-lose Verbindungszeichenfolge in Ihrer Anwendung an.

Informationen zum Konfigurieren der `odbcinst.ini`-Datei in diesem Fall finden Sie unter „Konfigurieren einer DNS-losen Verbindung auf einem Nicht-Windows-Computer“ im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

Verwenden Sie das folgende Format auf Linux-Betriebssystemen.

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

Im folgenden Beispiel wird die `odbcinst.ini`-Konfiguration für den 64-Bit-Treiber gezeigt, der bei Linux-Betriebssystemen in den Standardverzeichnissen installiert ist:

```
[ODBC Drivers]
Amazon Redshift (x64)=Installed

[Amazon Redshift (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
```

Im folgenden Beispiel wird die `odbcinst.ini`-Konfiguration für den 32-Bit-Treiber gezeigt, der bei Linux-Betriebssystemen in den Standardverzeichnissen installiert ist:

```
[ODBC Drivers]
Amazon Redshift (x86)=Installed

[Amazon Redshift (x86)]
Description=Amazon Redshift ODBC Driver (32-bit)
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so
```

Verwenden Sie das folgende Format auf macOS X-Betriebssystemen.

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/lib/amazonredshiftodbc.dylib

...
```

Im folgenden Beispiel wird die `odbcinst.ini`-Konfiguration für den Treiber gezeigt, der im Standardverzeichnis von macOS X-Betriebssystemen installiert ist.

```
[ODBC Drivers]
Amazon RedshiftODBC DSN=Installed

[Amazon RedshiftODBC DSN]
Description=Amazon Redshift ODBC Driver for macOS X
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
```

Konfigurieren von Umgebungsvariablen

Verwenden Sie den richtigen ODBC-Treibermanager, um den korrekten Treiber zu laden. Legen Sie dazu die Umgebungsvariable für den Bibliothekspfad fest. Weitere Informationen finden Sie unter „Angeben von ODBC-Treibermanagern auf Nicht-Windows-Computern“ im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

Standardmäßig sind ODBC-Treibermanager so konfiguriert, dass sie versteckte Versionen der `odbc.ini`- und `odbcinst.ini`-Konfigurationsdateien (mit den Namen `odbc.ini` und.`odbcinst.ini`) im Home-Verzeichnis verwenden. Sie sind auch so konfiguriert, dass die

`amazon.redshiftodbc.ini`-Datei im `/lib`-Unterordner des Treiberinstallationsverzeichnisses verwendet wird. Wenn Sie diese Konfigurationsdateien an anderer Stelle speichern, werden die Umgebungsvariablen verwendet, damit der Treibermanager die Dateien finden kann. Weitere Informationen finden Sie unter „Festlegen der Speicherorte der Treiberkonfigurationsdateien“ im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

Konfigurieren von Verbindungsfunktionen

Sie können die folgenden Verbindungsfunktionen für Ihre ODBC-Einstellung konfigurieren:

- Konfigurieren Sie den ODBC-Treiber, um Anmeldeinformationen bereitzustellen und die Verbindung zur Amazon-Redshift-Datenbank zu authentifizieren.
- Konfigurieren Sie den ODBC-Treiber für die Herstellung einer Verbindung zu einem Socket, das mit Secure Sockets Layer (SSL) aktiviert ist, wenn Sie eine Verbindung zu einem Amazon-Redshift-Server herstellen, auf dem SSL aktiviert ist.
- Konfigurieren Sie den ODBC-Treiber für die Verbindung zu Amazon Redshift über einen Proxy-Server.
- Konfigurieren Sie den ODBC-Treiber so, dass er einen Abfrageverarbeitungsmodus verwendet, um zu verhindern, dass Abfragen zu viel Speicher belegen.
- Konfigurieren Sie den ODBC-Treiber so, dass IAM-Authentifizierungsprozesse über einen Proxy-Server übergeben werden.
- Konfigurieren Sie den ODBC-Treiber so, dass TCP-Keepalives verwendet werden, um ein Timeout für Verbindungen zu verhindern.

Informationen zu diesen Verbindungsfunktionen finden Sie im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

Konfigurieren von ODBC-Treiberoptionen

Sie können Konfigurationsoptionen verwenden, um das Verhalten des Amazon-Redshift-ODBC-Treibers zu steuern.

Unter Microsoft Windows legen Sie die Treiberoptionen in der Regel fest, wenn Sie einen Datenquellennamen (Data Source Name, DSN) konfigurieren. Sie können auch Treiberoptionen in der Verbindungszeichenfolge einstellen, wenn Sie eine programmgesteuerte Verbindung herstellen oder Registrierungsschlüssel in hinzufügen oder ändern `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\`*`your_DSN`*. Weitere Informationen zur Konfiguration eines DSN finden Sie unter Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows.

Unter Linux und macOS X legen Sie Treiberkonfigurationsoptionen in Ihren `odbc.ini`- und `amazon.redshiftodbc.ini`-Dateien fest, wie unter Verwenden Sie einen ODBC-Treibermanager, um den Treiber unter Linux und macOS X zu konfigurieren beschrieben. In einer `amazon.redshiftodbc.ini`-Datei eingestellte Konfigurationsoptionen gelten für alle Verbindungen. Konfigurationsoptionen, die in einer `odbc.ini`-Datei festgelegt wurden, gelten hingegen jeweils nur für eine bestimmte Verbindung. In `odbc.ini` eingestellte Konfigurationsoptionen haben Vorrang vor Konfigurationsoptionen, die in `amazon.redshiftodbc.ini` festgelegt sind.

Informationen zum Einrichten von ODBC-Treiberkonfigurationsoptionen finden Sie im Handbuch für die Installation und Konfigurierung des Amazon-Redshift-ODBC-Connectors.

Frühere ODBC-Treiberversionen

Sie sollten eine frühere Version des Amazon-Redshift-ODBC-Treibers nur dann herunterladen, wenn Ihr Tool eine spezifische Treiberversion benötigt.

Verwenden früherer ODBC-Treiberversionen für Windows

Im Folgenden sind die 64-Bit-Treiber aufgeführt:

- 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 Verwenden Sie in der Region China
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/ AmazonRedshiftodbc64-1.4.62.1000.msi Verwenden Sie in der Region China
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshiftodbc64-1.4.59.1000.msi Verwenden Sie in der Region China
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshiftodbc64-1.4.56.1000.msi Verwenden Sie in der Region
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.53.1000/ AmazonRedshiftodbc64-1.4.53.1000.msi Verwenden Sie in der Region
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshiftodbc64-1.4.52.1000.msi Verwenden Sie in der Region

32-Bit-Treiber werden eingestellt und frühere Versionen werden nicht unterstützt.

Verwenden früherer ODBC-Treiberversionen für Linux

Im Folgenden sind die Versionen des 64-Bit-Treibers aufgeführt:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/ AmazonRedshift ODBC-64-Bit-1.5.7.1007-1.x86_64.rpm Verwenden Sie in
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/ AmazonRedshift ODBC-64-Bit-1.4.65.1000-1.x86_64.rpm Verwenden Sie in der Region
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/ AmazonRedshift ODBC-64-Bit-1.4.62.1000-1.x86_64.rpm Verwenden Sie in der Region
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift ODBC-64-Bit-1.4.59.1000-1.x86_64.rpm Verwenden Sie in der Region
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift ODBC-64-Bit-1.4.59.1000-1.x86_64.deb Verwenden Sie in
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC-64-Bit-1.4.56.1000-1.x86_64.rpm Verwenden Sie in
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC-64-Bit-1.4.56.1000-1.x86_64.deb Verwenden Sie in
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC-64-Bit-1.4.52.1000-1.x86_64.rpm Verwenden Sie in
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC-64-Bit-1.4.52.1000-1.x86_64.deb Verwenden Sie in

32-Bit-Treiber werden eingestellt und frühere Versionen werden nicht unterstützt.

Verwenden früherer ODBC-Treiberversionen für macOS X

Im Folgenden finden Sie die Versionen des Amazon-Redshift-ODBC-Treibers für macOS X:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/ AmazonRedshift ODBC-1.5.7.1007.x86_64.dmg Verwenden Sie in der
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/ AmazonRedshift ODBC-1.4.65.1000.dmg Verwenden Sie in der Region China
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/ AmazonRedshift ODBC-1.4.62.1000.dmg Verwenden Sie in der Region China

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift ODBC-1.4.59.1000.dmg Verwenden Sie in der Region China
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC-1.4.56.1000.dmg Verwenden Sie in der Region
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC-1.4.52.1000.dmg Verwenden Sie in der Region

Konfigurieren von Sicherheitsoptionen für Verbindungen

Amazon Redshift unterstützt Secure Sockets Layer (SSL)-Verbindungen, um Daten und Serverzertifikate zu verschlüsseln, um das Zertifikat des Servers zu validieren, mit dem der Client die Verbindung herstellt.

Verbindung über SSL

Um SSL-Verbindungen zu unterstützen, erstellt und installiert Amazon Redshift auf jedem Cluster ein von AWS Certificate Manager (ACM) ausgegebenes SSL-Zertifikat. ACM-Zertifikaten wird von den meisten Betriebssystemen, Webbrowsern und Clients öffentlich vertraut. Sie müssen unter Umständen ein Zertifikatspaket herunterladen, wenn Ihre SQL-Clients oder -Anwendungen eine SSL-Verbindung zu Amazon Redshift herstellen und die Verbindungsoption `sslmode` auf `require`, `verify-ca` oder `verify-full` festgelegt ist. Wenn Ihr Kunde ein Zertifikat benötigt, stellt Amazon Redshift wie folgt ein Zertifikatspaket zur Verfügung:

- Laden Sie das Paket von https://s3.amazonaws.com/redshift-downloads/ .crt herunter. amazon-trust-ca-bundle
  - Die erwartete MD5-Prüfsummennummer ist 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - Die sha256-Prüfsummennummer ist 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  Verwenden Sie nicht das vorherige Zertifikatpaket, das auf `https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt` zu finden ist.
- Laden Sie das Paket in China AWS-Region von https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt herunter.
  - Die erwartete MD5-Prüfsummennummer ist 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - Die sha256-Prüfsummennummer ist 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

Verwenden Sie nicht vorherige Zertifikatpakete, die auf `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` und `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem` zu finden sind.

> **Important**
>
> Amazon Redshift hat die Verwaltung von SSL-Zertifikaten verändert. Sie müssen möglicherweise Ihre aktuellen vertrauenswürdigen CA-Stammzertifikate aktualisieren, um weiterhin mit SSL Verbindungen zu Ihren Clustern herstellen zu können. Weitere Informationen finden Sie unter Umstellung auf ACM-Zertifikate für SSL-Verbindungen.

Standardmäßig akzeptieren Cluster-Datenbanken eine Verbindung unabhängig davon, ob es sich um eine SSL-Verbindung handelt oder nicht. Um Ihren Cluster so zu konfigurieren, dass er eine SSL-Verbindung erfordert, legen Sie den Parameter `require_SSL` in der Parametergruppe, die mit dem Cluster verknüpft ist, auf `true` fest.

Amazon Redshift unterstützt ein mit Federal Information Processing Standard (FIPS) 140-2 kompatibles SSL-Modus. Der FIPS-kompatible SSL-Modus ist standardmäßig deaktiviert.

> **Important**
>
> Aktivieren Sie den FIPS-konformen SSL-Modus nur, wenn Ihr System FIPS-konform sein muss.

Wenn Sie den FIPS-kompatiblen SSL-Modus aktivieren möchten, legen Sie in der dem Cluster zugeordneten Parametergruppe für die Parameter `use_fips_ssl` und `require_SSL` den Wert `true` fest. Weitere Informationen zum Ändern von Parametergruppen finden Sie unter Amazon-Redshift-Parametergruppen.

Amazon Redshift unterstützt das Elliptic Curve Diffie–Hellman Ephemeral (ECDHE) Key Agreement-Protokoll. Mit ECDHE besitzen sowohl der Client als auch der Server ein öffentlich-privates Elliptic Curve-Schlüsselpaar, das verwendet wird, um ein gemeinsames Geheimnis über einen nicht sicheren Kanal einzurichten. Sie müssen nichts in Amazon Redshift konfigurieren, um ECDHE zu aktivieren. Wenn Sie sich von einem SQL-Client-Tool aus verbinden, das ECDHE verwendet, um

die Kommunikation zwischen dem Client und dem Server zu verschlüsseln, verwendet Amazon Redshift die angegebene Verschlüsselungsliste, um die entsprechende Verbindung herzustellen. Weitere Informationen finden Sie unter Diffie-Hellman-Schlüsselaustausch auf Wikipedia und Ciphers (Verschlüsselungsverfahren) auf der OpenSSL-Website.

Verwenden von SSL- und Trust CA-Zertifikaten in ODBC

Wenn Sie Verbindungen mithilfe der aktuellen Amazon Redshift-ODBC-Treiber (Version 1.3.7.1000 oder neuer) herstellen, können Sie diesen Abschnitt überspringen. Die neuesten Treiber finden Sie unter Konfigurierung einer ODBC-Verbindung.

Sie müssen möglicherweise Ihre aktuellen vertrauenswürdigen CA-Stammzertifikate aktualisieren, um weiterhin mit SSL Verbindungen zu Ihren Clustern herstellen zu können. Weitere Informationen finden Sie unter Verbindung über SSL.

Sie können überprüfen, ob das heruntergeladene Zertifikat mit der erwarteten MD5-Prüfsummenzahl übereinstimmt. Um dies zu tun, können Sie das MD5sum-Programm unter Linux oder ein anderes Tool unter Windows- und macOS X-Betriebssystemen verwenden.

ODBC DSNs enthalten eine `sslmode`-Einstellung, die festlegt, wie die Verschlüsselung für die Verifizierung von Clientverbindungen und Serverzertifikaten verarbeitet wird. Amazon Redshift unterstützt die folgenden `sslmode`-Werte aus der Clientverbindung:

- `disable`

  SSL ist deaktiviert und die Verbindung ist nicht verschlüsselt.
- `allow`

  SSL wird verwendet, wenn der Server es fordert.
- `prefer`

  SSL wird verwendet, wenn der Server es unterstützt. Amazon Redshift unterstützt SSL. Daher wird SSL verwendet, wenn Sie`sslmode` auf `prefer` festlegen.
- `require`

  SSL ist erforderlich.
- `verify-ca`

  SSL muss verwendet werden und das Serverzertifikat muss bestätigt werden.

- `verify-full`

  SSL muss verwendet werden. Das Serverzertifikat muss bestätigt werden und der Server-Hostname muss mit dem Hostnamen-Attribut auf dem Zertifikat übereinstimmen.

Sie können festlegen, ob SSL verwendet wird und Serverzertifikate in einer Verbindung zwischen Client und Server verifiziert werden. Dazu müssen Sie die `sslmode`-Einstellung für Ihren ODBC-DSN auf dem Client und die `require_SSL`-Einstellung für den Amazon-Redshift-Cluster auf dem Server überprüfen. In der folgenden Tabelle wird das Verschlüsselungsergebnis für die verschiedenen Kombinationen von Client- und Servereinstellungen beschrieben:

sslmode (Client)	require_SSL (Server)	Ergebnis
`disable`	`false`	Die Verbindung ist nicht verschlüsselt.
`disable`	`true`	Die Verbindung kann nicht hergestellt werden, da der Server SSL erfordert und auf dem Client SSL für die Verbindung deaktiviert ist.
`allow`	`true`	Die Verbindung ist verschlüsselt.
`allow`	`false`	Die Verbindung ist nicht verschlüsselt.
`prefer` oder `require`	`true`	Die Verbindung ist verschlüsselt.
`prefer` oder `require`	`false`	Die Verbindung ist verschlüsselt.
`verify-ca`	`true`	Die Verbindung ist verschlüsselt und das Serverzertifikat ist bestätigt.
`verify-ca`	`false`	Die Verbindung ist verschlüsselt und das Serverzertifikat ist bestätigt.
`verify-full`	`true`	Die Verbindung ist verschlüsselt und das Serverzertifikat und der Host-Name sind bestätigt.

sslmode (Client)	require_SSL (Server)	Ergebnis
`verify-full`	`false`	Die Verbindung ist verschlüsselt und das Serverzertifikat und der Host-Name sind bestätigt.

Verbindung unter Verwendung des Serverzertifikats mit ODBC in Microsoft Windows

Wenn Sie mithilfe von SSL und dem Serverzertifikat eine Verbindung mit dem Cluster herstellen möchten, laden Sie das Zertifikat zuerst auf den Clientcomputer oder die Amazon-EC2-Instance herunter. Konfigurieren Sie dann den ODBC-DSN.

1. Laden Sie das Amazon-Redshift-Zertifizierungsstellen-Bundle auf Ihren Client-Computer in den Ordner `lib` in Ihrem Verzeichnis für die Treiberinstallation herunter und speichern Sie die Datei als `root.crt`. Informationen zum Download finden Sie unter Verbindung über SSL.
2. Öffnen Sie ODBC Data Source Administrator (OBDC-Datenquellenadministrator) und fügen Sie den DSN-Eintrag des Systems für Ihre ODBC-Verbindung hinzu oder bearbeiten Sie diesen. Wählen Sie für SSL Mode (SSL-Modus) die Option `verify-full` aus, wenn Sie kein DNS-Alias verwenden. Wählen Sie aus, wenn Sie ein DNS-Alias verwenden `verify-ca`. Wählen Sie dann Speichern.

   Weitere Informationen zum Konfigurieren des ODBC-DSN finden Sie unter Konfigurierung einer ODBC-Verbindung.

Verwenden von SSL- und Serverzertifikaten in Java

SSL stellt eine einzelne Sicherheitsschicht bereit, indem Daten verschlüsselt werden, die zwischen Ihrem Client und Ihrem Cluster verschoben werden. Die Verwendung eines Serverzertifikats bietet eine zusätzliche Sicherheitsschicht, da auf diese Weise überprüft wird, ob es sich beim Cluster um einen Amazon-Redshift-Cluster handelt. Dies erfolgt durch Prüfung des Serverzertifikats, das automatisch auf allen von Ihnen bereitgestellten Clustern installiert wird. Weitere Informationen zur Verwendung von Serverzertifikaten mit JDBC finden Sie unter Configuring the client in der PostgreSQL-Dokumentation.

Verbindungsherstellung unter Verwendung von Trust CA-Zertifikaten in Java

> **Important**
>
> Amazon Redshift hat die Verwaltung von SSL-Zertifikaten verändert. Sie müssen möglicherweise Ihre aktuellen vertrauenswürdigen CA-Stammzertifikate aktualisieren, um weiterhin mit SSL Verbindungen zu Ihren Clustern herstellen zu können. Weitere Informationen finden Sie unter Verbindung über SSL.

Mithilfe von Trust CA-Zertifikaten stellen Sie eine Verbindung wie folgt her

Sie können die `redshift-keytool.jar` Datei verwenden, um CA-Zertifikate aus dem Amazon Redshift Certificate Authority Bundle in ein Java-Format TrustStore oder Ihr privates TrustStore zu importieren.

1. Wenn Sie die Option `-Djavax.net.ssl.trustStore` für die Java-Befehlszeile verwenden, entfernen Sie es falls möglich aus der Befehlszeile.
2. Laden Sie redshift-keytool.jar herunter.
3. Führen Sie eine der folgenden Aktionen aus:

   - Führen Sie den folgenden Befehl aus, um das Amazon Redshift Certificate Authority Bundle in Java TrustStore zu importieren.

     ```
     java -jar redshift-keytool.jar -s
     ```

   - Führen Sie den folgenden Befehl aus, um das Amazon Redshift Certificate Authority Bundle in Ihr privates TrustStore Paket zu importieren:

     ```
     java -jar redshift-keytool.jar -k <your_private_trust_store> -
     p <keystore_password>
     ```

Umstellung auf ACM-Zertifikate für SSL-Verbindungen

Amazon Redshift ersetzt die SSL-Zertifikate Ihrer Cluster durch von AWS Certificate Manager (ACM) ausgegebene Zertifikate. ACM ist eine vertrauenswürdige öffentliche Zertifizierungsstelle, der die meisten Systeme vertrauen. Sie müssen möglicherweise Ihre aktuellen vertrauenswürdigen CA-

Stammzertifikate aktualisieren, um weiterhin mit SSL Verbindungen zu Ihren Clustern herstellen zu können.

Diese Änderung betrifft Sie nur, wenn alle folgenden Bedingungen zutreffen:

- Die SQL-Clients bzw. -Anwendungen stellen Verbindungen zu Amazon Redshift mithilfe von SSL her, wenn die Verbindungsoption `sslMode` auf die Konfigurationsoptionen `require`, `verify-ca` oder `verify-full` festgelegt ist.
- Sie verwenden nicht die Amazon-Redshift-ODBC- oder -JDBC-Treiber oder Sie verwenden Amazon-Redshift-Treiber älter als ODBC-Version 1.3.7.1000 oder JDBC-Version 1.2.8.1005.

Falls diese Änderung Sie in kommerziellen Amazon-Redshift-Regionen betrifft, müssen Sie Ihre aktuellen vertrauenswürdigen CA-Stammzertifikate vor dem 23. Oktober 2017 aktualisieren. Amazon Redshift führt die Umstellung Ihrer Cluster auf die Nutzung von ACM-Zertifikaten im Zeitraum von heute bis zum 23. Oktober 2017 durch. Diese Änderung sollte nur geringe oder keine Auswirkungen auf die Leistung und Verfügbarkeit Ihres Clusters haben.

Wenn diese Änderung Sie in Regionen AWS GovCloud (US) (USA) betrifft, müssen Sie Ihre aktuellen Trust-Root-CA-Zertifikate vor dem 1. April 2020 aktualisieren, um Serviceunterbrechungen zu vermeiden. Ab diesem Datum benötigen Clients, die sich über SSL-verschlüsselte Verbindungen mit Amazon-Redshift-Clustern verbinden, eine zusätzliche vertrauenswürdige Zertifizierungsstelle (CA). Clients verwenden vertrauenswürdige Zertifizierungsstellen, um die Identität des Amazon-Redshift-Clusters zu bestätigen, wenn sie eine Verbindung zu ihm herstellen. Ihre Aktion ist erforderlich, um Ihre SQL-Clients und -Anwendungen zu aktualisieren, um ein aktuelles Zertifikatpaket zu verwenden, das die neue vertrauenswürdige Zertifizierungsstelle enthält.

> **Important**
>
> In den Regionen Chinas ersetzt Amazon Redshift am 5. Januar 2021 die SSL-Zertifikate auf Ihren Clustern durch AWS Certificate Manager (ACM) ausgestellte Zertifikate. Wenn sich diese Änderung auf die Region China (Peking) oder China (Ningxia) auswirkt, müssen Sie Ihre aktuellen CA-Stammzertifikate vor dem 5. Januar 2021 aktualisieren, um Serviceunterbrechungen zu vermeiden. Ab diesem Datum benötigen Clients, die sich über SSL-verschlüsselte Verbindungen mit Amazon-Redshift-Clustern verbinden, eine zusätzliche vertrauenswürdige Zertifizierungsstelle (CA). Clients verwenden vertrauenswürdige Zertifizierungsstellen, um die Identität des Amazon-Redshift-Clusters zu bestätigen, wenn sie eine Verbindung zu ihm herstellen. Ihre Aktion ist erforderlich, um Ihre SQL-Clients und -

Anwendungen zu aktualisieren, um ein aktuelles Zertifikatpaket zu verwenden, das die neue vertrauenswürdige Zertifizierungsstelle enthält.

- Verwendung der aktuellen Amazon-Redshift-ODBC- bzw. -JDBC-Treiber
- Verwendung älterer Amazon-Redshift-ODBC- bzw. -JDBC-Treiber
- Verwendung anderer SSL-Verbindungstypen

Verwendung der aktuellen Amazon-Redshift-ODBC- bzw. -JDBC-Treiber

Bevorzugt verwenden Sie die aktuellen Amazon Redshift-ODBC- bzw. -JDBC-Treiber. Amazon Redshift-Treiber ab ODBC-Version 1.3.7.1000 und JDBC-Version 1.2.8.1005 verwalten die Umstellung von einem selbstsignierten Amazon Redshift-Zertifikat auf ein ACM-Zertifikat automatisch. Die neuesten Treiber finden Sie unter Konfigurierung einer ODBC-Verbindung oder Konfigurieren einer Verbindung für JDBC-Treiberversion 2.1 für Amazon Redshift.

Falls Sie die aktuellen Amazon Redshift-JDBC-Treiber verwenden, sollten Sie die Option `-Djavax.net.ssl.trustStore` in den JVM-Optionen nicht verwenden. Falls Sie `-Djavax.net.ssl.trustStore` verwenden müssen, importieren Sie das Redshift-Zertifizierungsstellen-Bundle in den TrustStore, auf den es verweist. Informationen zum Download finden Sie unter Verbindung über SSL. Weitere Informationen finden Sie unter Importieren des Amazon Redshift Redshift-Zertifizierungsstellenpakets in ein TrustStore.

Verwendung älterer Amazon-Redshift-ODBC- bzw. -JDBC-Treiber

- Falls Ihr ODBC-DSN mit `SSLCertPath` konfiguriert ist, überschreiben Sie die Zertifikatsdatei im angegebenen Verzeichnis.
- Falls `SSLCertPath` nicht konfiguriert ist, überschreiben Sie die Zertifikatdatei `root.crt` im Treiber-DLL-Verzeichnis.

Wenn Sie Amazon-Redshift-JDBC-Treiber verwenden müssen, die älter als Version 1.2.8.1005 sind, führen Sie einen der folgenden Schritte aus:

- Entfernen Sie die Option `sslCert`, falls Ihre JDBC-Verbindungszeichenfolge die Option `sslCert` verwendet. Importieren Sie dann das Redshift Certificate Authority Bundle in Ihr Java TrustStore. Informationen zum Download finden Sie unter Verbindung über SSL. Weitere Informationen finden Sie unter Importieren des Amazon Redshift Redshift-Zertifizierungsstellenpakets in ein TrustStore.

- Wenn Sie die Option `-Djavax.net.ssl.trustStore` für die Java-Befehlszeile verwenden, entfernen Sie es falls möglich aus der Befehlszeile. Importieren Sie dann das Redshift Certificate Authority Bundle in Ihr Java TrustStore. Informationen zum Download finden Sie unter Verbindung über SSL. Weitere Informationen finden Sie unter Importieren des Amazon Redshift Redshift-Zertifizierungsstellenpakets in ein TrustStore.

Importieren des Amazon Redshift Redshift-Zertifizierungsstellenpakets in ein TrustStore

Sie können verwenden`redshift-keytool.jar`, um CA-Zertifikate aus dem Amazon Redshift Certificate Authority Bundle in einen Java TrustStore - oder Ihren privaten Truststore zu importieren.

Um das Amazon Redshift Certificate Authority Bundle in ein TrustStore

1. Laden Sie redshift-keytool.jar herunter.
2. Führen Sie eine der folgenden Aktionen aus:

   - Führen Sie den folgenden Befehl aus, um das Amazon Redshift Certificate Authority Bundle in Java TrustStore zu importieren.

     ```
     java -jar redshift-keytool.jar -s
     ```

   - Führen Sie den folgenden Befehl aus, um das Amazon Redshift Certificate Authority Bundle in Ihr privates TrustStore Paket zu importieren:

     ```
     java -jar redshift-keytool.jar -k <your_private_trust_store> -
     p <keystore_password>
     ```

Verwendung anderer SSL-Verbindungstypen

Befolgen Sie die Anweisungen in diesem Abschnitt, wenn Sie eine der folgenden Möglichkeiten zur Verbindungsherstellung nutzen:

- Open-Source-ODBC-Treiber
- Open-Source-JDBC-Treiber
- Die Befehlszeilenschnittstelle von Amazon Redshift RSQL
- Sprachbindungen auf Grundlage von libpq, z. B. psycopg2 (Python) und ruby-pg (Ruby)

Verwenden Sie ACM-Zertifikate wie folgt mit anderen SSL-Verbindungstypen:

1. Laden Sie das Amazon-Redshift-Zertifizierungsstellen-Bundle herunter. Informationen zum Download finden Sie unter Verbindung über SSL.
2. Platzieren Sie die Zertifikate des Bundle in der Datei `root.crt`.
   - Unter Linux- und macOS X-Betriebssystemen ist diese Datei `~/.postgresql/root.crt`.
   - Unter Microsoft Windows ist diese Datei `%APPDATA%\postgresql\root.crt`.

Herstellen von Verbindungen von Client-Tools aus und mit Code

Amazon Redshift stellt Amazon Redshift Query Editor v2 zum Herstellen einer Verbindung mit Ihren Clustern und Arbeitsgruppen bereit. Weitere Informationen finden Sie unter Abfragen für Datenbanken mit dem Amazon-Redshift-Abfrage-Editor v2.

In diesem Abschnitt sind einige Optionen für Drittanbietertools zum Herstellen einer Verbindung aufgeführt. Außerdem wird beschrieben, wie Sie programmbasiert eine Verbindung mit Ihrem Cluster herstellen.

Themen

- Verbinden mit Amazon-Redshift-RSQL
- Verbinden mit einem Cluster mit Amazon-Redshift-RSQL
- Amazon-Redshift-RSQL-Metabefehle
- Amazon-Redshift-RSQL-Variablen
- Amazon-Redshift-RSQL-Fehlercodes
- Amazon-Redshift-RSQL-Umgebungsvariablen

Verbinden mit Amazon-Redshift-RSQL

Amazon-Redshift-RSQL ist ein Befehlszeilenclient für die Interaktion mit Amazon-Redshift-Clustern und -Datenbanken. Sie können eine Verbindung zu einem Amazon-Redshift-Cluster herstellen, Datenbankobjekte beschreiben, Daten abfragen und Abfrageergebnisse in verschiedenen Ausgabeformaten anzeigen.

Amazon-Redshift-RSQL unterstützt die Funktionen des PostgreSQL PSQL-Befehlszeilentools mit zusätzlichen Funktionen, die für Amazon Redshift spezifisch sind. Diese umfassen u. a. folgende:

- Sie können die Single Sign-On-Authentifizierung mit ADFS, Okta PingIdentity, Azure AdM oder anderen SAML/JWT-basierten Identitätsanbietern verwenden. Sie können auch browserbasierte SAML-Identitätsanbieter für die Mehrfaktor-Authentifizierung (MFA) verwenden.
- Sie können Eigenschaften oder Attribute von Amazon-Redshift-Objekten wie Tabellenverteilungsschlüssel, Tabellensortierschlüssel, späte Bindungsansichten (LBVs) und Materialized Views beschreiben. Sie können auch Eigenschaften oder Attribute externer Tabellen in einem AWS Glue -Katalog oder Apache Hive Metastore, externe Datenbanken in Amazon RDS for PostgreSQL, Amazon Aurora PostgreSQL kompatible Edition, RDS for MySQL (Vorschau) und Amazon Aurora MySQL-kompatible Edition (Vorschau) und Tabellen beschreiben, die mithilfe der Amazon-Redshift-Datenfreigabe freigegeben werden.
- Sie können auch erweiterte Steuerflussbefehle wie `IF` (`\ELSEIF`, `\ELSE,`, `\ENDIF`), `\GOTO` und `\LABEL` verwenden.

Im Amazon-Redshift-RSQL-Batchmodus, der ein Skript ausführt, das als Eingabeparameter übergeben wird, können Sie Skripte ausführen, die sowohl SQL als auch komplexe Geschäftslogik enthalten. Wenn Sie bereits über selbstverwaltete On-Premises-Data-Warehouses verfügen, können Sie Amazon-Redshift-RSQL verwenden, um vorhandene ETL-Skripte (ETL = Extrahieren, Transformieren, Laden) und Automatisierungsskripte wie Teradata-BTEQ-Skripte zu ersetzen. Die Verwendung von RSQL hilft Ihnen, Skripte in einer prozeduralen Sprache manuell neu zu implementieren.

Amazon Redshift ist verfügbar für Linux-, Windows- und macOS-X-Betriebssysteme.

Um Probleme mit Amazon Redshift RSQL zu melden, schreiben Sie an `<redshift-rsql-support@amazon>` .com.

Themen

- Erste Schritte mit Amazon-Redshift-RSQL
- Änderungsprotokoll für Amazon Redshift-RSQL

Erste Schritte mit Amazon-Redshift-RSQL

Installieren Sie Amazon-Redshift-RSQL auf einem Computer mit einem Linux-, macOS- oder Microsoft Windows-Betriebssystem.

RSQL herunterladen

- Linux 64-Bit-RPM: RSQL-Version 1.0.8

- Mac OS 64-Bit-DMG: RSQL-Version 1.0.8
- Windows 64-Bit MSI: RSQL-Version 1.0.8

Siehe das Änderungsprotokoll und die Downloads für frühere Versionen unter Änderungsprotokoll für Amazon Redshift-RSQL.

RSQL für Linux installieren

Gehen Sie wie folgt vor, um RSQL für Linux zu installieren.

1. Installieren Sie den Treibermanager mit dem folgenden Befehl:

   ```
   sudo yum install unixODBC openssl
   ```

   OpenSSL ist für Linux-Verteilungen erforderlich. Die OpenSSL-Bibliothek befindet sich im Linux OpenSSL-Github-Repository. Weitere Informationen zu OpenSSL finden Sie unter OpenSSL.
2. Installieren Sie den ODBC-Treiber: Installieren des Amazon-Redshift-Treibers auf Linux-Betriebssystemen.
3. Kopieren Sie die .ini-Datei in Ihr aktuelles Verzeichnis.

   ```
   cp /opt/amazon/redshiftodbc/Setup/odbc.ini ~/.odbc.ini
   ```
4. Stellen Sie die Umgebungsvariablen so ein, dass sie auf den Speicherort der Datei verweisen:

   ```
   export ODBCINI=~/.odbc.ini
       export ODBCSYSINI=/opt/amazon/redshiftodbc/Setup
       export AMAZONREDSHIFTODBCINI=/opt/amazon/redshiftodbc/lib/64/
   amazon.redshiftodbc.ini
   ```

   Weitere Informationen zur Konfiguration der ODBC-Umgebungsvariablen finden Sie unter Konfigurieren von Umgebungsvariablen.
5. Sie können jetzt RSQL installieren, indem Sie folgenden Befehl ausführen.

   ```
   sudo rpm -i AmazonRedshiftRsql-<version>-1.x86_64.rpm
   ```

RSQL für Mac installieren

Gehen Sie wie folgt vor, um RQL für Mac OSX zu installieren.

1. Installieren Sie den Treibermanager mit dem folgenden Befehl:

   ```
   brew install unixodbc openssl@1.1 --build-from-source
   ```

2. Installieren Sie den ODBC-Treiber: Installieren des Amazon-Redshift-ODBC-Treibers unter macOS X.
3. Kopieren Sie die .ini-Datei in Ihr aktuelles Verzeichnis.

   ```
   cp /opt/amazon/redshift/Setup/odbc.ini ~/.odbc.ini
   ```

4. Stellen Sie die Umgebungsvariablen so ein, dass sie auf den Speicherort der Datei verweisen:

   ```
   export ODBCINI=~/.odbc.ini
   export ODBCSYSINI=/opt/amazon/redshift/Setup
   export AMAZONREDSHIFTODBCINI=/opt/amazon/redshift/lib/amazon.redshiftodbc.ini
   ```

   Weitere Informationen zur Konfiguration der ODBC-Umgebungsvariablen finden Sie unter Konfigurieren von Umgebungsvariablen.

5. Geben Sie mit `DYLD_LIBRARY_PATH` den Speicherort Ihrer libodbc.dylib an, wenn diese nicht in `/usr/local/lib` ist.

   ```
   export DYLD_LIBRARY_PATH=$DYLD_LIBRARY_PATH:/usr/local/lib
   ```

6. Doppelklicken Sie auf die DMG-Datei, um das Disk Image zu mounten.
7. Doppelklicken Sie auf die PKG-Datei, um das Installationsprogramm auszuführen.
8. Befolgen Sie die Schritte im Installationsassistenten, um die Installation abzuschließen. Stimmen Sie den Bedingungen der Lizenzvereinbarung zu.

Installieren von RSQL für Windows

Zum Installieren des Treibers folgen Sie den Anweisungen in Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows. Windows benötigt keinen Treibermanager.

OpenSSL ist für Amazon-Redshift-RSQL unter Windows erforderlich. Die Windows OpenSSL-Bibliothek befindet sich im Windows OpenSSL-Repository GitHub . Weitere Informationen zu OpenSSL finden Sie unter OpenSSL.

Doppelklicken Sie auf die RSQL-Download-Datei, um das Installationsprogramm auszuführen, und folgen Sie den angezeigten Schritten, um die Installation abzuschließen.

Änderungsprotokoll für Amazon Redshift-RSQL

1.0.6 (19.06.2023)

Fehlerbehebungen

- Es wurde ein Problem behoben, bei dem die Ausgabe mit SHOW-Befehlen abgeschnitten wurde.
- Zu \de wurde Unterstützung für die Beschreibung externer Kinesis-Streams und Kafka-Themen hinzugefügt.

1.0.7 (22.03.2023)

Fehlerbehebungen

- Das Problem, dass RSQL keine materialisierten Ansichten beschreiben konnte, wurde behoben.
- Ein Fehler aufgrund einer verweigerten Berechtigung in stl_connection_log bei Verwendung von Amazon Redshift Serverless wurde behoben.
- Das Problem, dass RSQL \GOTO-Labels möglicherweise falsch verarbeitet, wurde behoben.
- Das Problem, dass SSL-Nachrichten im Modus „Quiet“ gedruckt werden, wurde behoben.
- Das Problem, dass bei der Beschreibung von gespeicherten Prozeduren zufällige Zeichen angezeigt werden, wurde behoben.
- Das Problem, dass doppelte ERROR/INFO-Meldungen gedruckt werden, wurde behoben.

Neu

- RSQL erhält jetzt SSL-Informationen direkt vom ODBC-Treiber.

1.0.6 (21.02.2023)

Fehlerbehebungen

- Das Problem, dass \d einen Fehler – ungültige Eingabesyntax für Ganzzahl: „xid“ – auslöst, wurde in Redshift-Patch 1.0.46086 (P173) behoben.

Neu

- Die Installationsdateien wurden umbenannt, um die unterstützte Architektur widerzuspiegeln.

1.0.5 (27.06.2022)

Fehlerbehebungen

- Sendet SQL-Fehlermeldungen an den Standardfehler (stderr).
- Problem mit Exitcodes bei Verwendung von ON_ERROR_STOP behoben. Skripte werden jetzt nach dem Auftreten eines Fehlers beendet und geben die korrekten Exitcodes zurück.
- Maxerror berücksichtigt jetzt Groß- und Kleinschreibung nicht mehr.

Neu

- Support für ODBC 2.x-Treiber hinzugefügt.

1.0.4 (19.03.2022)

- Hinzufügung von Unterstützung für die RSPASSWORD-Umgebungsvariable. Festlegen eines Passworts, um eine Verbindung zu Amazon Redshift herzustellen. Zum Beispiel `export RSPASSWORD=TestPassw0rd`.

1.0.3 (2021-12-08)

Fehlerbehebungen

- Das Popup des Dialogs bei Verwendung von `\c` oder `\logon`, um zwischen Datenbanken im Windows-Betriebssystem zu wechseln, wurde behoben.
- Absturz beim Überprüfen von SSL-Informationen wurde behoben.

Vorgängerversionen von Amazon-Redshift-RSQL

Wählen Sie einen der Links aus, um die benötigte Version von Amazon-Redshift-RSQL basierend auf Ihrem Betriebssystem herunterzuladen.

Linux 64-Bit-RPM

- RSQL-Version 1.0.7
- RSQL-Version 1.0.6
- RSQL-Version 1.0.5
- RSQL-Version 1.0.4
- RSQL-Version 1.0.3
- RSQL-Version 1.0.1

Mac OS 64-Bit-DMG

- RSQL-Version 1.0.7
- RSQL-Version 1.0.6
- RSQL-Version 1.0.5
- RSQL-Version 1.0.4
- RSQL-Version 1.0.3
- RSQL-Version 1.0.1

Windows 64-Bit MSI

- RSQL-Version 1.0.7
- RSQL-Version 1.0.6
- RSQL-Version 1.0.5
- RSQL-Version 1.0.4
- RSQL-Version 1.0.3
- RSQL-Version 1.0.1

Verbinden mit einem Cluster mit Amazon-Redshift-RSQL

Verbinden ohne DSN

1. Wählen Sie in der Amazon-Redshift-Konsole den Cluster aus, mit dem Sie eine Verbindung herstellen möchten, und notieren Sie sich den Endpunkt, die Datenbank und den Port.
2. Geben Sie in der Eingabeaufforderung die Verbindungsinformationen an, indem Sie entweder Befehlszeilenparameter verwenden.

   ```
   rsql -h <endpoint> -U <username> -d <databasename> -p <port>
   ```

   Hier gilt Folgendes:

   - *<endpoint>* ist der Endpoint (Endpunkt), den Sie im vorherigen Schritt notiert haben.
   - *<username>* ist der Name eines Benutzers mit Berechtigungen für die Verbindung mit dem Cluster.
   - *<databasename>* ist der Database Name (Datenbankname), den Sie im vorherigen Schritt notiert haben.
   - *<port>* ist der Port, den Sie im vorherigen Schritt notiert haben. *<port>* ist ein optionaler Parameter.

   Ein Beispiel folgt.

   ```
   rsql -h testcluster.example.amazonaws.com -U user1 -d dev -p 5439
   ```

3. Wenn Sie aufgefordert werden, das Passwort einzugeben, geben Sie das Passwort für den Benutzer *<username>* ein.

   Ein erfolgreiches Ergebnis sieht wie folgt aus.

   ```
   % 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=#
```

Der Befehl zum Verbinden hat dieselben Parameter unter Linux, Mac OS und Windows.

Verbinden mit einem DSN

Sie können RSQL über einen Datenquellennamen (DSN) mit Amazon Redshift verbinden, um die Organisation von Verbindungseigenschaften zu vereinfachen. Weitere Informationen finden Sie unter Konfigurieren von Verbindungsfunktionen. Dieses Thema enthält Anweisungen zur ODBC-Treiberinstallation und Beschreibungen für DSN-Eigenschaften. Der folgende Abschnitt Installation und Konfiguration des ODBC-Treibers von Amazon Redshift unter Microsoft Windows zeigt beispielsweise, wie Sie mithilfe von Windows eine Verbindung mit einem DSN herstellen.

Verwenden einer DSN-Verbindung mit einem Passwort

Im Folgenden wird ein Beispiel für eine DSN-Verbindungskonfiguration gezeigt, die ein Passwort verwendet. Der Standard-`<path to driver>` ist `/opt/amazon/redshift/lib/libamazonredshiftodbc.dylib` für Mac OSX und `/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so` für Linux.

```
[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
```

Die folgende Ausgabe erfolgt bei einer erfolgreichen Verbindung.

```
% 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=#
```

Verwenden von Single-Sign-on-DSN

Sie können einen DSN für die Single-Sign-On-Authentifizierung konfigurieren. Im Folgenden wird ein Beispiel für eine DSN-Verbindungskonfiguration gezeigt, die den Okta Single Sign-On verwendet.

```
[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>
```

Beispielausgabe einer erfolgreichen Verbindung.

```
% 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=#
```

Im Folgenden wird ein Beispiel für eine DSN-Verbindungskonfiguration gezeigt, die den Azure Single Sign-On verwendet.

```
[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>
```

Verwenden einer DSN-Verbindung mit einem IAM-Profil

Sie können sich über Ihr konfiguriertes IAM-Profil mit Amazon Redshift verbinden. Das IAM-Profil muss über Berechtigungen zum Aufrufen von `GetClusterCredentials` verfügen. Das folgende Beispiel zeigt die zu verwendenden DSN-Eigenschaften. Die Parameter `ClusterID` und `Region` sind nur erforderlich, wenn `Host` kein von Amazon bereitgestellter Endpunkt wie `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com` ist.

```
[testiam]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Profile=default
```

Der Wert für den `Profile` Schlüssel ist das benannte Profil, das Sie aus Ihren AWS CLI-Anmeldeinformationen auswählen. Dieses Beispiel zeigt die Anmeldeinformationen für das Profil `default`.

```
$ cat .aws/credentials
[default]
aws_access_key_id = ASIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

Nachfolgend ist die Beispielantwort dargestellt.

```
$ 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=>
```

Verwenden einer DSN-Verbindung mit einem Instance-Profil

Sie können über Ihr Amazon-EC2-Instance-Profil eine Verbindung zu Amazon Redshift herstellen. Das Instance-Profil muss über Berechtigungen zum Aufrufen von `GetClusterCredentials` verfügen. Im folgenden Beispiel finden Sie die zu verwendenden DSN-Eigenschaften. Die Parameter `ClusterID` und `Region` sind nur erforderlich, wenn `Host` kein von Amazon bereitgestellter Endpunkt wie `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com` ist.

```
[testinstanceprofile]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Instanceprofile=1
```

Nachfolgend ist die Beispielantwort dargestellt.

```
$ 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=>
```

Verwenden einer DSN-Verbindung mit der standardmäßigen Anbieterkette von Anmeldeinformationen

Um eine Verbindung über die standardmäßige Anbieterkette für Anmeldeinformationen herzustellen, geben Sie nur die IAM-Eigenschaft an. Amazon Redshift RSQL versucht dann, Anmeldeinformationen in der unter Arbeiten mit AWS Anmeldeinformationen im SDK for Java beschriebenen Reihenfolge abzurufen. AWS Mindestens einer der Anbieter in der Kette muss die Berechtigung `GetClusterCredentials` besitzen. Dies ist beispielsweise nützlich, um eine Verbindung über ECS-Container herzustellen.

```
[iamcredentials]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
```

Amazon-Redshift-RSQL-Metabefehle

Amazon-Redshift-RSQL-Metabefehle geben Informationsdatensätze über Datenbanken oder bestimmte Datenbankobjekte zurück. Die Ergebnisse können verschiedene Spalten und Metadaten enthalten. Andere Befehle führen bestimmte Aktionen aus. Diesen Befehlen geht ein umgekehrter Schrägstrich voraus.

\d[S+]

Listet lokal vom Benutzer erstellte Tabellen, reguläre Ansichten, späte Bindungsansichten und materialisierte Ansichten auf. `\dS` listet wie `\d` auch Tabellen und Ansichten auf,

aber in den zurückgegebenen Datensätzen sind Systemobjekte enthalten. Das + ergibt die zusätzliche Metadatenspalte `description` für alle aufgelisteten Objekte. Im Folgenden werden Beispieldatensätze angezeigt, die als Ergebnis des Befehls zurückgegeben wurden.

```
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

Beschreibt eine Tabelle, eine Ansicht oder einen Index. Beinhaltet die Spaltennamen und -typen. Bietet auch Diststyle, Backup-Konfiguration, Erstellungsdatum (Tabellen, die nach Oktober 2018 erstellt wurden) und Einschränkungen. Zum Beispiel gibt `\dS+ sample` Objekteigenschaften zurück. Angabe von S+ ergibt zusätzliche Spalten, die in den zurückgegebenen Datensätzen enthalten sind.

```
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)
```

Der Verteilungsstil oder Diststyle der Tabelle kann KEY, AUTO, EVEN oder ALL sein.

Backup gibt an, ob die Tabelle gesichert wird, wenn ein Snapshot erstellt wird. Gültige Werte sind YES oder NO.

Created (erstellt) ist der Zeitstempel für die Erstellung der Tabelle. Das Erstellungsdatum ist für Amazon-Redshift-Tabellen, die vor November 2018 erstellt wurden, nicht verfügbar. Für Tabellen, die vor diesem Datum erstellt wurden, wird n/a (nicht verfügbar) angezeigt.

Unique Constraints (eindeutige Einschränkungen) listet eindeutige und Primärschlüsseleinschränkungen für die Tabelle auf.

Foreign-key constraints (Fremdschlüsseleinschränkungen) listet fremde Schlüsseleinschränkungen für die Tabelle auf.

\dC[+] [MUSTER]

Listet Casts auf. Beinhaltet den Quelltyp, den Zieltyp und ob der Cast implizit ist.

Im Folgenden wird eine Teilmenge der Ergebnisse von \dC+ angezeigt.

```
List of casts
         source type         |         target type         |      function       |
 implicit?   | description
-----------------------------+-----------------------------+---------------------
+---------------+-------------
 "char"                      | character                   | bpchar              | in
 assignment |
 "char"                      | character varying           | text                | in
 assignment |
 "char"                      | integer                     | int4                | no
          |
 "char"                      | text                        | text                | yes
          |
```

```
"path"                      | point                       | point              | no
        |
"path"                      | polygon                     | polygon            | in
assignment |
abstime                     | date                        | date               | in
assignment |
abstime                     | integer                     | (binary coercible) | no
        |
abstime                     | time without time zone      | time               | in
assignment |
abstime                     | timestamp with time zone    | timestamptz        | yes
        |
abstime                     | timestamp without time zone | timestamp          | yes
        |
bigint                      | bit                         | bit                | no
        |
bigint                      | boolean                     | bool               | yes
        |
bigint                      | character                   | bpchar             | in
assignment |
bigint                      | character varying           | text               | in
assignment |
bigint                      | double precision            | float8             | yes
        |
bigint                      | integer                     | int4               | in
assignment |
bigint                      | numeric                     | numeric            | yes
        |
bigint                      | oid                         | oid                | yes
        |
bigint                      | real                        | float4             | yes
        |
bigint                      | regclass                    | oid                | yes
        |
bigint                      | regoper                     | oid                | yes
        |
bigint                      | regoperator                 | oid                | yes
        |
bigint                      | regproc                     | oid                | yes
        |
bigint                      | regprocedure                | oid                | yes
        |
bigint                      | regtype                     | oid                | yes
        |
```

```
 bigint                      | smallint                  | int2              | in
 assignment |
 bigint                      | super                     | int8_partiql      | in
 assignment |
```

\dd[S] [MUSTER]

Zeigt Objektbeschreibungen an, die an anderer Stelle nicht angezeigt werden

\de

Listet externe Tabellen auf. Dazu gehören Tabellen im AWS Glue Datenkatalog, Hive Metastore und Verbundtabellen aus Amazon RDS/Aurora MySQL, Amazon RDS/Aurora PostgreSQL und Amazon Redshift Datashare.

\de NAME

Beschreibt eine externe Tabelle.

AWS Glue Das folgende Beispiel zeigt eine externe Tabelle.

```
# \de spectrum.lineitem
                          Glue External table "spectrum.lineitem"
     Column      | External Type | Redshift Type | Position | Partition Key | Nullable
-----------------+---------------+---------------+----------+---------------+----------
 l_orderkey      | bigint        | bigint        | 1        | 0             |
 l_partkey       | bigint        | bigint        | 2        | 0             |
 l_suppkey       | int           | int           | 3        | 0             |
 l_linenumber    | int           | int           | 4        | 0             |
 l_quantity      | decimal(12,2) | decimal(12,2) | 5        | 0             |
 l_extendedprice | decimal(12,2) | decimal(12,2) | 6        | 0             |
 l_discount      | decimal(12,2) | decimal(12,2) | 7        | 0             |
 l_tax           | decimal(12,2) | decimal(12,2) | 8        | 0             |
 l_returnflag    | char(1)       | char(1)       | 9        | 0             |
 l_linestatus    | char(1)       | char(1)       | 10       | 0             |
 l_shipdate      | date          | date          | 11       | 0             |
 l_commitdate    | date          | date          | 12       | 0             |
 l_receiptdate   | date          | date          | 13       | 0             |
 l_shipinstruct  | char(25)      | char(25)      | 14       | 0             |
 l_shipmode      | char(10)      | char(10)      | 15       | 0             |
 l_comment       | varchar(44)   | varchar(44)   | 16       | 0             |
```

```
Location: s3://redshiftbucket/kfhose2019/12/31
Input_format: org.apache.hadoop.mapred.TextInputFormat
Output_format: org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat
Serialization_lib: org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe
Serde_parameters: {"field.delim":"|","serialization.format":"|"}
Parameters:
 {"EXTERNAL":"TRUE","numRows":"178196721475","transient_lastDdlTime":"1577771873"}
```

Eine Hive-Metastore-Tabelle.

```
# \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"}
```

Eine externe PostgreSQL-Tabelle.

```
# \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+] [MUSTER]

Listet Funktionen verschiedener Typen auf. Der Befehl `\df` gibt beispielsweise eine Liste von Funktionen zurück. Zu den Ergebnissen gehören Eigenschaften wie Name, zurückgegebener Datentyp, Zugriffsberechtigungen und zusätzliche Metadaten. Funktionstypen können Trigger, gespeicherte Prozeduren, Fensterfunktionen und andere Typen umfassen. Wenn Sie `S+` an den Befehl anhängen, zum Beispiel `\dfantS+`, sind zusätzliche Metadatenspalten wie `owner`, `security` und `access privileges` enthalten.

\dL[S+] [MUSTER]

Listet Daten zu Prozedursprachen auf, die mit der Datenbank verknüpft sind. Die Informationen umfassen den Namen, z. B. plpgsql, und zusätzliche Metadaten, unter anderem Vertrauenswürdigkeit, Zugriffsrechte und Beschreibung. Ein Beispielaufruf ist `\dLS+`, der Sprachen und ihre Eigenschaften auflistet. Wenn Sie `S+` an den Befehl anhängen, sind zusätzliche Metadatenspalten wie `call handler` und `access privileges` enthalten.

Beispielergebnisse:

```
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+] [MUSTER]

Listet materialisierte Ansichten auf. Zum Beispiel listet \dmS+ materialisierte Ansichten und ihre Eigenschaften auf. Wenn Sie S+ an den Befehl anhängen, sind zusätzliche Metadatenspalten enthalten.

\dn[S+] [MUSTER]

Listet Schemata auf Wenn Sie S+ an den Befehl anhängen, zum Beispiel \dnS+, sind zusätzliche Metadatenspalten wie `description` und `access privileges` enthalten.

\dp [MUSTER]

Listet Zugriffsberechtigungen für Tabellen, Anzeigen und Sequenzen auf.

\dt[S+] [MUSTER]

Listet Tabellen auf. Wenn Sie S+ an den Befehl anhängen, zum Beispiel \dtS+, sind zusätzliche Metadatenspalten wie `description` enthalten.

\du

Listet die Benutzer für die Datenbank auf. Enthält deren Namen und Rollen, z. B. Superuser, und Attribute.

\dv[S+] [MUSTER]

Listet Ansichten auf. Umfasst Schema, Typ und Besitzerdaten. Wenn Sie S+ an den Befehl anhängen, zum Beispiel \dvS+, sind zusätzliche Metadatenspalten enthalten.

\H

Schaltet die HTML-Ausgabe ein. Dies ist hilfreich, um schnell formatierte Ergebnisse zurückzugeben. Zum Beispiel gibt `select * from sales; \H` Ergebnisse aus der Verkaufstabelle in HTML

zurück. Um zurück zu tabellarischen Ergebnissen zu wechseln, verwenden Sie `\q` oder verlassen Sie die Anzeige.

\i

Führt Befehle aus einer Datei aus. Angenommen, Sie haben rsql_steps.sql in Ihrem Arbeitsverzeichnis, dann führen Sie die Befehle in der Datei `\i rsql_steps.sql` wie folgt aus.

\l[+] [MUSTER]

Listet Datenbanken auf. Beinhaltet Besitzer, Kodierung und zusätzliche Informationen.

\q

Das Beenden oder der \q-Befehl meldet Datenbanksitzungen ab und beendet RSQL.

\sv[+] VIEWNAME

Zeigt die Definition einer Ansicht an.

\timing

Zeigt beispielsweise die Laufzeit für eine Abfrage an.

\z [MUSTER]

Dieselbe Ausgabe wie\ dp.

\?

Zeigt Hilfeinformationen an. Der optionale Parameter gibt das zu erklärende Element an.

\VERLASSEN

Meldet alle Datenbanksitzungen ab und beendet Amazon-Redshift-RSQL. Darüber hinaus können Sie einen optionalen Beendigungscode angeben. Zum Beispiel beendet `\EXIT 15` das Amazon-Redshift-RSQL-Terminal und gibt den Beendigungscode 15 zurück.

Das folgende Beispiel zeigt die Ausgabe einer Verbindung und das Beenden von 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

Gibt den Namen einer Exportdatei an, die RSQL zum Speichern von Datenbankinformationen verwendet, die von einer nachfolgenden SQL-SELECT-Anweisung zurückgegeben werden.

export_01.sql

```
\export report file='E:\\accounts.out'
\rset rformat off
\rset width 1500
\rset heading "General Title"
\rset titledashes on
select * from td_dwh.accounts;
\export reset
```

Konsolenausgabe

```
Rformat is off.
Target width is 1500.
Heading is set to: General Title
Titledashes is on.
(exported 40 rows)
```

\ANMELDUNG

Verbindung zu einer Datenbank herstellen. Sie können Verbindungsparameter mithilfe der Positionssyntax oder als Verbindungszeichenfolge angeben.

Die Befehlssyntax ist wie folgt: `\logon {[DBNAME|- USERNAME|- HOST|- PORT|- [PASSWORD]] | conninfo}`

DBNAME ist der Name der Datenbank, mit der eine Verbindung hergestellt werden soll. USERNAME ist der Benutzername für die Verbindung. Der Standardwert HOST ist `localhost`. Der Standardwert PORT ist 5439.

Wird ein Hostname in einem \LOGON-Befehl angegeben, wird dies der Standard-Hostname für zusätzliche \LOGON-Befehle. Um den Standard-Hostnamen zu ändern, geben Sie einen neuen HOST mit einem zusätzlichen \LOGON-Befehl an.

Beispielausgabe des \LOGON-Befehls für `user1` siehe unten.

```
(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=#
```

Beispielausgabe für user2 (Benutzer 2).

```
(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=#
```

\ANMERKUNG

Eine Erweiterung des \echo-Befehls. \REMARK gibt die angegebene Zeichenfolge in den Ausgabestream aus. \REMARK erweitert \echo, indem die Möglichkeit hinzugefügt wird, die Ausgabe über separate Zeilen zu verteilen.

Das folgende Beispiel zeigt die Ausgabe des Befehls.

```
(testcluster) user1@dev=# \remark 'hello//world'
hello
world
```

\RSET

Der Befehl `\rset` legt Befehlsparameter und Variablen fest. `\rset` hat sowohl einen interaktiven als auch einen Batch-Modus. Es unterstützt keine Optionen als Bash-Optionen, wie -x oder Argumente zum Beispiel --<arg>.

Es legt Variablen wie die folgenden fest:

- ERRORLEVEL
- HEADING und RTITLE
- RFORMAT
- MAXERROR
- TITLEDASHES
- WIDTH

Das folgende Beispiel gibt eine Überschrift an.

```
\rset heading "Winter Sales Report"
```

Weitere Beispiele für die Verwendung von `\rset` finden Sie in den Amazon-Redshift-RSQL-Variablen-Themen.

\AUSFÜHREN

Führt das Amazon-Redshift-RSQL-Skript aus, das in der angegebenen Datei enthalten ist. `\RUN` ist eine Erweiterung des `\i`-Befehls durch Hinzufügen einer Option zum Überspringen von Kopfzeilen in einer Datei.

Wenn der Dateiname ein Komma, ein Semikolon oder ein Leerzeichen enthält, schließen Sie ihn in einfache Anführungszeichen ein. Wenn dem Dateinamen Text folgt, schließen Sie ihn ebenfalls in Anführungszeichen ein. Unter UNIX muss bei den Dateinamen die Groß- und Kleinschreibung beachtet werden. Unter Windows wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Das folgende Beispiel zeigt die Ausgabe des Befehls.

```
(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)
```

\BS

Ein Alias für den \!-Befehl. \OS führt den Betriebssystembefehl aus, der als Parameter übergeben wird. Der Controller kehrt nach Ausführung des Befehls zu Amazon-Redshift-RSQL zurück. Sie können z. B. den folgenden Befehl ausführen, um die aktuelle Systemzeit zu drucken und zum RSQL-Terminal zurückzukehren: `\os date`.

```
(testcluster) user1@dev=# \os date
Tue Sep 7 20:47:54 UTC 2021
```

\GOTO

Ein neuer Befehl für Amazon-Redshift-RSQL. \GOTO überspringt alle dazwischenliegenden Befehle und setzt die Verarbeitung am angegebenen \LABEL fort. \LABEL muss eine Vorwärtsreferenz sein. Sie können nicht zu einem \LABEL springen, das \GOTO lexikalisch vorangeht.

Das folgende Beispiel zeigt die Beispielausgabe.

```
(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

Ein neuer Befehl für Amazon-Redshift-RSQL. \LABEL legt einen Einstiegspunkt für die Ausführung des Programms als Ziel für einen \GOTO-Befehl fest.

Das folgende Beispiel zeigt die Ausgabe des Befehls.

```
(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)

\IF und verwandte Befehle führen bedingt Teile des Eingabeskripts aus. Eine Erweiterung des PSQL \if-Befehls (\elif, \else, \endif). \IF und \ELSEIF unterstützt boolesche Ausdrücke einschließlich Bedingungen AND, OR und NOT.

Das folgende Beispiel zeigt die Ausgabe der Befehle.

```
(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
```

Verwenden von ERRORCODE in Ihrer Verzweigungslogik.

```
\if :'ERRORCODE' = '00000'
    \remark 'The statement was executed without error'
\else
```

```
    \remark :LAST_ERROR_MESSAGE
\endif
```

Verwenden von `\GOTO` innerhalb eines `\IF`-Blocks, um zu steuern, wie Code ausgeführt wird.

Amazon-Redshift-RSQL-Variablen

Einige Schlüsselwörter fungieren in RSQL als Variablen. Sie können jede auf einen bestimmten Wert festlegen oder den Wert erneut festlegen. Die meisten sind auf `\rset` festgelegt, das über einen interaktiven Modus und einen Batch-Modus verfügt. Befehle können in Klein- oder Großbuchstaben definiert werden.

ACTIVITYCOUNT

Gibt die Anzahl der Zeilen an, die von der zuletzt übermittelten Anfrage betroffen sind. Bei einer Datenrückgabeanforderung ist dies die Anzahl der Zeilen, die aus der Datenbank an RSQL zurückgegeben werden. Der Wert ist 0 oder eine positive ganze Zahl. Der Höchstwert beträgt 18.446.744.073.709.551.615.

Die speziell behandelte Variable `ACTIVITYCOUNT` ähnelt der Variable `ROW_COUNT`. Allerdings meldet `ROW_COUNT` die Anzahl der betroffenen Zeilen nach Beendigung des Befehls nicht an die Clientanwendung für `SELECT`, `COPY` oder `UNLOAD`. Aber `ACTIVITYCOUNT` meldet dies.

activitycount_01.sql:

```
select viewname, schemaname
from pg_views
where schemaname = 'not_existing_schema';
\if :ACTIVITYCOUNT = 0
\remark 'views do not exist'
\endif
```

Konsolenausgabe:

```
viewname | schemaname
----------+------------
(0 rows)

views do not exist
```

ERRORLEVEL

Weist Fehlern Schweregrade zu. Verwenden Sie den Schweregrad, um eine Aktion zu bestimmen. Wenn der ERRORLEVEL-Befehl nicht verwendet wurde, ist sein Wert standardmäßig ON.

errorlevel_01.sql:

```
\rset errorlevel 42P01 severity 0

select * from tbl;

select 1 as col;

\echo exit
\quit
```

Konsolenausgabe:

```
Errorlevel is on.
rsql: ERROR: relation "tbl" does not exist
(1 row)

col
1

exit
```

HEADING und RTITLE

Ermöglicht Benutzern, einen Header anzugeben, der oben in einem Bericht angezeigt wird. Der durch den RSET RTITLE-Befehl angegebene Header enthält automatisch das aktuelle Systemdatum des Client-Computers.

Inhalt von rset_heading_rtitle_02.rsql:

```
\remark Starting...
\rset rtitle "Marketing Department||Confidential//Third Quarter//Chicago"
\rset width 70
\rset rformat on
select * from rsql_test.tbl_currency order by id limit 2;
\exit
\remark Finishing...
```

Konsolenausgabe:

```
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

Gibt einen maximalen Fehlerschweregrad an, über den RSQL die Auftragsverarbeitung beendet. Rückgabecodes sind ganzzahlige Werte, die RSQL nach Beendigung jeder Aufgabe oder jedes Auftrags an das Client-Betriebssystem zurückgibt. Der Wert des Rückgabecodes gibt den Abschlussstatus des Auftrags oder Vorgangs an. Wenn ein Skript eine Anweisung enthält, die einen Fehlerschweregrad erzeugt, der größer als der festgelegte `maxerror`-Wert ist, wird RSQL sofort beendet. Verwenden Sie daher `RSET MAXERROR 7`, um eine RSQL-Beendigung bei einem Fehlerschweregrad von 8 zu erreichen.

Inhalt von maxerror_01.sql:

```
\rset maxerror 0

select 1 as col;

\quit
```

Konsolenausgabe:

```
Maxerror is default.
(1 row)

col
```

```
1
```

RFORMAT

Ermöglicht Benutzern, anzugeben, ob Einstellungen für die Formatierungsbefehle angewendet werden sollen.

Inhalt von rset_rformat.rsql:

```
\remark Starting...
\pset border 2
\pset format wrapped
\pset expanded on
\pset title 'Great Title'
select * from rsql_test.tbl_long where id = 500;
\rset rformat
select * from rsql_test.tbl_long where id = 500;
\rset rformat off
select * from rsql_test.tbl_long where id = 500;
\rset rformat on
select * from rsql_test.tbl_long where id = 500;
\exit
\remark Finishing...
```

Konsolenausgabe:

```
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

Ruft die Anzahl der Datensätze ab, die von der vorherigen Abfrage betroffen sind. Es wird normalerweise verwendet, um ein Ergebnis zu überprüfen, wie im folgenden Codefragment:

```
SET result = ROW_COUNT;

IF result = 0
...
```

TITLEDASHES

Mit diesem Steuerelement können Benutzer angeben, ob eine Zeile von Strichzeichen über den für SQL-Anweisungen zurückgegebenen Spaltendaten gedruckt werden soll.

Beispiel:

```
\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;
```

Konsolenausgabe:

```
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

Legt das Ausgabeformat auf umgebrochen fest und gibt die Zielbreite für jede Zeile in einem Bericht an. Ohne einen Parameter gibt es die aktuellen Einstellungen sowohl für das Format als auch für die Zielbreite zurück.

Inhalt von rset_width_01.rsql:

```
\echo Starting...
\rset width
\rset width 50
\rset width
\quit
\echo Finishing...
```

Konsolenausgabe:

```
Starting...
Target width is 75.
Target width is 50.
```

```
Target width is 50.
Press any key to continue . . .
```

Beispiel mit Parameter:

```
\echo Starting...
\rset rformat on
\pset format wrapped
select * from rsql_test.tbl_long where id = 500;
\rset width 50
select * from rsql_test.tbl_long where id = 500;
\quit
\echo Finishing...
```

Konsolenausgabe:

```
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 . . .
```

Amazon-Redshift-RSQL-Fehlercodes

Erfolgsmeldungen, Warnungen und Ausnahmen:

Fehlercode	Fehlerklasse	Bedingungsname
00000	Klasse 00 – Erfolgreicher Abschluss	successful_completion

Fehlercode	Fehlerklasse	Bedingungsname
01000	Klasse 01 – Warnung	warning
0100C	Klasse 01 – Warnung	dynamic_result_sets_returned
01008	Klasse 01 – Warnung	mplicit_zero_bit_padding
01003	Klasse 01 – Warnung	null_value_eliminated_in_set_function
01007	Klasse 01 – Warnung	null_value_eliminated_in_set_function
01006	Klasse 01 – Warnung	privilege_not_revoked
01004	Klasse 01 – Warnung	string_data_right_truncation
01P01	Klasse 01 – Warnung	deprecated_feature
02000	Klasse 02 – Keine Daten	no_data
02001	Klasse 02 – Keine Daten	no_additional_dynamic_result_sets_returned
03000	Klasse 03 – SQL-Anweisung noch nicht vollständig	sql_statement_not_yet_complete
08000	Klasse 08 – Verbindungsausnahme	connection_exception
08003	Klasse 08 – Verbindungsausnahme	connection_does_not_exist
08006	Klasse 08 – Verbindungsausnahme	connection_failure
08001	Klasse 08 – Verbindungsausnahme	sqlclient_unable_to_establish_sqlconnection
08004	Klasse 08 – Verbindungsausnahme	sqlserver_rejected_establishment_of_sqlconnection

Fehlercode	Fehlerklasse	Bedingungsname
08007	Klasse 08 – Verbindungsausnahme	transaction_resolution_unknown
08P01	Klasse 08 – Verbindungsausnahme	protocol_violation
09000	Klasse 09 – Ausgelöste Aktionsausnahme	triggered_action_exception
0A000	Klasse 0A – Funktion wird nicht unterstützt	feature_not_supported
0A000	Klasse 0A – Funktion wird nicht unterstützt	feature_not_supported
0B000	Klasse 0B – Ungültige Transaktionsauslösung	invalid_transaction_initiation
0F000	Klasse 0F – Locator-Ausnahme	locator_exception
0F001	Klasse 0F – Locator-Ausnahme	invalid_locator_specification
0L000	Klasse 0L – Ungültiger Berechtigungsverleiher	invalid_grantor
0LP01	Klasse 0L – Ungültiger Berechtigungsverleiher	invalid_grant_operation
0P000	Klasse 0P – Ungültige Rollenspezifikation	invalid_role_specification
0Z000	Klasse 0Z – Diagnoseausnahme	diagnostics_exception
0Z002	Klasse 0Z – Diagnoseausnahme	stacked_diagnostics_accessed_without_active_handler

Fehlercode	Fehlerklasse	Bedingungsname
20000	Klasse 20 – Fall nicht gefunden	case_not_found
21000	Klasse 21 – Verletzung der Kardinalität	cardinality_violation

Daten-Ausnahmen:

Fehlercode	Fehlerklasse	Bedingungsname
22000	Klasse 22 – Datenausnahme	data_exception
2202E	Klasse 22 – Datenausnahme	array_subscript_error
22021	Klasse 22 – Datenausnahme	character_not_in_repertoire
22008	Klasse 22 – Datenausnahme	datetime_field_overflow
2012	Klasse 22 – Datenausnahme	division_by_zero
22005	Klasse 01 – Warnung	error_in_assignment
2200B	Klasse 01 – Warnung	escape_character_conflict
22022	Klasse 01 – Warnung	indicator_overflow
22015	Klasse 01 – Warnung	interval_feld_overflow
2201E	Klasse 01 – Warnung	invalid_argument_for_logarithm
2201F	Klasse 01 – Warnung	invalid_argument_for_power_function
2201G	Klasse 01 – Warnung	invalid_argument_for_width_bucket_function
22018	Klasse 01 – Warnung	invalid_character_value_for_cast
22007	Klasse 01 – Warnung	invalid_datetime_format

Fehlercode	Fehlerklasse	Bedingungsname
2019	Klasse 01 – Warnung	invalid_escape_character
2200D	Klasse 01 – Warnung	invalid_escape_octet
22025	Klasse 01 – Warnung	invalid_escape_sequence
22P06	Klasse 01 – Warnung	nonstandard_use_of_escape_character
2010	Klasse 01 – Warnung	invalid_indicator_parameter_value
22023	Klasse 01 – Warnung	invalid_parameter_value
2201B	Klasse 01 – Warnung	invalid_regular_expression
2009	Klasse 01 – Warnung	invalid_time_zone_displacement_value
2200C	Klasse 01 – Warnung	invalid_use_of_escape_character
2200G	Klasse 01 – Warnung	most_specific_type_mismatch
22004	Klasse 01 – Warnung	null_value_not_allowed
22002	Klasse 01 – Warnung	null_value_no_indicator_parameter
22003	Klasse 01 – Warnung	numeric_value_out_of_range
22026	Klasse 01 – Warnung	string_data_length_mismatch
22001	Klasse 01 – Warnung	string_data_right_truncation
22011	Klasse 01 – Warnung	substring_error
22027	Klasse 01 – Warnung	trim_error
22024	Klasse 01 – Warnung	unterminated_c_string
2200F	Klasse 01 – Warnung	zero_length_character_string
22P01	Klasse 01 – Warnung	floating_point_exception

Fehlercode	Fehlerklasse	Bedingungsname
22P02	Klasse 01 – Warnung	invalid_text_representation
22P03	Klasse 01 – Warnung	invalid_binary_representation
22P04	Klasse 01 – Warnung	bad_copy_file_format
22P05	Klasse 01 – Warnung	untranslatable_character

Verstöße gegen die Integritätsbeschränkung:

Fehlercode	Fehlerklasse	Bedingungsname
23000	Klasse 23 – Verletzung der Integritätsbeschränkung	integrity_constraint_violation
23001	Klasse 23 – Verletzung der Integritätsbeschränkung	restrict_violation
23502	Klasse 23 – Verletzung der Integritätsbeschränkung	not_null_violation
23503	Klasse 23 – Verletzung der Integritätsbeschränkung	foreign_key_violation
23505	Klasse 23 – Verletzung der Integritätsbeschränkung	unique_verletzung
23514	Klasse 23 – Verletzung der Integritätsbeschränkung	check_violation
24000	Klasse 24 – Ungültiger Cursorstatus	invalid_cursor_state
01004	Klasse 01 – Warnung	string_data_right_truncation
25000	Klasse 25 – Ungültiger Transaktionsstatus	invalid_transaction_state

Fehlercode	Fehlerklasse	Bedingungsname
25001	Klasse 25 – Ungültiger Transaktionsstatus	active_sql_transaction
25002	Klasse 25 – Ungültiger Transaktionsstatus	invalid_transaction_state
25008	Klasse 25 – Ungültiger Transaktionsstatus	held_cursor_requires_same_isolation_level
25003	Klasse 25 – Ungültiger Transaktionsstatus	inappropriate_access_mode_for_branch_transaction
25004	Klasse 25 – Ungültiger Transaktionsstatus	inappropriate_isolation_level_for_branch_transaction
25005	Klasse 25 – Ungültiger Transaktionsstatus	no_active_sql_transaction_for_branch_transaction
25006	Klasse 25 – Ungültiger Transaktionsstatus	read_only_sql_transaction
25007	Klasse 25 – Ungültiger Transaktionsstatus	no_active_sql_transaction_for_branch_transaction
25P01	Klasse 25 – Ungültiger Transaktionsstatus	no_active_sql_transaction
25P02	Klasse 25 – Ungültiger Transaktionsstatus	in_failed_sql_transaction
26000	Klasse 26 – Ungültiger Name der SQL-Anweisung	invalid_sql_statement_name
28000	Klasse 28 – Ungültige Autorisierungsspezifikation	invalid_authorization_specification

Fehlercode	Fehlerklasse	Bedingungsname
2B000	Klasse 2B – Abhängige Berechtigungsdeskriptoren existieren noch	dependent_privege_descriptors_still_exist
2 BP01	Klasse 2B – Abhängige Berechtigungsdeskriptoren existieren noch	dependent_objects_still_exist
2D000	Klasse 2D – Ungültige Transaktionsbeendigung	invalid_transaction_termination
2F000	Klasse 2F – SQL-Routi neausnahme	sql_routine_exception
2F005	Klasse 2F – SQL-Routi neausnahme	function_executed_no_return_statement
2F002	Klasse 2F – SQL-Routi neausnahme	modifying_sql_data_not_permitted
2F003	Klasse 2F – SQL-Routi neausnahme	prohibited_sql_statement_attempted
2F004	Klasse 2F – SQL-Routi neausnahme	reading_sql_data_not_permitted
34000	Klasse 34 – Ungültiger Cursorname	invalid_cursor_name
38000	Klasse 38 – Ausnahme bei externe Routinen	external_routine_exception
38001	Klasse 38 – Ausnahme bei externe Routinen	containing_sql_not_permitted
38002	Klasse 38 – Ausnahme bei externe Routinen	modifying_sql_data_not_permitted

Fehlercode	Fehlerklasse	Bedingungsname
38003	Klasse 38 – Ausnahme bei externe Routinen	prohibited_sql_statement_attempted
38004	Klasse 38 – Ausnahme bei externe Routinen	reading_sql_data_not_permitted
39000	Klasse 39 – Ausnahme beim Aufruf externer Routinen	external_routine_invocation_exception
39001	Klasse 39 – Ausnahme beim Aufruf externer Routinen	invalid_sqlstate_returned
39004	Klasse 39 – Ausnahme beim Aufruf externer Routinen	null_value_not_allowed
39P01	Klasse 39 – Ausnahme beim Aufruf externer Routinen	trigger_protocol_violated
39P02	Klasse 39 – Ausnahme beim Aufruf externer Routinen	srf_protocol_violated
3D000	Klasse 3D – Ungültiger Katalogname	invalid_catalog_name
3F000	Klasse 3F – Ungültiger Schemaname	invalid_schema_name
42000	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsr egel	syntax_error_or_access_rule_violation
42601	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsr egel	syntax_error

Fehlercode	Fehlerklasse	Bedingungsname
42501	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	insufficient_privilege
42846	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	cannot_coerce
42803	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	grouping_error
42830	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_foreign_key
42602	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_name
42622	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	name_too_long
42939	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	reserved_name
42804	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	datatype_mismatch
42P18	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	undeterminate_datatype

Fehlercode	Fehlerklasse	Bedingungsname
42809	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	wrong_object_type
42703	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	undefined_column
42883	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	undefined_function
42P01	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	undefined_table
42P02	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	undefined_parameter
42704	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	undefined_object
42701	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	duplicate_column
42P03	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	duplicate_cursor
42P04	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	duplicate_database

Fehlercode	Fehlerklasse	Bedingungsname
42723	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	duplicate_function
42P05	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	duplicate_prepared_statement
42P06	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	duplicate_schema
42P07	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	duplicate_table
42712	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	duplicate_alias
42710	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	duplicate_object
42702	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	ambiguous_column
42725	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	ambiguous_function
42P08	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	ambiguous_parameter

Fehlercode	Fehlerklasse	Bedingungsname
42P09	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	ambiguous_alias
42P10	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_column_reference
42611	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_column_definition
42P11	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_cursor_definition
42P12	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_database_definition
42P13	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_function_definition
42P14	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_prepared_statement_definition
42P15	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_schema_definition
42P16	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_table_definition

Fehlercode	Fehlerklasse	Bedingungsname
42P17	Klasse 42 – Syntaxfehler oder Verstoß gegen die Zugriffsregel	invalid_object_definition
44000	Klasse 44 – WITH-CHECK-OPTION-Verstoß	with_check_option_violation
53000	Klasse 53 – Unzureichende Ressourcen	insufficient_resources
53100	Klasse 53 – Unzureichende Ressourcen	disk_full
53200	Klasse 53 – Unzureichende Ressourcen	out_of_memory
53300	Klasse 53 – Unzureichende Ressourcen	too_many_connections
54000	Klasse 54 – Programmlimit überschritten	program_limit_exceeded
54001	Klasse 54 – Programmlimit überschritten	statement_too_complex
54011	Klasse 54 – Programmlimit überschritten	too_many_columns
54023	Klasse 54 – Programmlimit überschritten	too_many_arguments
55000	Klasse 55 – Objekt nicht im Voraussetzungstatus	object_not_in_prerequisite_state
5506	Klasse 55 – Objekt nicht im Voraussetzungstatus	object_in_use

Fehlercode	Fehlerklasse	Bedingungsname
55P02	Klasse 55 – Objekt nicht im Voraussetzungstatus	cant_change_runtime_param
55P03	Klasse 55 – Objekt nicht im Voraussetzungstatus	lock_not_available
57000	Klasse 57 – Bedienereingriff	operator_intervention
57014	Klasse 57 – Bedienereingriff	query_cancelled
57P01	Klasse 57 – Bedienereingriff	admin_shutdown
57P02	Klasse 57 – Bedienereingriff	crash_shutdown
57P03	Klasse 57 – Bedienereingriff	cannot_connect_now
58000	Klasse 58 – Systemfeh ler (Fehler außerhalb von PostgreSQL)	system_error
58030	Klasse 58 – Systemfeh ler (Fehler außerhalb von PostgreSQL)	io_Fehler
58P01	Klasse 58 – Systemfeh ler (Fehler außerhalb von PostgreSQL)	undefined_file
58P02	Klasse 58 – Systemfeh ler (Fehler außerhalb von PostgreSQL)	duplicate_file
F0000	Klasse F0 – Fehler in der Konfigurationsdatei	duplicate_file
F0001	Klasse F0 – Fehler in der Konfigurationsdatei	lock_file_exists

Fehlercode	Fehlerklasse	Bedingungsname
P0000	Klasse P0 – PL/PgSQL-Fehler	plpgsql_error
P0001	Klasse P0 – PL/PgSQL-Fehler	raise_exception
P0002	Klasse P0 – PL/PgSQL-Fehler	no_data_found
P0003	Klasse P0 – PL/PgSQL-Fehler	too_many_rows
XX000	Klasse XX – Interner Fehler	internal_error
XX001	Klasse XX – Interner Fehler	data_corrupted
XX002	Klasse XX – Interner Fehler	index_corrupted

Amazon-Redshift-RSQL-Umgebungsvariablen

Amazon Redshift RSQL kann Umgebungsvariablen verwenden, um Standardparameterwerte auszuwählen.

RSPASSWORD

> **Important**
>
> Wir empfehlen aus Sicherheitsgründen nicht, diese Umgebungsvariable zu verwenden, da einige Betriebssysteme Nicht-Administratoren erlauben, Prozessumgebungsvariablen anzuzeigen.

Legt das Passwort fest, das Amazon Redshift RSQL zum Herstellen einer Verbindung mit Amazon Redshift verwenden soll. Diese Umgebungsvariable erfordert Amazon Redshift RSQL 1.0.4 und höher.

RSQL priorisiert RSPASSWORD, wenn es festgelegt ist. Wenn RSPASSWORD nicht festgelegt ist und Sie eine Verbindung mit einem DSN herstellen, entnimmt RSQL das Passwort den Parametern der DSN-Datei. Wenn RSPASSWORD nicht festgelegt ist und Sie keinen DSN verwenden, gibt RSQL nach dem Versuch, eine Verbindung herzustellen, eine Passwortaufforderung an.

Im Folgenden finden Sie ein Beispiel für das Festlegen eines RSPASSWORD:

```
export RSPASSWORD=TestPassw0rd
```

Verbinden mit SQL Workbench/J

Sie können eine Verbindung zu einer Datenbank mithilfe von SQL Workbench/J herstellen, einem kostenlosen plattformübergreifenden SQL-Abfrage-Tool, das nicht von einem bestimmten DBMS abhängig ist.

Von Amazon Redshift werden keine SQL-Client-Tools von Drittanbietern bereitgestellt oder installiert. Daher müssen Sie Tools, die Sie mit Ihrer Datenbank verwenden möchten, selbst installieren. Um SQL Workbench/J zu installieren, folgen Sie den Anweisungen in der SQL-Workbench/J-Dokumentation (SQL Workbench/J). Im Allgemeinen gehen Sie wie folgt vor, um SQL Workbench/J zu verwenden:

- Lesen Sie die Softwarelizenz zu SQL Workbench/J.
- Laden Sie das entsprechende SQL-Workbench/J-Paket für Ihr Betriebssystem auf Ihren Client-Computer oder in Ihre Amazon-EC2-Instance herunter.
- Installieren Sie SQL Workbench/J auf Ihrem System.

  Sorgen Sie dafür, dass Java Runtime Environment (JRE) auf Ihrem System installiert ist. Stellen Sie sicher, dass Sie die richtige Version der JRE installiert haben, die durch den SQL Workbench/J-Client vorausgesetzt wird.
- Stellen Sie eine Verbindung mit Ihrer Datenbank über eine JDBC-Verbindung in SQL Workbench/J her.

  Stellen Sie sicher, dass Ihr Client-Computer oder Ihre Amazon-EC2-Instance über den empfohlenen Amazon-Redshift-JDBC-Treiber verfügt. Links zum Herunterladen der neuesten Treiber finden Sie unter Herunterladen von Version 2.1 des JDBC-Treibers für Amazon Redshift. Stellen Sie außerdem sicher, dass Ihre Firewall-Einstellungen so konfiguriert sind, dass der Zugriff auf Ihre Datenbank zugelassen wird. Weitere Informationen finden Sie unter Schritt 4: Autorisieren des Zugriffs auf den Cluster im Amazon Redshift Getting Started Guide.
- Erstellen Sie in SQL Workbench/J ein neues Verbindungsprofil, das den Amazon-Redshift-Treiber verwendet.

Stellen Sie programmgesteuert Connect zu Ihrem Data Warehouse her

Informationen zu Tools zum Erstellen von Anwendungen für die Verbindung mit Ihrem Data Warehouse finden Sie unter Tools zum Entwickeln in AWS.

Verwenden eines Authentifizierungsprofils zur Verbindung mit Amazon Redshift

Wenn Sie viele Verbindungen zu Amazon Redshift haben, kann es schwierig sein, Einstellungen für alle zu verwalten. Oft verwendet jede JDBC- oder ODBC-Verbindung bestimmte Konfigurationsoptionen. Mithilfe eines Authentifizierungsprofils können Sie Verbindungsoptionen zusammen speichern. Auf diese Weise können Ihre Benutzer ein Profil auswählen, mit dem Sie sich verbinden, und die Verwaltung von Einstellungen für einzelne Optionen vermeiden. Profile können für verschiedene Szenarien und Benutzertypen gelten.

Nachdem Sie ein Authentifizierungsprofil erstellt haben, können Benutzer das ready-to-use Profil zu einer Verbindungszeichenfolge hinzufügen. So können sie eine Verbindung zu Amazon Redshift mit den richtigen Einstellungen für jede Rolle und jeden Anwendungsfall herstellen.

Informationen zur Amazon Redshift Redshift-API finden Sie unter CreateAuthenticationProfile.

Erstellen eines Authentifizierungsprofils

Mithilfe von AWS CLI erstellen Sie ein Authentifizierungsprofil mit dem `create-authentication-profile` Befehl. Dies setzt voraus, dass Sie einen vorhandenen Amazon-Redshift-Cluster und eine vorhandene Datenbank besitzen. Ihre Anmeldeinformationen müssen über die Berechtigung verfügen, sich mit der Amazon-Redshift-Datenbank zu verbinden, und die Berechtigung zum Abrufen des Authentifizierungsprofils haben. Sie geben die Konfigurationsoptionen als JSON-Zeichenfolge an oder verweisen auf eine Datei, die Ihre JSON-Zeichenfolge enthält.

```
create-authentication-profile --authentication-profile-name<value: String> --
authentication-profile-content<value: String>
```

Im folgenden Beispiel wird ein Profil namens `ExampleProfileName` erstellt. Hier können Sie Schlüssel und Werte hinzufügen, die Ihren Clusternamen und andere Optionseinstellungen als JSON-Zeichenfolge definieren.

```
create-authentication-profile --authentication-profile-name "ExampleProfileName"
 --authentication-profile-content "{\"AllowDBUserOverride\":\"1\",\"Client_ID
```

```
\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID\",\"AutoCreate\":false,
\"enableFetchRingBuffer\":true,\"databaseMetadataCurrentDbOnly\":true}"
}
```

Dieser Befehl erstellt das Profil mit den angegebenen JSON-Einstellungen. Folgendes wird zurückgegeben, was darauf hinweist, dass das Profil erstellt wurde.

```
{"AuthenticationProfileName": "ExampleProfileName",
"AuthenticationProfileContent": "{\"AllowDBUserOverride\":\"1\",
\"Client_ID\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID\",
\"AutoCreate\":false,\"enableFetchRingBuffer\":true,
\"databaseMetadataCurrentDbOnly\":true}" }
```

Einschränkungen und Kontingente für das Erstellen eines Authentifizierungsprofils

Jeder Kunde hat ein Kontingent von zehn (10) Authentifizierungsprofilen.

Bei Authentifizierungsprofilen können bestimmte Fehler auftreten. Zum Beispiel wenn Sie ein neues Profil mit einem vorhandenen Namen erstellen oder wenn Sie Ihr Profilkontingent überschreiten. Weitere Informationen finden Sie unter CreateAuthenticationProfile.

Sie können bestimmte Optionsschlüssel und Werte für JDBC-, ODBC- und Python-Verbindungszeichenfolgen nicht im Authentifizierungsprofilspeicher speichern:

- `AccessKeyID`
- `access_key_id`
- `SecretAccessKey`
- `secret_access_key_id`
- `PWD`
- `Password`
- `password`

Sie können den Schlüssel oder den Wert `AuthProfile` nicht im Profilspeicher für JDBC- oder ODBC-Verbindungszeichenfolgen speichern. Bei Python-Verbindungen können Sie `auth_profile` nicht speichern.

Authentifizierungsprofile werden in Amazon DynamoDB gespeichert und von verwaltet. AWS

Arbeiten mit Authentifizierungsprofilen

Nachdem Sie ein Authentifizierungsprofil erstellt haben, können Sie den Profilnamen als Verbindungsoption für JDBC-Version 2.0 `AuthProfile` angeben. Mit dieser Verbindungsoption werden die gespeicherten Einstellungen abgerufen.

```
jdbc:redshift:iam://endpoint:port/database?AuthProfile=<Profile-
Name>&AccessKeyID=<Caller-Access-Key>&SecretAccessKey=<Caller-Secret-Key>
```

Im Folgenden wird ein Beispiel für eine JDBC-URL-Zeichenfolge gezeigt:

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
AuthProfile="ExampleProfile"&AccessKeyID="AKIAIOSFODNN7EXAMPLE"&SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

Geben Sie sowohl `AccessKeyID` als auch `SecretAccessKey` in der JDBC-URL zusammen mit dem Namen des Authentifizierungsprofils an.

Sie können die Konfigurationsoptionen auch durch Semikolon-Trennzeichen trennen, wie im folgenden Beispiel mit Optionen für die Protokollierung.

```
jdbc:redshift:iam://my_redshift_end_point:5439/dev?LogLevel=6;LogPath=/
tmp;AuthProfile=my_profile;AccessKeyID="AKIAIOSFODNN7EXAMPLE";SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

> **Note**
>
> Fügen Sie dem Authentifizierungsprofil keine vertraulichen Informationen hinzu. Speichern Sie z. B. keine `AccessKeyID`- oder `SecretAccessKey`-Werte in einem Authentifizierungsprofil. Der Authentifizierungsprofilspeicher verfügt über Regeln, um das Speichern geheimer Schlüssel zu verbieten. Sie erhalten eine Fehlermeldung, wenn Sie versuchen, einen Schlüssel und einen Wert zu speichern, der mit sensiblen Informationen verknüpft ist.

Authentifizierungsprofile abrufen

Um vorhandene Authentifizierungsprofile aufzulisten, rufen Sie den folgenden Befehl auf.

```
describe-authentication-profiles --authentication-profile-name <value: String>
```

Das folgende Beispiel zeigt zwei abgerufene Profile. Alle Profile werden zurückgegeben, wenn Sie keinen Profilnamen angeben.

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

Beheben von Problemen mit Verbindungen in Amazon Redshift

Wenn Sie Probleme haben, aus einem SQL-Client-Tool Verbindungen mit Ihrem Cluster herzustellen, gibt es mehrere Dinge, die Sie überprüfen können, um das Problem einzuengen. Wenn Sie SSL oder Serverzertifikate verwenden, entfernen Sie zunächst diese Komplexität, während Sie das Verbindungsproblem untersuchen. Fügen Sie diese Komponenten wieder hinzu, wenn Sie eine Lösung gefunden haben. Weitere Informationen finden Sie unter Konfigurieren von Sicherheitsoptionen für Verbindungen.

> **Important**
>
> Amazon Redshift hat die Verwaltung von SSL-Zertifikaten verändert. Wenn Sie Probleme mit der Verbindungsherstellung mit SSL haben, müssen Sie unter Umständen die aktuellen vertrauenswürdigen CA-Stammzertifikate aktualisieren. Weitere Informationen finden Sie unter Umstellung auf ACM-Zertifikate für SSL-Verbindungen.

Im folgenden Abschnitt werden einige beispielhafte Fehlermeldungen und mögliche Lösungen für Verbindungsprobleme gezeigt. Da die verschiedenen SQL-Client-Tools verschiedene Fehlermeldungen anzeigen, ist diese Liste nicht vollständig. Sie sollte jedoch einen guten Ausgangspunkt für die Behebung von Problemen darstellen.

Themen

- Herstellen von Verbindungen von außerhalb von Amazon EC2 – Problem mit Firewall-Zeitüberschreitung
- Verbindung wird zurückgewiesen oder schlägt fehl
- Client und Treiber sind nicht kompatibel
- Abfragen scheinen zu hängen und erreichen manchmal den Cluster nicht
- Festlegen des JDBC-Parameters für die Abrufgröße

Herstellen von Verbindungen von außerhalb von Amazon EC2 – Problem mit Firewall-Zeitüberschreitung

Beispiel für ein Problem

Ihre Client-Verbindung mit der Datenbank scheint zu hängen oder Zeitüberschreitungen zu unterliegen, wenn lange Abfragen wie COPY-Befehle ausgeführt werden. Wenn dies der Fall ist, sehen Sie möglicherweise in der Amazon-Redshift-Konsole, dass die Abfrage abgeschlossen ist, aber das Client-Tool scheint die Abfrage noch nicht abgeschlossen zu haben. Je nachdem, wann die Verbindung unterbrochen wurde, fehlen möglicherweise Abfrageergebnisse oder sind unvollständig.

Mögliche Lösungen

Dieses Problem tritt auf, wenn Sie eine Verbindung zu Amazon Redshift von einer anderen Maschine als einer Amazon-EC2-Instance herstellen. In diesem Fall werden Leerlaufverbindungen durch eine Zwischennetzwerkkomponente, z. B. eine Firewall, nach einem Inaktivitätszeitraum beendet. Dieses Verhalten ist typisch, wenn Sie sich über ein Virtual Private Network (VPN) oder Ihr lokales Netzwerk anmelden.

Um diese Zeitüberschreitungen zu vermeiden, werden folgende Änderungen empfohlen:

- Erhöhen Sie die Client-Systemwerte, die TCP/IP-Zeitüberschreitungen betreffen. Sie sollten diese Änderungen auf dem Computer ausführen, den Sie für die Verbindung mit Ihrem Cluster verwenden. Der Zeitraum für die Zeitüberschreitung sollte an Ihren Client und Ihr Netzwerk angepasst sein. Weitere Informationen finden Sie unter Ändern der TCP/IP-Einstellungen für Zeitüberschreitungen.
- Optional können Sie das Keepalive-Verhalten auf DSN-Ebene festlegen. Weitere Informationen finden Sie unter Ändern der DSN-Einstellungen für Zeitüberschreitungen.

Ändern der TCP/IP-Einstellungen für Zeitüberschreitungen

Um die TCP/IP-Einstellungen für Zeitüberschreitungen zu ändern, konfigurieren Sie die Einstellungen für Zeitüberschreitungen entsprechend dem Betriebssystem, das Sie für Verbindung mit Ihrem Cluster verwenden.

- Linux – Wenn Ihr Client unter Linux ausgeführt wird, führen Sie den folgenden Befehl als Root-Benutzer aus, um die Timeout-Einstellungen für die aktuelle Sitzung zu ändern:

  ```
  /sbin/sysctl -w net.ipv4.tcp_keepalive_time=200 net.ipv4.tcp_keepalive_intvl=200
   net.ipv4.tcp_keepalive_probes=5
  ```

  Um die Einstellungen dauerhaft festzulegen, erstellen Sie die Datei `/etc/sysctl.conf` mit den folgenden Werten oder aktualisieren sie entsprechend und starten anschließend Ihr System neu.

  ```
  net.ipv4.tcp_keepalive_time=200
  net.ipv4.tcp_keepalive_intvl=200
  net.ipv4.tcp_keepalive_probes=5
  ```

- Windows — Wenn Ihr Client unter Windows läuft, bearbeiten Sie die Werte für die folgenden Registrierungseinstellungen unter HKEY_LOCAL_MACHINE\ SYSTEM\\ Services\ Tcpip\ ParametersCurrentControlSet\:
  - KeepAliveTime: 30000
  - KeepAliveInterval: 1000
  - TcpMaxDataRetransmissions: 10

  Diese Einstellungen verwenden den DWORD-Datentyp. Wenn die am Registrierungspfad nicht vorhanden sind, können Sie die Einstellungen erstellen und diese empfohlenen Werte angeben. Weitere Informationen zum Bearbeiten der Windows-Registrierung finden Sie in der Windows-Dokumentation.

  Nachdem Sie diese Werte festgelegt haben, starten Sie Ihren Computer neu, damit die Änderungen wirksam werden.

- Mac – Wenn Ihr Client auf einem Mac ausgeführt wird, führen Sie die folgenden Befehle aus, um die Timeout-Einstellungen für die aktuelle Sitzung zu ändern:

```
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
```

Um die Einstellungen dauerhaft festzulegen, erstellen Sie die Datei `/etc/sysctl.conf` mit den folgenden Werten:

```
net.inet.tcp.keepidle=200000
net.inet.tcp.keepintvl=200000
net.inet.tcp.keepinit=200000
net.inet.tcp.always_keepalive=1
```

Starten Sie Ihren Computer neu und führen Sie anschließend die folgenden Befehle aus, um zu überprüfen, ob die Werte festgelegt wurden.

```
sysctl net.inet.tcp.keepidle
sysctl net.inet.tcp.keepintvl
sysctl net.inet.tcp.keepinit
sysctl net.inet.tcp.always_keepalive
```

Ändern der DSN-Einstellungen für Zeitüberschreitungen

Sie können das Keepalive-Verhalten auf DSN-Ebene festlegen, wenn Sie dies wünschen. Sie tun dies, indem Sie die folgenden Parameter in der odbc.ini-Datei hinzufügen oder ändern:

KeepAlivesCount

Die Anzahl der TCP-Keepalive-Pakete, die verloren gehen dürfen, bevor die Verbindung als abgebrochen betrachtet wird.

KeepAlivesIdle

Die Anzahl der Inaktivitätsekunden, bevor der Treiber ein TCP-Keepalive-Paket sendet.

KeepAlivesInterval

Die Anzahl der Sekunden zwischen den einzelnen TCP-Keepalive-Übertragungen.

In Windows ändern Sie diese Parameter in der Registrierung, indem Sie Schlüssel in HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI*Ihr_DSN* hinzufügen oder ändern. Unter Linux und macOS fügen Sie diese Parameter im DSN-Zieleintrag direkt in der odbc.ini-Datei ein oder ändern sie dort. Weitere Informationen zum Ändern der odbc.ini-Datei auf Linux- und macOs-Computern finden Sie unter Verwenden Sie einen ODBC-Treibermanager, um den Treiber unter Linux und macOS X zu konfigurieren.

Wenn diese Parameter nicht vorhanden sind oder den Wert 0 aufweisen, verwendet das System die für TCP/IP angegebenen Keepalive-Parameter, um das DSN-Keepalive-Verhalten festzulegen. Unter Windows finden Sie die TCP/IP-Parameter in der Registrierung in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\`. Unter Linux und macOS befinden sich die TCP/IP-Parameter in der sysctl.conf-Datei.

Verbindung wird zurückgewiesen oder schlägt fehl

Fehlerbeispiele

- „Fehler bei der Herstellung einer Verbindung mit *<endpoint>*."
- „Keine Verbindung mit dem Server möglich: Zeitüberschreitung für die Verbindung. Wird der Server auf dem Host *'<endpoint>'* ausgeführt und werden TCP/IP-Verbindungen auf Port *'<port>'* akzeptiert?"
- „Verbindung zurückgewiesen. Überprüfen Sie, ob Host-Name und Port korrekt sind und der Postmaster TCP/IP-Verbindungen akzeptiert."

Mögliche Lösungen

Wenn Sie eine Fehlermeldung erhalten, die besagt, dass keine Verbindung hergestellt werden kann, bedeutet dies im Allgemeinen, dass es ein Problem mit der Berechtigung für den Zugriff auf den Cluster gibt.

Um sich von einem Client-Tool außerhalb des Netzwerks, in dem sich der Cluster befindet, mit dem Cluster zu verbinden, fügen Sie der Sicherheitsgruppe des Clusters eine Eingangsregel hinzu. Die Regelkonfiguration hängt davon ab, ob der Amazon-Redshift-Cluster in einer Virtual Private Cloud (VPC) erstellt wurde:

- Wenn Sie Ihren Amazon-Redshift-Cluster in einer Virtual Private Cloud (VPC) basierend auf Amazon VPC erstellt haben, fügen Sie in Amazon VPC eine Eingangsregel der VPC-Sicherheitsgruppe hinzu, die die Client-CIDR/IP-Adresse angibt. Weitere Informationen zum

Konfigurieren von VPC-Sicherheitsgruppen für Ihren Cluster sowie zu öffentlich zugänglichen Optionen finden Sie unter Verwaltung von Clustern in einer VPC.

- Wenn Sie Ihren Amazon-Redshift-Cluster außerhalb einer VPC erstellt haben, fügen Sie Ihre Client-CIDR/IP-Adresse der Cluster-Sicherheitsgruppe in Amazon Redshift hinzu. Weitere Informationen zum Konfigurieren von Cluster-Sicherheitsgruppen finden Sie unter Amazon-Redshift-Cluster-Sicherheitsgruppen.

Wenn Sie versuchen, sich von einem Client-Tool in einer Amazon-EC2-Instance aus mit dem Cluster zu verbinden, fügen Sie ebenfalls eine Zugangsregel hinzu. Fügen Sie in diesem Fall der Cluster-Sicherheitsgruppe eine Regel hinzu. Die Regel muss die Amazon-EC2-Sicherheitsgruppe angeben, die der Amazon-EC2-Instance des Client-Tools zugeordnet ist.

In einigen Fällen haben Sie möglicherweise eine Ebene zwischen dem Client und dem Server, z. B. eine Firewall. Stellen Sie in diesen Fällen sicher, dass die Firewall eingehende Verbindungen über den Port akzeptiert, den Sie für Ihren Cluster konfiguriert haben.

Client und Treiber sind nicht kompatibel

Fehlerbeispiel

„Die Architektur von Treiber und Anwendung im angegebenen DSN stimmt nicht überein.“

Mögliche Lösung

Wenn Sie versuchen, eine Verbindung herzustellen, und einen Fehler bezüglich einer Architekturunstimmigkeit erhalten, bedeutet dies, dass das Client-Tool und der Treiber nicht kompatibel sind. Dies tritt auf, wenn ihre Systemarchitektur nicht übereinstimmt. Dies kann beispielsweise vorkommen, wenn Sie ein 32-Bit-Client-Tool verwenden, jedoch die 64-Bit-Version des Treibers installiert haben. Manchmal können 64-Bit-Client-Tools 32-Bit-Treiber verwenden. Sie können 32-Bit-Anwendungen jedoch nicht mit 64-Bit-Treibern verwenden. Stellen Sie sicher, dass Treiber und Client-Tool dieselbe Version der Systemarchitektur verwenden.

Abfragen scheinen zu hängen und erreichen manchmal den Cluster nicht

Beispiel für ein Problem

Sie haben ein Problem mit dem Abschluss von Abfragen. Die Abfragen werden anscheinend ausgeführt, hängen jedoch im SQL-Client-Tool. Manchmal erreichen die Abfragen den Cluster anscheinend nicht, beispielsweise in Systemtabellen oder in der Amazon-Redshift-Konsole.

Mögliche Lösung

Dieses Problem kann aufgrund von Paketverlusten auftreten. In diesem Fall gibt es einen Unterschied in der maximalen Größe der Übertragungseinheit (MTU) im Netzwerkpfad zwischen zwei Internet Protocol (IP) Hosts. Der MTU-Wert legt die maximale Größe für die Übertragung eines Pakets in einem Ethernet-Frame über eine Netzwerkverbindung in Bytes fest. In AWS unterstützen einige Amazon EC2 EC2-Instance-Typen eine MTU von 1500 (Ethernet v2-Frames) und andere Instance-Typen unterstützen eine MTU von 9001 (TCP/IP-Jumbo-Frames).

Um Probleme im Zusammenhang mit unterschiedlichen MTU-Größen zu vermeiden, wird eine der folgenden Aktionen empfohlen:

- Wenn Ihr Cluster die EC2-VPC-Plattform verwendet, konfigurieren Sie die Amazon-VPC-Sicherheitsgruppe mit einer ICMP-Regel (Inbound Custom Internet Control Message Protocol), die zurückgibt `Destination Unreachable`. Die Regel weist also den Ursprungshost an, die niedrigste MTU-Größe entlang des Netzwerkpfades zu verwenden. Details zu diesem Ansatz finden Sie unter Konfigurieren von Sicherheitsgruppen, um ICMP „Ziel kann nicht erreicht werden“ zuzulassen.
- Wenn Ihr Cluster die EC2-Classic-Plattform verwendet oder Sie die ICMP-Eingangsregel nicht zulassen können, deaktivieren Sie TCP/IP-Jumbo-Frames, so dass Ethernet v2-Frames verwendet werden. Details zu diesem Ansatz finden Sie unter Konfigurieren der MTU einer Instance.

Konfigurieren von Sicherheitsgruppen, um ICMP „Ziel kann nicht erreicht werden“ zuzulassen

Wenn es im Netzwerk zwischen zwei Hosts unterschiedliche MTU-Größen gibt, stellen Sie zunächst sicher, dass Ihre Netzwerkeinstellungen die Pfad-MTU-Erkennung (Path MTU Discovery, PMTUD) nicht blockieren. PMTUD ermöglicht dem empfangenden Host, dem sendenden Host mit der folgenden ICMP-Meldung zu antworten: `Destination Unreachable: fragmentation needed and DF set (ICMP Type 3, Code 4)`. Diese Meldung weist den sendenden Host an, die kleinste MTU-Größe zu verwenden, die auf dem Netzwerkpfad zulässig ist, und die Anforderung neu zu senden. Ohne diese Verhandlung können Paketverluste auftreten, da die Anforderung für den empfangenden Host zu groß ist, um sie akzeptieren zu können. Weitere Informationen zu dieser ICMP-Meldung finden Sie unter RFC792 auf der Website Internet Engineering Task Force (IETF).

Wenn Sie diese ICMP-Eingangsregel nicht ausdrücklich für Ihre Amazon-VPC-Sicherheitsgruppe konfigurieren, wird PMTUD blockiert. Bei Sicherheitsgruppen handelt es sich um virtuelle Firewalls AWS, die Regeln für eingehenden und ausgehenden Datenverkehr zu einer Instance festlegen. Informationen zu Amazon-Redshift-Cluster-Sicherheitsgruppen finden Sie unter Amazon-Redshift-

Cluster-Sicherheitsgruppen. Im Fall von Clustern, die die EC2-VPC-Plattform verwenden, verwendet Amazon Redshift VPC-Sicherheitsgruppen, um Datenverkehr zum Cluster zuzulassen oder abzulehnen. Standardmäßig sind die Sicherheitsgruppen restriktiv und lehnen jeden eingehenden Datenverkehr ab. Informationen zum Festlegen der Regeln für ein- und ausgehenden Datenverkehr für EC2-Classic- oder EC2-VPC-Instances finden Sie unter Unterschiede zwischen Instances in EC2-Classic und einer VPC im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Weitere Informationen zum Hinzufügen von Regeln zu VPC-Sicherheitsgruppen finden Sie unter Verwalten von VPC-Sicherheitsgruppen für einen Cluster. Weitere Informationen zu spezifischen PMTUD-Einstellungen, die in dieser Regel erforderlich sind, finden Sie unter Pfad-MTU-Erkennung im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Konfigurieren der MTU einer Instance

In einigen Fällen verwendet Ihr Cluster möglicherweise die EC2-Classic-Plattform, oder Sie können die benutzerdefinierte ICMP-Regel für eingehenden Datenverkehr nicht zulassen. In diesen Fällen wird empfohlen, die MTU auf der Netzwerkschnittstelle (NIC) der EC2-Instances, von denen Sie eine Verbindung mit dem Amazon-Redshift-Cluster herstellen, auf 1500 zu setzen. Durch diese Einstellung werden TCP/IP-Jumbo-Frames deaktiviert, um sicherzustellen, dass Verbindungen stets dieselbe Paketgröße verwenden. Diese Option reduziert den maximalen Netzwerkdurchsatz für die Instance insgesamt und nicht nur für Verbindungen mit Amazon Redshift. Weitere Informationen finden Sie in den folgenden Verfahren.

So legen Sie die MTU in einem Microsoft Windows-Betriebssystem fest

Wenn Ihr Client in einem Microsoft Windows-Betriebssystem ausgeführt wird, können Sie den MTU-Wert für den Ethernet-Adapter anzeigen und festlegen, indem Sie den Befehl `netsh` verwenden.

1. Führen Sie den folgenden Befehl aus, um den aktuellen MTU-Wert zu ermitteln:

   ```
   netsh interface ipv4 show subinterfaces
   ```

2. Überprüfen Sie den `MTU`-Wert für den `Ethernet`-Adapter in der Ausgabe.
3. Wenn der Wert nicht `1500` ist, führen Sie den folgenden Befehl aus, um ihn festzulegen:

   ```
   netsh interface ipv4 set subinterface "Ethernet" mtu=1500 store=persistent
   ```

   Nachdem Sie diesen Wert festgelegt haben, starten Sie Ihren Computer neu, damit die Änderungen wirksam werden.

So legen Sie die MTU in einem Linux-Betriebssystem fest

Wenn Ihr Client in einem Linux-Betriebssystem ausgeführt wird, können Sie den MTU-Wert für den Ethernet-Adapter anzeigen und festlegen, indem Sie den Befehl `ip` verwenden.

1. Führen Sie den folgenden Befehl aus, um den aktuellen MTU-Wert zu ermitteln:

```
$ ip link show eth0
```

2. Überprüfen Sie den Wert nach `mtu` in der Ausgabe.
3. Wenn der Wert nicht `1500` ist, führen Sie den folgenden Befehl aus, um ihn festzulegen:

```
$ sudo ip link set dev eth0 mtu 1500
```

So legen Sie die MTU in einem Mac-Betriebssystem fest

- Folgen Sie den Anweisungen auf der Supportwebsite von MacOS zu `How to change the MTU for troubleshooting purposes`. Weitere Informationen finden Sie auf der Supportwebsite.

Festlegen des JDBC-Parameters für die Abrufgröße

Der JDBC-Treiber stellt bei Abfragen alle Ergebnisse auf einmal zusammen. Wenn Sie versuchen, eine große Ergebnismenge über eine JDBC-Verbindung abzurufen, kann es daher zu einem clientseitigen Fehler kommen. out-of-memory Damit Ihr Client Ergebnismengen stapelweise statt in einem einzigen Abruf abrufen kann, legen Sie den Parameter all-or-nothing JDBC-Abrufgröße in Ihrer Client-Anwendung fest.

> **Note**
>
> Abrufgröße wird für ODBC nicht unterstützt

Legen Sie die Abrufgröße auf den höchsten Wert fest, der nicht zu Fehlern aufgrund von unzureichendem Arbeitsspeicher führt, um die Leistung zu optimieren. Wenn der Wert für die Abrufgröße kleiner gewählt wird, führt dies zu mehr Übertragungsvorgängen zwischen Server und Client, was die Ausführungszeit vergrößert. Der Server reserviert Ressourcen wie den WLM-

Abfrageplatz und den zugehörigen Arbeitsspeicher, bis der Client die Ergebnismenge abruft oder die Abfrage abgebrochen wird. Wenn die Abrufgröße richtig eingestellt ist, werden diese Ressourcen schneller wieder freigegeben und sind für andere Abfragen verfügbar.

> **Note**
>
> Wenn Sie große Datensätze extrahieren müssen, empfehlen wir, eine UNLOAD-Anweisung zu verwenden, um die Daten an Amazon S3 zu übertragen. Wenn Sie UNLOAD verwenden, arbeiten die Datenverarbeitungsknoten parallel, um die Übertragung der Daten zu beschleunigen.

Weitere Informationen zum Festlegen des Parameters für die JDBC-Abrufgröße finden Sie unter Getting results based on a cursor in der PostgreSQL-Dokumentation.

Verwenden der Amazon Redshift Data API

Sie können über die integrierte Amazon Redshift Data API auf Ihre Amazon-Redshift-Datenbank zugreifen. Mithilfe dieser API können Sie mit Webservice-basierten Anwendungen, einschließlich AWS Lambda SageMaker Amazon-Notebooks und, auf Amazon Redshift-Daten zugreifen. AWS Cloud9 Weitere Informationen zu diesen Anwendungen finden Sie AWS Lambdaunter Amazon SageMaker und AWS Cloud9.

Die Data API erfordert keine persistente Verbindung zu Ihrer Datenbank. Stattdessen bietet es einen sicheren HTTP-Endpunkt und die Integration mit AWS SDKs. Über den Endpunkt können Sie SQL-Anweisungen ausführen, ohne Verbindungen zu verwalten. Aufrufe der Data API erfolgen asynchron.

Die Daten-API verwendet entweder in gespeicherten Anmeldeinformationen AWS Secrets Manager oder temporäre Datenbankanmeldeinformationen. Bei keiner der Autorisierungsmethoden müssen Sie Passwörter in den API-Aufrufen übergeben. Weitere Informationen zu AWS Secrets Manager finden Sie unter Was ist AWS Secrets Manager? im AWS Secrets Manager Benutzerhandbuch.

Weitere Informationen zu den Data-API-Vorgängen finden Sie in der Amazon-Redshift-Data-API-Referenz.

Arbeiten mit der Amazon Redshift Data API

Bevor Sie die Amazon Redshift Data API verwenden, überprüfen Sie die folgenden Schritte:

1. Ermitteln Sie, ob Sie als Aufrufer der Data API autorisiert sind. Weitere Informationen zur -Autorisierung finden Sie unter Autorisieren des Zugriffs auf die Amazon Redshift Data API.
2. Ermitteln Sie, ob Sie planen, die Data API mit Authentifizierungsanmeldeinformationen von Secrets Manager oder temporären Anmeldeinformationen aufzurufen. Weitere Informationen finden Sie unter Auswählen der Anmeldeinformationen für die Datenbankauthentifizierung beim Aufrufen der Amazon Redshift Data API.
3. Richten Sie ein Secret ein, wenn Sie Secrets Manager für die Authentifizierungsanmeldeinformationen verwenden. Weitere Informationen finden Sie unter Speichern von Datenbankanmeldedaten in AWS Secrets Manager.
4. Beachten Sie die Punkte und Einschränkungen, die beim Aufrufen der Data API zu berücksichtigen sind. Weitere Informationen finden Sie unter Wichtige Punkte beim Aufrufen der Amazon Redshift Data API.
5. Rufen Sie die Daten-API über AWS Command Line Interface (AWS CLI), über Ihren eigenen Code oder mithilfe des Abfrage-Editors in der Amazon Redshift Redshift-Konsole auf. Beispiele für das Aufrufen von der aus finden Sie AWS CLI unterAufrufen der Daten-API.

Wichtige Punkte beim Aufrufen der Amazon Redshift Data API

Beachten Sie Folgendes, wenn Sie die Data API aufrufen:

- Die Amazon Redshift Data API kann auf Datenbanken in von Amazon Redshift bereitgestellten Clustern und Redshift-Serverless-Arbeitsgruppen zugreifen. Eine Liste, AWS-Regionen wo die Redshift Data API verfügbar ist, finden Sie in den Endpunkten, die für die Redshift Data API aufgeführt sind. Allgemeine Amazon Web Services-Referenz
- Die maximale Dauer einer Abfrage beträgt 24 Stunden.
- Die maximale Anzahl aktiver Abfragen (`STARTED`- und`SUBMITTED`-Abfragen) pro Amazon-Redshift-Cluster beträgt 200.
- Die maximale Größe der Abfrageergebnisse beträgt 100 MB (nach Gzip-Komprimierung). Wenn ein Aufruf mehr als 100 MB an Antwortdaten zurückgibt, wird der Aufruf beendet.
- Die maximale Aufbewahrungszeit für Abfrageergebnisse beträgt 24 Stunden.
- Die maximale Größe von Abfrageanweisungen beträgt 100 KB.
- Die Data API ist für die Abfrage von Clustern mit einem Knoten und mehreren Knoten der folgenden Knotentypen verfügbar:
  - dc2.large

- dc2.8xlarge
- ds2.xlarge
- ds2.8xlarge
- ra3.xlplus
- ra3.4xlarge
- ra3.16xlarge

- Der Cluster muss sich in einer auf dem Amazon-VPC-Service basierenden Virtual Private Cloud (VPC) befinden.
- Standardmäßig können Benutzer mit derselben IAM-Rolle oder denselben IAM-Berechtigungen wie der Ausführer eines `ExecuteStatement`- oder `BatchExecuteStatement`-API-Vorgangs auf dieselbe Anweisung mit `CancelStatement`-, `DescribeStatement`-, `GetStatementResult`- und `ListStatements`-API-Vorgängen reagieren. Um auf dieselbe SQL-Anweisung eines anderen Benutzers reagieren zu können, muss der Benutzer die IAM-Rolle des Benutzers übernehmen können, der die SQL-Anweisung ausgeführt hat. Weitere Informationen zum Übernehmen einer Rolle finden Sie unter Autorisieren des Zugriffs auf die Amazon Redshift Data API.
- Die SQL-Anweisungen im Parameter `Sqls` der API-Operation `BatchExecuteStatement` werden als eine einzige Transaktion ausgeführt. Sie werden seriell in der Reihenfolge des Arrays ausgeführt. Nachfolgende SQL-Anweisungen werden erst gestartet, wenn die vorherige Anweisung im Array abgeschlossen ist. Wenn eine SQL-Anweisung fehlschlägt, wird die gesamte Arbeit zurückgesetzt, da die Anweisungen als eine Transaktion ausgeführt werden.
- Die maximale Aufbewahrungszeit für ein Client-Token, das in der API-Operation `ExecuteStatement` oder `BatchExecuteStatement` verwendet wird, beträgt 8 Stunden.
- Jede API in der Redshift-Daten-API verfügt über ein Kontingent von Transaktionen pro Sekunde, bevor Anforderungen gedrosselt werden. Informationen zu dem Kontingent finden Sie unter Kontingente für die Amazon-Redshift-Daten-API. Wenn die Anforderungsrate das Kontingent überschreitet, wird eine `ThrottlingException` mit dem HTTP-Statuscode: 400 zurückgegeben. Um auf die Drosselung zu reagieren, verwenden Sie eine Wiederholungsstrategie, wie unter Wiederholungsverhalten im Referenzhandbuch zu AWS -SDKs und Tools beschrieben. Diese Strategie wird in einigen SDKs automatisch implementiert, um Fehler zu drosseln. AWS

> **Note**
>
> Standardmäßig sind AWS Step Functions Wiederholungsversuche nicht aktiviert. Wenn Sie eine Redshift-Daten-API in einem Step-Functions-Zustandsautomat aufrufen müssen, fügen Sie den Idempotenzparameter `ClientToken` in Ihren Redshift-Daten-API-Aufruf

ein. Der Wert für `ClientToken` muss auch bei Wiederholungsversuchen beibehalten werden. Im folgenden Beispielausschnitt einer Anforderung an die `ExecuteStatement`-API verwendet der Ausdruck `States.ArrayGetItem(States.StringSplit($$.Execution.Id, ':'), 7)` eine intrinsische Funktion, um den UUID-Teil von `$$.Execution.Id` zu extrahieren, der für jede Ausführung des Zustandsautomats eindeutig ist. Weitere Informationen finden Sie unter Intrinsische Funktionen im AWS Step Functions -Entwicklerhandbuch.

```
{
  "Database": "dev",
  "Sql": "select 1;",
  "ClusterIdentifier": "MyCluster",
  "ClientToken.$": "States.ArrayGetItem(States.StringSplit($$.Execution.Id,
 ':'), 7)"
}
```

Auswählen der Anmeldeinformationen für die Datenbankauthentifizierung beim Aufrufen der Amazon Redshift Data API

Wenn Sie die Data API aufrufen, verwenden Sie eine der folgenden Authentifizierungsmethoden für einige API-Vorgänge. Jede Methode erfordert eine andere Kombination von Parametern.

AWS Secrets Manager

Geben Sie bei dieser Methode den Wert `secret-arn` eines Geheimnisses an AWS Secrets Manager , in dem `username` und `password` gespeichert ist. Das angegebene Secret enthält Anmeldeinformationen zum Verbinden mit der von Ihnen angegebenen `database`. Wenn Sie eine Verbindung zu einem Cluster herstellen, geben Sie auch den Datenbanknamen an. Wenn Sie eine Clusterkennung (`dbClusterIdentifier`) angeben, muss diese mit der in dem Secret gespeicherten Clusterkennung übereinstimmen. Wenn Sie eine Verbindung zu einer Serverless-Arbeitsgruppe herstellen, geben Sie auch den Datenbanknamen an. Weitere Informationen finden Sie unter Speichern von Datenbankanmeldedaten in AWS Secrets Manager.

Temporäre Anmeldeinformationen

Wählen Sie bei dieser Methode eine der folgenden Optionen aus:

- Wenn Sie eine Verbindung zu einer Serverless-Arbeitsgruppe herstellen, geben Sie den Arbeitsgruppennamen und den Datenbanknamen an. Der Datenbankbenutzername wird

von der IAM-Identität abgeleitet. Für `arn:iam::123456789012:user:foo` lautet der Datenbankbenutzername beispielsweise `IAM:foo`. Auch die Berechtigung zum Aufruf der `redshift-serverless:GetCredentials`-Operation ist erforderlich.

- Geben Sie die Clusterkennung und den Datenbanknamen an, wenn Sie eine Verbindung zu einem Cluster als IAM-Identität herstellen. Der Datenbankbenutzername wird von der IAM-Identität abgeleitet. Für `arn:iam::123456789012:user:foo` lautet der Datenbankbenutzername beispielsweise `IAM:foo`. Auch die Berechtigung zum Aufruf der `redshift:GetClusterCredentialsWithIAM`-Operation ist erforderlich.
- Geben Sie die Clusterkennung, den Datenbanknamen und den Namen des Datenbankbenutzers an, wenn Sie eine Verbindung zu einem Cluster als Datenbankbenutzer herstellen. Auch die Berechtigung zum Aufruf der `redshift:GetClusterCredentials`-Operation ist erforderlich. Hinweise dazu, wie Sie Datenbankgruppen beitreten, wenn Sie mit dieser Methode eine Verbindung herstellen, finden Sie unter Beitreten zu Datenbankgruppen beim Herstellen einer Verbindung mit einem Cluster.

Mit diesen Methoden können Sie auch einen `region` Wert angeben, der angibt, AWS-Region wo sich Ihre Daten befinden.

Zuordnen von JDBC-Datentypen beim Aufrufen der Amazon Redshift Data API

In der folgenden Tabelle sind den Datentypen, die Sie in Daten-API-Aufrufen angeben, JDBC-Datentypen (Java Database Connectivity) zugeordnet.

JDBC-Datentyp	Daten-API-Datentyp
`INTEGER, SMALLINT, BIGINT`	`LONG`
`FLOAT, REAL, DOUBLE`	`DOUBLE`
`DECIMAL`	`STRING`
`BOOLEAN, BIT`	`BOOLEAN`
`BLOB, BINARY, LONGVARBINARY, VARBINARY`	`BLOB`
`VARBINARY`	`STRING`

JDBC-Datentyp	Daten-API-Datentyp
`CLOB`	`STRING`
Andere Typen (einschließlich datums- und zeitbezogener Typen)	`STRING`

Zeichenfolgenwerte werden an die Amazon-Redshift-Datenbank übergeben und implizit in einen Datenbankdatentyp umgewandelt.

> **Note**
>
> Derzeit unterstützt die Data API keine Arrays von Universal Unique Identifiers (UUIDs).

Ausführen von SQL-Anweisungen mit Parametern beim Aufrufen der Amazon Redshift Data API

Sie können den an die Datenbank-Engine übermittelten SQL-Text kontrollieren, indem Sie den Data-API-Vorgang mithilfe von Parametern für Teile der SQL-Anweisung aufrufen. Benannte Parameter bieten eine flexible Möglichkeit, Parameter zu übergeben, ohne sie im SQL-Text hart zu codieren. Sie helfen Ihnen, SQL-Text wiederzuverwenden und SQL-Injections-Probleme zu vermeiden.

Das folgende Beispiel zeigt die benannten Parameter eines `parameters` `execute-statement` AWS CLI Befehlsfeldes.

```
--parameters "[{\"name\": \"id\", \"value\": \"1\"},{\"name\": \"address\", \"value\":
 \"Seattle\"}]"
```

Beachten Sie Folgendes, wenn Sie benannte Parameter verwenden:

- Benannte Parameter können nur verwendet werden, um Werte in SQL-Anweisungen zu ersetzen.
  - Sie können die Werte in einer INSERT-Anweisung, wie z. B. `INSERT INTO mytable VALUES(:val1)`, ersetzen.

    Die benannten Parameter können in beliebiger Reihenfolge vorliegen und Parameter können mehrmals im SQL-Text verwendet werden. Die in einem vorherigen Beispiel gezeigte

Parameteroption, die Werte 1 und `Seattle` werden in die Tabellenspalten `id` und `address` eingefügt. Im SQL-Text geben Sie die benannten Parameter wie folgt an:

```
--sql "insert into mytable values (:id, :address)"
```

- Sie können die Werte in einer Bedingungsklausel ersetzen, z. B. `WHERE attr >= :val1`, `WHERE attr BETWEEN :val1 AND :val2` und `HAVING COUNT(attr) > :val`.
- Sie können in einer SQL-Anweisung keine Spaltennamen ersetzen, wie z. B. `SELECT column-name`, `ORDER BY column-name` oder `GROUP BY column-name`.

  Die folgende SELECT-Anweisung schlägt beispielsweise aufgrund bei einer ungültigen Syntax fehl.

  ```
  --sql "SELECT :colname, FROM event" --parameters "[{\"name\": \"colname\", \"value
  \": \"eventname\"}]"
  ```

  Wenn Sie die Anweisung mit dem Syntaxfehler beschreiben (`describe-statement`-Operation), ersetzt der zurückgegebene `QueryString` nicht den Spaltennamen für den Parameter (`"QueryString": "SELECT :colname, FROM event"`) und es wird ein Fehler gemeldet (ERROR: Syntaxfehler bei oder nahe \"FROM\"\n Position: 12).
- Sie können in einer Aggregatfunktion keine Spaltennamen ersetzen, wie z. B. `COUNT(column-name)`, `AVG(column-name)` oder `SUM(column-name)`.
- Sie können Spaltennamen in einer JOIN-Klausel nicht ersetzen.

- Wenn die SQL-Anweisung ausgeführt wird, werden Daten implizit in einen Datentyp umgewandelt. Weitere Informationen zur Datentypumwandlung finden Sie unter Datentypen im Datenbankentwicklerhandbuch zu Amazon Redshift.
- Sie können einen Wert nicht auf NULL setzen. Die Data API interpretiert ihn als Literalzeichenfolge `NULL`. Im folgenden Beispiel wird `id` durch die Literalzeichenfolge `null` ersetzt, nicht durch den SQL-NULL-Wert.

  ```
  --parameters "[{\"name\": \"id\", \"value\": \"null\"}]"
  ```
- Sie können keinen Wert mit Länge null festlegen. Die SQL-Anweisung der Data API schlägt fehl. Im folgenden Beispiel wird versucht, `id` mit einem Wert der Länge null festzulegen, was zum Fehlschlagen der SQL-Anweisung führt.

  ```
  --parameters "[{\"name\": \"id\", \"value\": \"\"}]"
  ```

- Sie können einen Tabellennamen in der SQL-Anweisung nicht mit einem Parameter festlegen. Die Data API folgt der Regel des JDBC-`PreparedStatement`.
- Die Ausgabe der Operation `describe-statement` gibt die Abfrageparameter einer SQL-Anweisung zurück.
- Nur der `execute-statement`-Vorgang unterstützt SQL-Anweisungen mit Parametern.

Ausführen von SQL-Anweisungen mit einem Idempotenz-Token beim Aufrufen der Amazon Redshift Data API

Wenn Sie eine ändernde API-Anfrage stellen, gibt die Anfrage in der Regel ein Ergebnis zurück, bevor die asynchronen Workflows der Operation abgeschlossen sind. Es können auch ein Timeout oder andere Serverprobleme auftreten, bevor Operationen abgeschlossen sind, obwohl die Anfrage bereits ein Ergebnis zurückgegeben hat. Dadurch lässt sich möglicherweise nur schwer feststellen, ob die Anfrage erfolgreich war oder nicht, und es werden möglicherweise mehrere Wiederholungsversuche vorgenommen, um sicherzustellen, dass die Operation erfolgreich abgeschlossen wird. Wenn die ursprüngliche Anfrage und die nachfolgenden Wiederholungsversuche jedoch erfolgreich sind, wird die Operation mehrmals abgeschlossen. Das bedeutet, dass Sie möglicherweise mehr Ressourcen aktualisieren als beabsichtigt.

Idempotenz stellt sicher, dass eine API-Anfrage nicht mehr als einmal abgeschlossen wird. Wenn bei einer idempotenten Anfrage die ursprüngliche Anfrage erfolgreich abgeschlossen wird, werden alle nachfolgenden Wiederholungen erfolgreich abgeschlossen, ohne dass weitere Aktionen ausgeführt werden. Die Data-API-Operationen `ExecuteStatement` und `BatchExecuteStatement` weisen den optionalen idempotenten Parameter `ClientToken` auf. Das `ClientToken` läuft nach 8 Stunden ab.

> **Important**
>
> Wenn Sie von einem AWS SDK aus aufrufen `ExecuteStatement` und `BatchExecuteStatement` Operationen ausführen, generiert es automatisch ein Client-Token, das bei einem erneuten Versuch verwendet wird. In diesem Fall empfehlen wir, den Parameter `client-token` nicht mit den Operationen `ExecuteStatement` und `BatchExecuteStatement` zu verwenden. Sehen Sie CloudTrail sich das Protokoll an, um das `ClientToken` zu sehen. Ein Beispiel für ein CloudTrail Protokoll finden Sie unterAmazon-Redshift-Daten-API – Beispiele.

Der folgende `execute-statement` AWS CLI Befehl veranschaulicht den optionalen `client-token` Parameter für Idempotenz.

```
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
```

Die folgende Tabelle zeigt einige häufig vorkommende Antworten, die Sie auf idempotente API-Anfragen erhalten könnten, und stellt Empfehlungen zu Wiederholungsversuchen bereit.

Antwort	Empfehlung	Kommentare
200 (OK)	Nicht erneut versuchen	Die ursprüngliche Anfrage wurde erfolgreich abgeschlossen. Alle nachfolgenden Wiederholungsversuche werden als erfolgreich zurückgegeben.
Antwortcodes der Serie 400	Nicht erneut versuchen	Es liegt eins der folgenden Probleme mit der Anfrage vor: • Sie enthält einen Parameter oder eine Parameterkombination, der/die nicht gültig ist. • Sie verwendet eine Aktion oder Ressource, für die Sie keine Berechtigungen haben. • Sie verwendet eine Ressource, deren Status sich gerade ändert. Wenn die Anfrage eine Ressource umfasst, deren Status sich gerade ändert, könnte ein erneuter Anfrageversuch möglicherweise erfolgreich sein.

Antwort	Empfehlung	Kommentare
Antwortcodes der Serie 500	Erneut versuchen	Der Fehler wird durch ein AWS serverseitiges Problem verursacht und ist im Allgemeinen vorübergehend. Wiederholen Sie die Anfrage mit einer geeigneten Backoff-Strategie.

Weitere Informationen zu den Amazon-Redshift-Antwortcodes finden Sie unter Häufige Fehler in der API-Referenz zu Amazon Redshift.

Autorisieren des Zugriffs auf die Amazon Redshift Data API

Ein Benutzer muss zum Zugriff auf die Data API autorisiert sein. Sie können einen Benutzer zum Zugriff auf die Data API autorisieren, indem Sie dem betreffenden Benutzer eine verwaltete Richtlinie, eine vordefinierte AWS Identity and Access Management (IAM)-Richtlinie, hinzufügen. Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift. Informationen zu den Berechtigungen, die von verwalteten Richtlinien zugelassen und verweigert werden, finden Sie in der IAM-Konsole (https://console.aws.amazon.com/iam/).

Amazon Redshift stellt die von `AmazonRedshiftDataFullAccess` verwaltete Richtlinie bereit. Diese Richtlinie bietet vollständigen Zugriff auf die Amazon-Redshift-Data-API-Vorgänge. Diese Richtlinie ermöglicht auch den bereichsbezogenen Zugriff auf bestimmte Amazon Redshift- und IAM-API-Operationen AWS Secrets Manager, die für die Authentifizierung und den Zugriff auf einen Amazon Redshift Redshift-Cluster oder eine Redshift Serverless-Arbeitsgruppe erforderlich sind.

Sie können auch eine eigene IAM-Richtlinie erstellen, die den Zugriff auf bestimmte Ressourcen ermöglicht. Um Ihre Richtlinie zu erstellen, verwenden Sie die `AmazonRedshiftDataFullAccess`-Richtlinie als Ausgangspunkt. Nach dem Erstellen Ihrer Richtlinie können Sie diese jedem Benutzer hinzufügen, der Zugriff auf die Data API benötigt.

Berücksichtigen Sie die folgenden Anforderungen der IAM-Richtlinie, die mit dem Benutzer verknüpft ist:

- Wenn Sie die Authentifizierung verwenden, vergewissern Sie AWS Secrets Manager sich, dass die Richtlinie die Verwendung der Aktion zum Abrufen des mit dem Schlüssel markierten Geheimnisses `secretsmanager:GetSecretValue` zulässt. `RedshiftDataFullAccess`

- Wenn Sie temporäre Anmeldeinformationen für die Authentifizierung verwenden, prüfen Sie, ob die Richtlinie die Verwendung der `redshift:GetClusterCredentials`-Aktion für den Datenbankbenutzernamen `redshift_data_api_user` für jede Datenbank im Cluster erlaubt. Dieser Benutzername muss bereits in Ihrer Datenbank erstellt worden sein.
- Wenn Sie temporäre Anmeldeinformationen verwenden, um sich bei einer Serverless-Arbeitsgruppe zu authentifizieren, bestätigen Sie, dass die Richtlinie die Verwendung der Aktion `redshift-serverless:GetCredentials` zum Abrufen der mit dem Schlüssel `RedshiftDataFullAccess` gekennzeichneten Arbeitsgruppe zulässt. Der Datenbankbenutzer wird der Quellidentität AWS Identity and Access Management (IAM) 1:1 zugeordnet. Der Benutzer sample_user ist beispielsweise einem Datenbankbenutzer `IAM:sample_user` und die IAM-Rolle sample_role ist `IAMR:sample_role` zugeordnet. Weitere Informationen zu unterschiedlichen IAM-Identitäten finden Sie unter IAM-Identitäten (Benutzer, Benutzergruppen und Rollen) im IAM-Benutzerhandbuch.

Um eine Abfrage in einem Cluster auszuführen, der einem anderen Konto gehört, muss das besitzende Konto eine IAM-Rolle bereitstellen, die die Data API im aufrufenden Konto übernehmen kann. Angenommen, Konto B besitzt einen Cluster, auf den Konto A zugreifen muss. Konto B kann die AWS-verwaltete Richtlinie `AmazonRedshiftDataFullAccess` der IAM-Rolle von Konto B zuordnen. Dann vertraut Konto B Konto A mit einer Vertrauensrichtlinie wie der folgenden:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::accountID-of-account-A:role/someRoleA"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Schließlich muss die IAM-Rolle von Konto A die IAM-Rolle von Konto B übernehmen können.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::accountID-of-account-B:role/someRoleB"
  }
}
```

Unter den folgenden Links finden Sie weitere Informationen zum AWS Identity and Access Management IAM-Benutzerhandbuch.

- Weitere Informationen zum Erstellen von IAM-Rollen finden Sie unter Erstellen von IAM-Rollen.
- Informationen zum Erstellen einer IAM-Richtlinie finden Sie unter Erstellen von IAM-Richtlinien.
- Informationen zum Hinzufügen einer IAM-Richtlinie zu einem Benutzer finden Sie unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen.

Speichern von Datenbankanmeldedaten in AWS Secrets Manager

Wenn Sie die Data API aufrufen, können Sie die Anmeldeinformationen für den Cluster oder die Serverless-Arbeitsgruppe unter Verwendung eines Secrets in AWS Secrets Managerübergeben. Zum Übermitteln der Anmeldeinformationen auf diese Weise geben Sie den Namen des Secrets oder den Amazon-Ressourcennamen (ARN) des Secrets an.

Um Anmeldeinformationen mit Secrets Manager zu speichern, benötigen Sie eine von `SecretManagerReadWrite` verwaltete Richtlinienberechtigung. Weitere Informationen zu den Mindestberechtigungen finden Sie unter Creating and Managing AWS Secrets with Secrets Manager im AWS Secrets Manager Benutzerhandbuch.

So speichern Sie Ihre Anmeldeinformationen in einem Secret für einen Amazon-Redshift-Cluster

1. Verwenden Sie die AWS Secrets Manager Konsole, um einen geheimen Schlüssel zu erstellen, der Anmeldeinformationen für Ihren Cluster enthält:

   - Wenn Sie Store a new secret (Neues Secret speichern) auswählen, wählen Sie Credentials for Redshift cluster (Anmeldeinformationen für Redshift-Cluster) aus.
   - Speichern Sie Ihre Werte für User name (Benutzername) (Datenbankbenutzer),Password (Passwort) und DB cluster (DB-Cluster) (Cluster-ID) in Ihrem Secret.

- Markieren Sie das Secret mit dem Schlüssel `RedshiftDataFullAccess`. Die von AWS verwaltete Richtlinie `AmazonRedshiftDataFullAccess` erlaubt nur die Aktion `secretsmanager:GetSecretValue` für Secrets, die mit dem Schlüssel `RedshiftDataFullAccess` markiert sind.

Anweisungen finden Sie unter Erstellen eines Basis-Secrets im AWS Secrets Manager - Benutzerhandbuch.

2. Verwenden Sie die AWS Secrets Manager Konsole, um die Details für das von Ihnen erstellte Geheimnis anzuzeigen, oder führen Sie den `aws secretsmanager describe-secret` AWS CLI Befehl aus.

   Notieren Sie sich den Namen und den ARN des Secrets. Sie können diese in Aufrufen an die Data API verwenden.

So speichern Sie Ihre Anmeldeinformationen in einem Secret für eine Serverless-Arbeitsgruppe

1. Verwenden Sie AWS Secrets Manager AWS CLI Befehle, um ein Geheimnis zu speichern, das Anmeldeinformationen für Ihre serverlose Arbeitsgruppe enthält:

   - Erstellen Sie Ihr Secret in einer Datei, zum Beispiel einer JSON-Datei mit dem Namen `mycreds.json`. Geben Sie die Werte für User name (Benutzername) (d. h. den Namen des Datenbankbenutzers) und Password (Kennwort) in der Datei an.

     ```
     {
           "username": "myusername",
           "password": "mypassword"
     }
     ```

   - Speichern Sie Ihre Werte in Ihrem Secret und markieren Sie das Secret mit dem Schlüssel `RedshiftDataFullAccess`.

     ```
     aws secretsmanager create-secret --name MyRedshiftSecret  --tags
      Key="RedshiftDataFullAccess",Value="serverless" --secret-string file://
     mycreds.json
     ```

     Nachfolgend sehen Sie die Ausgabe.

     ```
     {
     ```

```
    "ARN":
 "arn:aws:secretsmanager:region:accountId:secret:MyRedshiftSecret-mvLHxf",
    "Name": "MyRedshiftSecret",
    "VersionId": "a1603925-e8ea-4739-9ae9-e509eEXAMPLE"
}
```

Weitere Informationen finden Sie unter Erstellen eines Basis-Secrets mit der AWS CLI im AWS Secrets Manager -Benutzerhandbuch.

2. Verwenden Sie die AWS Secrets Manager Konsole, um die Details für das von Ihnen erstellte Geheimnis anzuzeigen, oder führen Sie den `aws secretsmanager describe-secret` AWS CLI Befehl aus.

   Notieren Sie sich den Namen und den ARN des Secrets. Sie können diese in Aufrufen an die Data API verwenden.

Erstellen eines Amazon-VPC-Endpunkts (AWS PrivateLink) für die Data API

Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie AWS Ressourcen wie Amazon Redshift Redshift-Cluster und -Anwendungen in einer Virtual Private Cloud (VPC) starten. AWS PrivateLink bietet private Konnektivität zwischen virtuellen privaten Clouds (VPCs) und sicheren AWS Diensten im Amazon-Netzwerk. Mit AWS PrivateLink können Sie VPC-Endpunkte erstellen, mit denen Sie eine Verbindung zu Services über verschiedene Konten und VPCs basierend auf Amazon VPC herstellen können. Weitere Informationen AWS PrivateLink finden Sie unter VPC Endpoint Services (AWS PrivateLink) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Sie können die Daten-API mit Amazon VPC-Endpunkten aufrufen. Durch die Verwendung eines Amazon VPC-Endpunkts wird der Datenverkehr zwischen Anwendungen in Ihrer Amazon VPC und der Daten-API im AWS Netzwerk aufrechterhalten, ohne öffentliche IP-Adressen zu verwenden. Amazon-VPC-Endpunkte können Ihnen dabei helfen, Compliance- und behördliche Anforderungen im Zusammenhang mit der Einschränkung der öffentlichen Internetkonnektivität zu erfüllen. Wenn Sie beispielsweise einen Amazon VPC-Endpunkt verwenden, können Sie den Datenverkehr zwischen einer Anwendung, die auf einer Amazon EC2-Instance ausgeführt wird, und der Daten-API in den VPCs, die diese enthalten, beibehalten.

Nachdem Sie den Amazon VPC-Endpunkt erstellt haben, können Sie ihn verwenden, ohne Code- oder Konfigurationsänderungen in der Anwendung vorzunehmen.

So erstellen Sie einen Amazon VPC-Endpunkt für die Daten-API

1. Melden Sie sich bei der Amazon VPC-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie Endpunkte und dann Endpunkt erstellen aus.
3. Wählen Sie auf der Seite Create Endpoint (Endpunkt erstellen) für Service category (Servicekategorie) die Option AWS -Services aus. Wählen Sie bei Service Name redshift-data (`com.amazonaws.region.redshift-data`) aus.
4. Wählen Sie für VPC die VPC aus, in der der Endpunkt erstellt werden soll.

   Wählen Sie die VPC aus, die die Anwendung enthält, die Daten-API-Aufrufe ausführt.
5. Wählen Sie für Subnetze das Subnetz für jede Availability Zone (AZ) aus, die von dem AWS Service verwendet wird, auf dem Ihre Anwendung ausgeführt wird.

   Um einen Amazon-VPC-Endpunkt zu erstellen, geben Sie den privaten IP-Adressbereich an, in dem der Endpunkt zugänglich ist. Wählen Sie dazu das Subnetz für jede Availability Zone aus. Dadurch wird der VPC-Endpunkt auf den privaten IP-Adressbereich beschränkt, der für jede Availability Zone spezifisch ist. Außerdem wird in jeder Availability Zone ein Amazon VPC-Endpunkt erstellt.
6. Wählen Sie für DNS-Namen aktivieren die Option Für diesen Endpunkt aktivieren aus.

   Private DNS löst den standardmäßigen DNS-Hostnamen der Daten-API (`https://redshift-data.region.amazonaws.com`) in die privaten IP-Adressen auf, die mit dem für Ihren Amazon VPC-Endpunkt spezifischen DNS-Hostnamen verknüpft sind. Daher können Sie mit den AWS CLI oder AWS SDKs auf den Daten-API-VPC-Endpunkt zugreifen, ohne Code- oder Konfigurationsänderungen vornehmen zu müssen, um die Daten-API-Endpunkt-URL zu aktualisieren.
7. Wählen Sie für Sicherheitsgruppe eine Sicherheitsgruppe aus, die dem Amazon VPC-Endpunkt zugeordnet werden soll.

   Wählen Sie die Sicherheitsgruppe aus, die den Zugriff auf den AWS Dienst ermöglicht, auf dem Ihre Anwendung ausgeführt wird. Wenn beispielsweise eine Amazon EC2-Instance Ihre Anwendung ausführt, wählen Sie die Sicherheitsgruppe aus, die den Zugriff auf die Amazon EC2-Instance ermöglicht. Mit der Sicherheitsgruppe können Sie den Datenverkehr zum Amazon VPC-Endpunkt von Ressourcen in Ihrer VPC steuern.
8. Wählen Sie Create endpoint.

Nachdem der Endpunkt erstellt wurde, wählen Sie den Link in, AWS Management Console um die Endpunktdetails anzuzeigen.

Auf der Registerkarte Details des Endpunkts werden die DNS-Hostnamen angezeigt, die beim Erstellen des Amazon VPC-Endpunkts generiert wurden.

Sie können den Standardendpunkt (`redshift-data.`*`region`*`.amazonaws.com`) oder einen der VPC-spezifischen Endpunkte verwenden, um die Daten-API innerhalb der Amazon VPC aufzurufen. Der standardmäßige Daten-API-Endpunkt leitet automatisch an den Amazon VPC-Endpunkt weiter. Dieses Routing tritt auf, weil der private DNS-Hostname beim Erstellen des Amazon VPC-Endpunkts aktiviert wurde.

Wenn Sie einen Amazon VPC-Endpunkt in einem Daten-API-Aufruf verwenden, verbleibt der gesamte Datenverkehr zwischen Ihrer Anwendung und der Daten-API in den Amazon VPCs, die sie enthalten. Sie können einen Amazon VPC-Endpunkt für jeden Typ von Daten-API-Aufruf verwenden. Informationen zum Aufrufen der Daten-API finden Sie unter Wichtige Punkte beim Aufrufen der Amazon Redshift Data API.

Beitreten zu Datenbankgruppen beim Herstellen einer Verbindung mit einem Cluster

Datenbankgruppen sind Sammlungen von Datenbankbenutzern. Datenbankberechtigungen können Gruppen gewährt werden. Ein Administrator kann eine IAM-Rolle so konfigurieren, dass diese Datenbankgruppen berücksichtigt werden, wenn Ihr SQL mit der Daten-API ausgeführt wird. Weitere Informationen über Datenbankgruppen finden Sie unter Gruppen im Datenbankentwicklerhandbuch zu Amazon Redshift.

Sie können die IAM-Rolle eines Daten-API-Aufrufers so konfigurieren, dass der im Aufruf angegebene Datenbankbenutzer Datenbankgruppen beitritt, wenn die Daten-API eine Verbindung mit einem Cluster herstellt. Diese Funktion wird nur unterstützt, wenn eine Verbindung mit bereitgestellten Clustern hergestellt wird. Sie wird nicht unterstützt beim Herstellen einer Verbindung mit Redshift-Serverless-Arbeitsgruppen. Die IAM-Rolle des Aufrufers der Daten-API muss außerdem die Aktion `redshift:JoinGroup` zulassen.

Konfigurieren Sie dies, indem Sie IAM-Rollen Tags hinzufügen. Der Administrator der IAM-Rolle des Aufrufers fügt Tags mit dem Schlüssel `RedshiftDbGroups` und einem Schlüsselwert einer Liste von Datenbankgruppen. Der Wert ist eine Liste von durch Doppelpunkt (:) getrennten Namen von Datenbankgruppen mit einer Gesamtlänge von bis zu 256 Zeichen. Die Datenbankgruppen müssen zuvor in der verbundenen Datenbank definiert worden sein. Wenn eine angegebene Gruppe in der Datenbank nicht zu finden ist, wird sie ignoriert. Zum Beispiel lautet der Schlüsselwert für die

Datenbankgruppen `accounting` und `retail` `accounting:retail`. Das Tag-Schlüssel-Wert-Paar `{"Key":"RedshiftDbGroups","Value":"accounting:retail"}` wird von der Daten-API verwendet, um zu ermitteln, welche Datenbankgruppen dem angegebenen Datenbankbenutzer beim Aufruf der Daten-API zugeordnet sind.

So fügen Sie einer IAM-Rolle Datenbankgruppen als Tag hinzu

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der Konsole Rollen aus und wählen Sie dann den Namen der Rolle aus, die Sie bearbeiten möchten.
3. Wählen Sie die Registerkarte Tags und dann Tags verwalten aus.
4. Wählen Sie Tag hinzufügen und fügen Sie dann den Schlüssel RedshiftDbGroupsund einen Wert hinzu, der eine Liste von *`database-groups-colon-separated`*ist.
5. Wählen Sie Änderungen speichern aus.

   Wenn nun ein IAM-Prinzipal (mit angefügter IAM-Rolle) die Daten-API aufruft, tritt der angegebene Datenbankbenutzer den in der IAM-Rolle angegebenen Datenbankgruppen bei.

Weitere Informationen darüber, wie Sie ein Tag an einen Prinzipal anhängen, einschließlich IAM-Rollen und IAM-Benutzern, finden Sie unter Markieren von IAM-Ressourcen im IAM-Benutzerhandbuch.

Aufrufen der Daten-API

Sie können die Daten-API oder die aufrufen AWS CLI , um SQL-Anweisungen auf Ihrem Cluster oder Ihrer serverlosen Arbeitsgruppe auszuführen. Die primären Operationen zum Ausführen von SQL-Anweisungen sind `ExecuteStatement` und `BatchExecuteStatement` in der Amazon-Redshift-Daten-API-Referenz. Die Daten-API unterstützt die Programmiersprachen, die AWS vom SDK unterstützt werden. Weitere Informationen finden Sie unter Tools für AWS.

Codebeispiele für den Aufruf der Daten-API finden Sie unter Erste Schritte mit der Redshift Data API in GitHub. Dieses Repository enthält Beispiele für AWS Lambda den Zugriff auf Amazon Redshift Redshift-Daten aus Amazon EC2 und Amazon AWS Glue Data Catalog SageMaker Runtime. Beispiele für Programmiersprachen sind Python, Go, Java und Javascript.

Sie können die Daten-API über die aufrufe AWS CLI.

In den folgenden Beispielen wird die AWS CLI zum Aufrufen der Daten-API verwendet. Um die Beispiele auszuführen, bearbeiten Sie die Parameterwerte entsprechend Ihrer Umgebung. In vielen Beispielen wird eine `cluster-identifier` gegeben, die gegen einen Cluster ausgeführt wird. Wenn Sie mit einer Serverless-Arbeitsgruppe arbeiten, geben Sie stattdessen einen `workgroup-name` an. Diese Beispiele veranschaulichen einige der Data-API-Vorgänge. Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

Die Befehle in den folgenden Beispielen wurden zur besseren Lesbarkeit aufgeteilt und formatiert.

So führen Sie eine SQL-Anweisung aus

Verwenden Sie den `aws redshift-data execute-statement` AWS CLI Befehl, um eine SQL-Anweisung auszuführen.

Der folgende AWS CLI Befehl führt eine SQL-Anweisung für einen Cluster aus und gibt einen Bezeichner zum Abrufen der Ergebnisse zurück. In diesem Beispiel wird die AWS Secrets Manager Authentifizierungsmethode verwendet.

```
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
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "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"
}
```

Der folgende AWS CLI Befehl führt eine SQL-Anweisung für einen Cluster aus und gibt einen Bezeichner zum Abrufen der Ergebnisse zurück. In diesem Beispiel wird die Authentifizierungsmethode mit temporären Anmeldeinformationen verwendet.

```
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"
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

Der folgende AWS CLI Befehl führt eine SQL-Anweisung für eine serverlose Arbeitsgruppe aus und gibt einen Bezeichner zum Abrufen der Ergebnisse zurück. In diesem Beispiel wird die Authentifizierungsmethode mit temporären Anmeldeinformationen verwendet.

```
aws redshift-data execute-statement
    --database dev
    --workgroup-name myworkgroup
    --sql "select 1;"
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
 "CreatedAt": "2022-02-11T06:25:28.748000+00:00",
 "Database": "dev",
 "DbUser": "IAMR:RoleName",
 "Id": "89dd91f5-2d43-43d3-8461-f33aa093c41e",
 "WorkgroupName": "myworkgroup"
}
```

Der folgende AWS CLI Befehl führt eine SQL-Anweisung für einen Cluster aus und gibt einen Bezeichner zum Abrufen der Ergebnisse zurück. In diesem Beispiel werden die AWS Secrets Manager Authentifizierungsmethode und ein Idempotenz-Token verwendet.

```
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
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "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"
}
```

So führen Sie eine SQL-Anweisung mit Parametern aus

Verwenden Sie den Befehl, um eine SQL-Anweisung auszuführen. `aws redshift-data execute-statement` AWS CLI

Der folgende AWS CLI Befehl führt eine SQL-Anweisung für einen Cluster aus und gibt einen Bezeichner zum Abrufen der Ergebnisse zurück. In diesem Beispiel wird die AWS Secrets Manager Authentifizierungsmethode verwendet. Der SQL-Text weist den benannten Parameter `distance` auf. In diesem Fall lautet die im Prädikat verwendete Entfernung `5`. In einer SELECT-Anweisung können benannte Parameter für Spaltennamen nur im Prädikat verwendet werden. Die Werte für benannte Parameter für die SQL-Anweisung werden in der Option `parameters` angegeben.

```
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
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "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"
}
```

Im folgenden Beispiel wird die EVENT-Tabelle aus der Beispieldatenbank verwendet. Weitere Informationen finden Sie unter EVENT-Tabelle im Datenbankentwicklerhandbuch zu Amazon Redshift.

Wenn Ihre Datenbank noch nicht die EVENT-Tabelle enthält, können Sie mit der Data API eine wie folgt erstellen:

```
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)"
```

Mit dem folgenden Befehl wird eine Zeile in der EVENT-Tabelle eingefügt.

```
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\"}]"
```

Mit dem folgenden Befehl wird eine zweite Zeile in der EVENT-Tabelle eingefügt. In diesem Beispiel werden die folgenden Aufgaben durchgeführt:

- Der Parameter namens `id` wird viermal im SQL-Text verwendet.
- Implizite Typumwandlung wird automatisch angewendet, wenn der Parameter eingefügt wird `starttime`.
- Für die Spalte `venueid` wird die Typumwandlung in den SMALLINT-Datentyp durchgeführt.
- Zeichenfolgen, die den Datentyp DATE darstellen, werden implizit in den Datentyp TIMESTAMP konvertiert.
- Kommentare können in SQL-Text verwendet werden.

```
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\"}]"
```

Hier sehen Sie die beiden eingefügten Zeilen:

```
 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
```

Der folgende Befehl verwendet einen benannten Parameter in einer WHERE-Klausel, um die Zeile abzurufen, in der `eventid` 1 ist.

```
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\"}]"
```

Führen Sie den folgenden Befehl aus, um die SQL-Ergebnisse der vorherigen SQL-Anweisung abzurufen:

```
aws redshift-data get-statement-result --id 7529ad05-b905-4d71-9ec6-8b333836eb5a
```

Bietet folgende Ergebnisse:

```
{
    "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
}
```

So führen Sie mehrere SQL-Anweisungen aus

Um mehrere SQL-Anweisungen mit einem Befehl auszuführen, verwenden Sie den `aws redshift-data batch-execute-statement` AWS CLI Befehl.

Der folgende AWS CLI Befehl führt drei SQL-Anweisungen für einen Cluster aus und gibt einen Bezeichner zum Abrufen der Ergebnisse zurück. In diesem Beispiel wird die Authentifizierungsmethode mit temporären Anmeldeinformationen verwendet.

```
aws redshift-data batch-execute-statement
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --sqls "set timezone to BST" "select * from mytable" "select * from another_table"
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

So listen Sie Metadaten über SQL-Anweisungen auf

Verwenden Sie den `aws redshift-data list-statements` AWS CLI Befehl, um Metadaten zu SQL-Anweisungen aufzulisten. Die Autorisierung zum Ausführen dieses Befehls basiert auf den IAM-Berechtigungen des Aufrufers.

Der folgende AWS CLI Befehl listet die ausgeführten SQL-Anweisungen auf.

```
aws redshift-data list-statements
    --region us-west-2
```

```
    --status ALL
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "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
        }
    ]
}
```

So beschreiben Sie Metadaten über eine SQL-Anweisung

Verwenden Sie den Befehl, um Beschreibungen der Metadaten für eine SQL-Anweisung `aws redshift-data describe-statement` AWS CLI abzurufen. Die Autorisierung zum Ausführen dieses Befehls basiert auf den IAM-Berechtigungen des Aufrufers.

Der folgende AWS CLI Befehl beschreibt eine SQL-Anweisung.

```
aws redshift-data describe-statement
    --id d9b6c0c9-0747-4bf4-b142-e8883122f766
    --region us-west-2
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "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
}
```

Es folgt ein Beispiel für eine `describe-statement`-Antwort nach dem Ausführen eines `batch-execute-statement`-Befehls mit mehreren SQL-Anweisungen.

```
{
    "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
}
```

So rufen Sie die Ergebnisse einer SQL-Anweisung ab

Verwenden Sie den `redshift-data get-statement-result` AWS CLI Befehl, um das Ergebnis einer ausgeführten SQL-Anweisung abzurufen. Sie können eine `Id` angeben, die Sie als Antwort auf `execute-statement` oder `batch-execute-statement` erhalten. Der `Id`-Wert für eine SQL-Anweisung, die von `batch-execute-statement` ausgeführt wurde, kann im Ergebnis von `describe-statement` abgerufen werden und erhält einen Doppelpunkt und eine Sequenznummer wie `b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2` als Suffix. Wenn Sie mehrere SQL-Anweisungen mit `batch-execute-statement` ausführen, hat jede SQL-Anweisung einen `Id`-Wert wie in `describe-statement` gezeigt. Die Autorisierung zum Ausführen dieses Befehls basiert auf den IAM-Berechtigungen des Aufrufers.

Die folgende Anweisung gibt das Ergebnis einer SQL-Anweisung zurück, die von `execute-statement` ausgeführt wurde.

```
aws redshift-data get-statement-result
    --id d9b6c0c9-0747-4bf4-b142-e8883122f766
```

```
    --region us-west-2
```

Die folgende Anweisung gibt das Ergebnis einer zweiten SQL-Anweisung zurück, die von ausgeführt wurde `batch-execute-statement`.

```
aws redshift-data get-statement-result
    --id b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2
    --region us-west-2
```

Das folgende Beispiel ist eine Antwort auf einen -Aufruf `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
}
```

So beschreiben Sie eine Tabelle

Verwenden Sie den `aws redshift-data describe-table` AWS CLI Befehl, um Metadaten abzurufen, die eine Tabelle beschreiben.

Der folgende AWS CLI Befehl führt eine SQL-Anweisung für einen Cluster aus und gibt Metadaten zurück, die eine Tabelle beschreiben. In diesem Beispiel wird die AWS Secrets Manager Authentifizierungsmethode verwendet.

```
aws redshift-data describe-table
    --region us-west-2
    --cluster-identifier mycluster-test
    --database dev
    --schema information_schema
    --table sql_features
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

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

Mit dem folgenden AWS CLI Befehl wird eine SQL-Anweisung für einen Cluster ausgeführt, der eine Tabelle beschreibt. In diesem Beispiel wird die Authentifizierungsmethode mit temporären Anmeldeinformationen verwendet.

```
aws redshift-data describe-table
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --schema information_schema
    --table sql_features
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

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

So listen Sie die Datenbanken in einem Cluster auf

Verwenden Sie den `aws redshift-data list-databases` AWS CLI Befehl, um die Datenbanken in einem Cluster aufzulisten.

Mit dem folgenden AWS CLI Befehl wird eine SQL-Anweisung für einen Cluster ausgeführt, um Datenbanken aufzulisten. In diesem Beispiel wird die AWS Secrets Manager Authentifizierungsmethode verwendet.

```
aws redshift-data list-databases
    --region us-west-2
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
    --cluster-identifier mycluster-test
    --database dev
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "Databases": [
        "dev"
    ]
}
```

Mit dem folgenden AWS CLI Befehl wird eine SQL-Anweisung für einen Cluster ausgeführt, um Datenbanken aufzulisten. In diesem Beispiel wird die Authentifizierungsmethode mit temporären Anmeldeinformationen verwendet.

```
aws redshift-data list-databases
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "Databases": [
        "dev"
```

```
    ]
}
```

So listen Sie die Schemata in einer Datenbank auf

Verwenden Sie den `aws redshift-data list-schemas` AWS CLI Befehl, um die Schemas in einer Datenbank aufzulisten.

Mit dem folgenden AWS CLI Befehl wird eine SQL-Anweisung für einen Cluster ausgeführt, um Schemas in einer Datenbank aufzulisten. In diesem Beispiel wird die AWS Secrets Manager Authentifizierungsmethode verwendet.

```
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
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "Schemas": [
        "information_schema",
        "pg_catalog",
        "pg_internal",
        "public"
    ]
}
```

Mit dem folgenden AWS CLI Befehl wird eine SQL-Anweisung für einen Cluster ausgeführt, um Schemas in einer Datenbank aufzulisten. In diesem Beispiel wird die Authentifizierungsmethode mit temporären Anmeldeinformationen verwendet.

```
aws redshift-data list-schemas
    --region us-west-2
    --db-user mysuser
    --cluster-identifier mycluster-test
    --database dev
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "Schemas": [
        "information_schema",
        "pg_catalog",
        "pg_internal",
        "public"
    ]
}
```

So listen Sie die Tabellen in einer Datenbank auf

Verwenden Sie den `aws redshift-data list-tables` AWS CLI Befehl, um die Tabellen in einer Datenbank aufzulisten.

Mit dem folgenden AWS CLI Befehl wird eine SQL-Anweisung für einen Cluster ausgeführt, um Tabellen in einer Datenbank aufzulisten. In diesem Beispiel wird die AWS Secrets Manager Authentifizierungsmethode verwendet.

```
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
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "Tables": [
        {
            "name": "sql_features",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        },
        {
            "name": "sql_implementation_info",
            "schema": "information_schema",
```

```
            "type": "SYSTEM TABLE"
        }
}
```

Mit dem folgenden AWS CLI Befehl wird eine SQL-Anweisung für einen Cluster ausgeführt, um Tabellen in einer Datenbank aufzulisten. In diesem Beispiel wird die Authentifizierungsmethode mit temporären Anmeldeinformationen verwendet.

```
aws redshift-data list-tables
     --region us-west-2
     --db-user myuser
     --cluster-identifier mycluster-test
     --database dev
     --schema information_schema
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "Tables": [
        {
            "name": "sql_features",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        },
        {
            "name": "sql_implementation_info",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        }
    ]
}
```

Beheben von Problemen mit der Amazon Redshift Data API

Verwenden Sie die folgenden Abschnitte mit dem Titel "Allgemeine Fehlermeldungen", um Probleme zu beheben, die Sie mit der Data-API haben.

Themen

- Packet for Query Is Too Large (Paket für Abfrage zu groß)

- Database Response Exceeded Size Limit Datenbankantwort überschreitet Größenlimit)

Packet for Query Is Too Large (Paket für Abfrage zu groß)

Wenn ein Fehler angezeigt wird, der angibt, dass das Paket für eine Abfrage zu groß ist, ist meist die Ergebnismenge, die für eine Zeile zurückgegeben wurde, zu groß. Die Größenbegrenzung der Data-API beträgt 64 KB pro Zeile in der von der Datenbank zurückgegebenen Ergebnismenge.

Um dieses Problem zu beheben, stellen Sie sicher, dass jede Zeile in einem Ergebnissatz höchstens 64 KB groß ist.

Database Response Exceeded Size Limit Datenbankantwort überschreitet Größenlimit)

Wenn Sie einen Fehler sehen, der darauf hinweist, dass die Datenbankantwort die Größenbeschränkung überschritten hat, war meist die von der Datenbank zurückgegebene Ergebnismenge zu groß. Das Data-API-Limit beträgt 100 MB für die von der Datenbank zurückgegebenen Ergebnismenge.

Um dieses Problem zu beheben, achten Sie darauf, dass Aufrufe der Data-API höchstens 100 MB an Daten zurückgeben. Wenn Sie mehr als 100 MB erhalten müssen, können Sie mit der `LIMIT`-Klausel in Ihrer Anfrage mehrere Anweisungsaufrufe ausführen.

Planung von Amazon Redshift Data API-Vorgängen mit Amazon EventBridge

Sie können Regeln für ausgewählte Ereignisse erstellen und an Ziele weiterleiten, um Aktionen durchzuführen. Sie können auch Regeln verwenden, um Aktionen nach einem vorher festgelegten Zeitplan durchzuführen. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Um Daten-API-Operationen mit planen zu können EventBridge, muss die zugehörige IAM-Rolle dem Principal for CloudWatch Events (events.amazonaws.com) vertrauen. Dieser Rolle sollte das Äquivalent der verwalteten Richtlinie `AmazonEventBridgeFullAccess` zugewiesen sein. Sie sollte auch über `AmazonRedshiftDataFullAccess`-Richtlinienberechtigungen verfügen, die von der Data API verwaltet werden. Sie können eine IAM-Rolle mit diesen Berechtigungen in der IAM-Konsole erstellen. Wählen Sie beim Erstellen einer Rolle in der IAM-Konsole die vertrauenswürdige Service-Entität für Ereignisse aus. AWS CloudWatch Geben Sie die IAM-Rolle im `RoleArn` JSON-

Wert im Ziel an EventBridge . Weitere Informationen zum Erstellen einer IAM-Rolle finden Sie unter Creating a Role for an AWS Service (Console) im IAM-Benutzerhandbuch.

Die name Regel, die Sie in Amazon erstellen, EventBridge muss mit der `StatementName` in der übereinstimmen`RedshiftDataParameters`.

Die folgenden Beispiele zeigen Varianten der EventBridge Regelerstellung mit einer oder mehreren SQL-Anweisungen und mit einem Amazon Redshift-Cluster oder einer Amazon Redshift Serverless-Arbeitsgruppe als Data Warehouse.

Aufrufen mit einer einzigen SQL-Anweisung und einem Cluster

Das folgende Beispiel verwendet die AWS CLI , um eine EventBridge Regel zu erstellen, die verwendet wird, um eine SQL-Anweisung für einen Amazon Redshift Redshift-Cluster auszuführen.

```
aws events put-rule
--name test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

Dann wird ein EventBridge Ziel erstellt, das nach dem in der Regel angegebenen Zeitplan ausgeführt wird.

```
aws events put-targets
--cli-input-json file://data.json
```

Die data.json-Eingabedatei ist wie folgt. Der JSON-Schlüssel `Sql` gibt an, dass es nur eine einzige SQL-Anweisung gibt. Der JSON-Wert `Arn` enthält eine Clusterkennung. Der JSON-Wert `RoleArn` enthält die IAM-Rolle, die verwendet wird, um SQL wie zuvor beschrieben auszuführen.

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

Aufrufen mit einer einzigen SQL-Anweisung und einer Arbeitsgruppe

Das folgende Beispiel verwendet die AWS CLI , um eine EventBridge Regel zu erstellen, die verwendet wird, um eine SQL-Anweisung für eine Amazon Redshift Serverless-Arbeitsgruppe auszuführen.

```
aws events put-rule
--name  test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

Dann wird ein EventBridge Ziel erstellt, das nach dem in der Regel angegebenen Zeitplan ausgeführt wird.

```
aws events put-targets
--cli-input-json file://data.json
```

Die data.json-Eingabedatei ist wie folgt. Der JSON-Schlüssel `Sql` gibt an, dass es nur eine einzige SQL-Anweisung gibt. Der JSON-Wert `Arn` enthält einen Arbeitsgruppennamen. Der JSON-Wert `RoleArn` enthält die IAM-Rolle, die verwendet wird, um SQL wie zuvor beschrieben auszuführen.

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

Aufrufen mit mehreren SQL-Anweisungen und einem Cluster

Das folgende Beispiel verwendet die AWS CLI , um eine EventBridge Regel zu erstellen, die verwendet wird, um mehrere SQL-Anweisungen für einen Amazon Redshift Redshift-Cluster auszuführen.

```
aws events put-rule
--name  test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

Dann wird ein EventBridge Ziel erstellt, das nach dem in der Regel angegebenen Zeitplan ausgeführt wird.

```
aws events put-targets
--cli-input-json file://data.json
```

Die data.json-Eingabedatei ist wie folgt. Der JSON-Schlüssel `Sqls` gibt an, dass es mehrere SQL-Anweisungen gibt. Der JSON-Wert `Arn` enthält eine Clusterkennung. Der JSON-Wert `RoleArn` enthält die IAM-Rolle, die verwendet wird, um SQL wie zuvor beschrieben auszuführen.

```
{
    "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
            }
```

```
        }
    ]
}
```

Aufrufen mit mehreren SQL-Anweisungen und einer Arbeitsgruppe

Das folgende Beispiel verwendet die AWS CLI , um eine EventBridge Regel zu erstellen, die verwendet wird, um mehrere SQL-Anweisungen für eine Amazon Redshift Serverless-Arbeitsgruppe auszuführen.

```
aws events put-rule
--name  test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

Dann wird ein EventBridge Ziel erstellt, das nach dem in der Regel angegebenen Zeitplan ausgeführt wird.

```
aws events put-targets
--cli-input-json file://data.json
```

Die data.json-Eingabedatei ist wie folgt. Der JSON-Schlüssel `Sqls` gibt an, dass es mehrere SQL-Anweisungen gibt. Der JSON-Wert `Arn` enthält einen Arbeitsgruppennamen. Der JSON-Wert `RoleArn` enthält die IAM-Rolle, die verwendet wird, um SQL wie zuvor beschrieben auszuführen.

```
{
    "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
            }
        }
    ]
```

```
}
```

Überwachen der Data API

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung der Daten-API und Ihrer anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um die Daten-API zu überwachen, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon EventBridge kann verwendet werden, um Ihre AWS Services zu automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Ereignisse aus AWS Services werden nahezu EventBridge in Echtzeit zugestellt. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis mit einer Regel übereinstimmt. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen zur Integration von Amazon Redshift finden Sie unter Logging with CloudTrail. AWS CloudTrail Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

Themen

- Überwachung von Ereignissen für die Amazon Redshift Data API in Amazon EventBridge

Überwachung von Ereignissen für die Amazon Redshift Data API in Amazon EventBridge

Sie können Daten-API-Ereignisse überwachen EventBridge, wodurch ein Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, software-as-a-service (SaaS-) Anwendungen und AWS Diensten bereitgestellt wird. EventBridge leitet diese Daten an Ziele wie AWS Lambda Amazon SNS weiter. Bei diesen Ereignissen handelt es sich um dieselben Ereignisse wie unter CloudWatch Ereignisse. Dadurch wird ein Strom von Systemereignissen nahezu in Echtzeit bereitgestellt, die Änderungen an Ressourcen beschreiben. AWS Ereignisse werden an das Konto gesendet, das die Amazon-Redshift-

Datenbank enthält. Wenn Sie beispielsweise eine Rolle in einem anderen Konto übernehmen, werden Ereignisse an dieses Konto gesendet. Weitere Informationen finden Sie unter EventBridge Amazon-Veranstaltungen im EventBridge Amazon-Benutzerhandbuch. .

Data-API-Ereignisse werden gesendet, wenn der API-Vorgang `ExecuteStatement` oder `BatchExecuteStatement` die Option `WithEvent` auf `true` festlegt. Das `state`-Feld des Ereignisses enthält einen der folgenden Werte:

- ABBORTED – Die Abfrage wurde vom Benutzer gestoppt.
- FAILED – Die Ausführung der Abfrage ist fehlgeschlagen.
- FINISHED – Die Ausführung der Abfrage ist abgeschlossen.

Ereignisse werden garantiert geliefert. Weitere Informationen finden Sie unter Events from AWS services im EventBridge Amazon-Benutzerhandbuch.

Beispiel für abgeschlossenes Data-API-Ereignis

Das folgende Beispiel zeigt ein Ereignis für die Data API, wenn der API-Vorgang `ExecuteStatement` abgeschlossen ist. Im folgenden Beispiel hat eine Anweisung namens `test.testtable` die Ausführung abgeschlossen.

```
{
    "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
    }
```

```
}
```

Amazon-Redshift-Parametergruppen

Übersicht

In Amazon Redshift verknüpfen Sie mit jedem von Ihnen erstellten Cluster eine Parametergruppe. Eine Parametergruppe ist eine Gruppe von Parametern, die für alle Datenbanken gelten, die Sie im Cluster erstellen. Diese Parameter konfigurieren Datenbankeinstellungen wie Abfrage-Timeout oder Datumsstil.

Über Parametergruppen

Jede Parametergruppe enthält verschiedene Parameter für die Konfiguration von Einstellungen für die Datenbank. Die Liste der verfügbaren Parameter hängt von der Parametergruppenfamilie ab, zu der die Parametergruppe gehört. Die Parametergruppenfamilie ist die Version der Amazon-Redshift-Engine, für die die Parameter in der Parametergruppe gelten. Das Namensformat für die Parametergruppenfamilie ist `redshift-`*`version`*, wobei *`Version`* die Engine-Version ist. Die aktuelle Version der Konfiguration ist z. B. `redshift-1.0`.

Amazon Redshift stellt eine Standard-Parametergruppe für jede Parametergruppenfamilie bereit. Die Standard-Parametergruppe enthält voreingestellte Werte für jeden ihrer Parameter und kann nicht verändert werden. Das Format der Standardparametergruppe ist `default.`*`parameter_group_family`*, wobei *`parameter_group_family`* die Version der Engine ist, zu der die Parametergruppe gehört. Beispielsweise hat die Standard-Parametergruppe für die Version `redshift-1.0` die Bezeichnung `default.redshift-1.0`.

> **Note**
>
> Zurzeit ist `redshift-1.0` die einzige Version der Amazon-Redshift-Engine. Daher ist `default.redshift-1.0` die einzige Standard-Parametergruppe.

Wenn Sie von der Standard-Parametergruppe abweichende Parameterwerte verwenden müssen, müssen Sie eine benutzerdefinierte Parametergruppe erstellen und Ihrem Cluster zuweisen. Anfänglich sind die Parameterwerte in einer benutzerdefinierten Parametergruppe mit denen der Standard-Parametergruppe identisch. Die anfängliche `source` für alle Parameter ist `engine-default`, da die Werte von Amazon Redshift voreingestellt sind. Nach der Änderung eines

Parameterwertes wechselt die `source` zu `user`, um anzuzeigen, dass der Wert gegenüber dem Standardwert geändert wurde.

> **Note**
>
> Die Amazon-Redshift-Konsole zeigt nicht die `source` jedes Parameters an. Sie müssen die Amazon Redshift API, die AWS CLI oder einen der AWS-SDKs verwenden, um die `source` anzuzeigen.

Für von Ihnen erstellte Parametergruppen können Sie Parameterwerte jederzeit ändern oder alle Parameterwerte auf ihre Standardwerte zurücksetzen. Sie können auch eine andere Parametergruppe mit einem Cluster verbinden. In einigen Fällen bearbeiten Sie Parameterwerte in einer Parametergruppe, die bereits mit einem Cluster verbunden ist, oder verbinden eine andere Parametergruppe mit einem Cluster. In diesen Fällen müssen Sie den Cluster neu starten, damit die aktualisierten Parameterwerte übernommen werden. Wenn der Cluster ausfällt und von Amazon Redshift neu gestartet wird, werden Ihre Änderungen zu diesem Zeitpunkt angewendet. Wenn der Cluster während der Wartung neu gestartet wird, werden die Änderungen nicht übernommen. Weitere Informationen finden Sie unter Dynamische und statische WLM-Eigenschaften.

Standard-Parameterwerte

Die nachfolgende Tabelle zeigt die Standard-Parameterwerte auf einen Blick mit Links zu eingehenderen Informationen zu jedem Parameter. Dies sind die Standardwerte für die `redshift-1.0`-Parametergruppenfamilie.

Parametername	Wert	Weitere Informationen
auto_analyze	true	auto_analyze im Datenbankentwicklerhandbuch zu Amazon Redshift
auto_mv	true	Automatisierte materialisierte Ansichten im Datenbankentwicklerhandbuch zu Amazon Redshift
datestyle	ISO, MDY	datestyle im Datenbankentwicklerhandbuch zu Amazon Redshift

Parametername	Wert	Weitere Informationen
enable_case_sensitive_identifier	false	enable_case_sensitive_identifier im Datenbankentwicklerhandbuch zu Amazon Redshift
enable_user_activity_logging	false	Datenbank-Prüfungsprotokollierung in dieser Anleitung
extra_float_digits	0	extra_float_digits im Datenbankentwicklerhandbuch zu Amazon Redshift
max_concurrency_scaling_clusters	1	max_concurrency_scaling_clusters im Datenbankentwicklerhandbuch zu Amazon Redshift
query_group	default	query_group im Datenbankentwicklerhandbuch zu Amazon Redshift
require_ssl	false	Konfigurieren von Sicherheitsoptionen für Verbindungen in dieser Anleitung
search_path	$user, public	search_path im Datenbankentwicklerhandbuch zu Amazon Redshift
statement_timeout	0	statement_timeout im Datenbankentwicklerhandbuch zu Amazon Redshift
wlm_json_configuration	[{"auto_wlm":true}]	Workload-Management-Konfiguration in dieser Anleitung
use_fips_ssl	false	Aktivieren Sie den FIPS-konformen SSL-Modus nur, wenn Ihr System FIPS-konform sein muss.

> **Note**
>
> Der Parameter `max_cursor_result_set_size` ist veraltet. Weitere Informationen zur Größe des Cursor-Ergebnissatzes finden Sie unter Einschränkungen für Cursors im Datenbankentwicklerhandbuch zu Amazon Redshift.

Sie können einen Parameter vorübergehend übergehen, indem Sie den Befehl `SET` in der Datenbank verwenden. Durch den Befehl `SET` wird der Parameter nur für die Dauer Ihrer aktuellen Sitzung übergangen. Zusätzlich zu den in der obigen Tabelle aufgeführten Parametern können Sie auch die Slot-Zahl vorübergehend anpassen, indem Sie `wlm_query_slot_count` in der Datenbank einstellen. Der Parameter `wlm_query_slot_count` steht nicht zur Konfiguration in Parametergruppen zur Verfügung. Weitere Informationen zur Anpassung der Slotzahl finden Sie unter wlm_query_slot_count im Datenbankentwicklerhandbuch zu Amazon Redshift. Weitere Informationen zum vorübergehenden Überschreiben der anderen Parameter finden Sie unter Modifizieren der Serverkonfiguration im Datenbankentwicklerhandbuch zu Amazon Redshift.

Konfiguration von Parameterwerten mit der AWS CLI

Um Amazon-Redshift-Parameter mittels der AWS CLI zu konfigurieren, verwenden Sie den `modify-cluster-parameter-group`-Befehl für eine spezifische Parametergruppe. Sie geben die zu modifizierende Parametergruppe in `parameter-group-name` an. Sie verwenden den Parameter `parameters` (für den Befehl `modify-cluster-parameter-group`) zur Angabe von Name/Wert-Paaren für jeden Parameter, den Sie in der Parametergruppe modifizieren möchten.

> **Note**
>
> Beim Konfigurieren des Parameters `wlm_json_configuration` mittels der AWS CLI müssen einige besondere Punkte beachtet werden. Die Beispiele in diesem Abschnitt gelten für alle Parameter mit Ausnahme von `wlm_json_configuration`. Weitere Informationen zum Konfigurieren von `wlm_json_configuration` mittels der AWS CLI finden Sie unter Workload-Management-Konfiguration.

Nach der Modifizierung von Parameterwerten müssen Sie alle Cluster neu starten, die mit der modifizierten Parametergruppe verbunden sind. Der Clusterstatus zeigt `applying` für `ParameterApplyStatus` an, während die Werte angewendet werden, und dann `pending-reboot`, nachdem sie angewendet wurden. Nach dem Neustart beginnen die Datenbanken in Ihrem Cluster mit der Verwendung der neuen Parameterwerte. Weitere Informationen zum Neustarten von Clustern finden Sie unter Neustart eines Clusters.

> **Note**
>
> Der Parameter `wlm_json_configuration` enthält einige Eigenschaften, die dynamisch sind und nicht erfordern, dass Sie verbundene Cluster neu starten, damit die Änderungen

angewendet werden. Für weitere Informationen zu dynamischen und statischen Eigenschaften vgl. Dynamische und statische WLM-Eigenschaften.

Syntax

Die folgende Syntax illustriert die Verwendung des Befehls `modify-cluster-parameter-group` zur Konfiguration eines Parameters. Sie geben *`parameter_group_name`* ein und ersetzen *`parameter_name`* und *`parameter_value`* durch einen tatsächlichen zu ändernden Parameter und einen Wert für diesen Parameter. Wenn Sie mehr als einen Parameter gleichzeitig modifizieren möchten, trennen Sie jeden Parameter-/Wert-Satz vom nächsten durch ein Leerzeichen.

```
aws redshift modify-cluster-parameter-group --parameter-group-name parameter_group_name
 --parameters ParameterName=parameter_name,ParameterValue=parameter_value
```

Beispiel

Das folgende Beispiel illustriert die Konfiguration der Parameter `statement_timeout` und `enable_user_activity_logging` für die Parametergruppe `myclusterparametergroup`.

> **Note**
>
> Zur besseren Lesbarkeit wird das Beispiel auf mehreren Zeilen dargestellt, in der tatsächlichen AWS CLI ist dies jedoch nur eine Zeile.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name myclusterparametergroup
--parameters ParameterName=statement_timeout,ParameterValue=20000
 ParameterName=enable_user_activity_logging,ParameterValue=true
```

Sie können Parametergruppen über die Konsole verwalten. Weitere Informationen finden Sie unter Verwaltung von Parametergruppen mit der Konsole.

Workload-Management-Konfiguration

In Amazon Redshift verwenden Sie Workload Management (WLM), um festzulegen, wie viele Abfragewarteschlangen verfügbar sind und wie Abfragen zur Verarbeitung an diese Warteschlangen

geleitet werden. WLM ist Teil der Parametergruppenkonfiguration. Ein Cluster verwendet die WLM-Konfiguration, die in seiner zugehörigen Parametergruppe angegeben ist.

Wenn Sie eine Parametergruppe erstellen, enthält die Standard-WLM-Konfiguration eine Warteschlange, die bis zu fünf Abfragen gleichzeitig enthalten kann. Sie können weitere Warteschlangen hinzufügen und in jeder davon WLM-Eigenschaften konfigurieren, wenn Sie die Abfrageverarbeitung besser steuern möchten. Jede von Ihnen hinzugefügte Warteschlange hat dieselbe Standard-WLM-Konfiguration, bis Sie ihre Eigenschaften konfigurieren.

Wenn Sie weitere Warteschlangen hinzufügen, ist die letzte Warteschlange in der Konfiguration die Standardwarteschlange. Sofern keine Abfrage auf der Grundlage der Kriterien in der WLM-Konfiguration zu einer anderen Warteschlange geleitet wird, wird sie von der Standard-Warteschlange verarbeitet. Sie können für die Standardwarteschlange Modus und Nebenläufigkeitsstufe (Abfrageslots) angeben, jedoch keine Benutzer- oder Abfragegruppen.

Wie bei anderen Parametern auch können Sie die WLM-Konfiguration in der Standard-Parametergruppe nicht ändern. Mit der Standard-Parametergruppe verbundene Cluster verwenden immer die Standard-WLM-Konfiguration. Zum Ändern der WLM-Konfiguration erstellen Sie eine neue Parametergruppe und verknüpfen diese mit allen Clustern, die die benutzerdefinierte WLM-Konfiguration erfordern.

Dynamische und statische WLM-Eigenschaften

Die WLM-Konfigurationseigenschaften sind dynamisch oder statisch. Sie können dynamische Eigenschaften ohne Neustart des Clusters auf die Datenbank anwenden. Statische Eigenschaften erfordern jedoch einen Neustart des Clusters, damit die Änderungen wirksam werden. Weitere Informationen zu statischen und dynamischen Eigenschaften finden Sie unter Dynamische und statische WLM-Konfigurationseigenschaften.

Eigenschaften des Parameters wlm_json_configuration

Sie können WLM über die Amazon-Redshift-Konsole, die AWS CLI, die Amazon Redshift API oder einen der AWS-SDKs konfigurieren. Die WLM-Konfiguration nutzt verschiedene Eigenschaften zur Definition des Warteschlangenverhaltens, wie etwa die Speicherzuweisung unter den Warteschlangen, die Anzahl der gleichzeitig in einer Warteschlange ausführbaren Abfragen usw.

> **Note**
>
> Die folgenden Eigenschaften werden mit ihren Amazon-Redshift-Konsolennamen und den entsprechenden JSON-Eigenschaftennamen in den Beschreibungen aufgeführt.

Die folgende Tabelle zeigt, ob eine Eigenschaft auf automatisches WLM oder manuelles WLM angewendet werden kann.

WLM-Eigenschaft	Automatisches WLM	Manuelles WLM
Automatisches WLM	Ja	Ja
Aktivieren der Beschleunigung kurzer Abfragen	Ja	Ja
Maximale Laufzeit für kurze Abfragen	Ja	Ja
Priorität	Ja	Nein
Warteschlangentyp	Ja	Ja
Queue name (Name der Warteschlange)	Ja	Ja
Concurrency Scaling mode (Nebenläufigkeitsskalierung smodus)	Ja	Ja
Nebenläufigkeit	Nein	Ja
Benutzergruppen	Ja	Ja
Benutzergruppenplatzhalter	Ja	Ja
Abfragegruppen	Ja	Ja
Abfragegruppenplatzhalter	Ja	Ja

WLM-Eigenschaft	Automatisches WLM	Manuelles WLM
Benutzerrollen	Ja	Ja
Platzhalter für die Benutzerrolle	Ja	Ja
Zeitüberschreitung	Nein	Als veraltet gekennzeichnet
Arbeitsspeicher	Nein	Ja
Query Monitoring Rules (Abfrageüberwachungsregeln)	Ja	Ja

Die folgende Liste enthält Beschreibungen der WLM-Eigenschaften, die Sie konfigurieren können.

Automatisches WLM

Automatisches WLM auf `true` gesetzt, aktiviert das automatische WLM. Automatisches WLM legt die Werte für Concurrency on main (Nebenläufigkeit auf dem Haupt-Cluster) und Memory (%) (Arbeitsspeicher (%)) auf `Auto` fest. Amazon Redshift verwaltet die Abfragenebenläufigkeit und die Arbeitsspeicherzuweisung. Der Standardwert ist `true`.

JSON-Eigenschaft: `auto_wlm`

Aktivieren von Short Query Acceleration

Wenn Sie Short Query Acceleration (SQA) verwenden, werden ausgewählte, kurze Abfragen gegenüber Abfragen mit einer höheren Dauer priorisiert. SQA führt kurze Abfragen an einer dedizierten Stelle aus, sodass SQA-Abfragen nicht hinter längeren Abfragen in Warteschlangen eingereiht werden. Mit SQA werden kürzere Abfragen schneller ausgeführt und der Benutzer sieht schneller Ergebnisse. Wenn Sie SQA aktivieren, können Sie auch die maximale Laufzeit für kurze Abfragen festlegen. Legen Sie den Wert `true` fest, um SQA zu aktivieren. Der Standardwert ist `false`. Diese Einstellung wird für die einzelnen Parametergruppen, nicht für die Warteschlangen angewendet.

JSON-Eigenschaft: `short_query_queue`

Maximum run time for short queries (Maximale Laufzeit für kurze Abfragen)

Wenn Sie SQA aktivieren, können Sie 0 angeben, damit WLM dynamisch die maximale Laufzeit für kurze Abfragen festlegt. Alternativ können Sie einen Wert zwischen 1 und 20 Sekunden in Millisekunden angeben. Der Standardwert ist `0`.

JSON-Eigenschaft: `max_execution_time`

Priority (Priorität)

Im Feld „Priority“ (Priorität) wird die Priorität der Abfragen festgelegt, die in einer Warteschlange ausgeführt werden. Um die Priorität festzulegen, muss WLM mode (WLM-Modus) auf Auto WLM (Automatisches WLM) festgelegt werden, d. h., `auto_wlm` muss `true` sein. Die Prioritätswerte können `highest`, `high`, `normal`, `low` und `lowest` sein. Der Standardwert ist `normal`.

JSON-Eigenschaft: `priority`

Queue type (Warteschlangentyp)

Der Warteschlangentyp bezeichnet eine Warteschlange als entweder von Auto WLM (Automatisches WLM) oder Manual WLM (Manuelles WLM) verwendet. Legen Sie `queue_type` auf `auto` oder `manual` fest. Wenn nichts angegeben ist, ist der Standardwert `manual`.

JSON-Eigenschaft: `queue_type`

Queue name (Name der Warteschlange)

Der Name der Warteschlange. Sie können den Namen der Warteschlange entsprechend Ihren geschäftlichen Anforderungen festlegen. Warteschlangennamen müssen innerhalb einer WLM-Konfiguration eindeutig sein und können bis zu 64 alphanumerische Zeichen, Unterstriche oder Leerzeichen enthalten. Sie dürfen keine Anführungszeichen enthalten. Wenn es beispielsweise eine Warteschlange für Ihre ETL-Abfragen gibt, können Sie sie mit `ETL queue` benennen. Dieser Name wird in Metriken, Systemtabellenwerten und in der Amazon-Redshift-Konsole zur Identifizierung der Warteschlange verwendet. Abfragen und Berichte, die den Namen aus diesen Quellen verwenden, müssen Änderungen des Namens verarbeiten können. Zuvor wurden die Warteschlangennamen von Amazon Redshift generiert. Die Standardnamen von Warteschlangen sind `Queue 1`, `Queue 2` bis zur letzten Warteschlange mit dem Namen `Default queue`.

> **Important**
>
> Wenn Sie einen Warteschlangennamen ändern, ändert sich auch der `QueueName` Dimensionswert von WLM-Warteschlangenmetriken (z. B. WLM QueueLength, WLM QueueWaitTime, WLM QueriesCompletedPerSecond, WLM QueryDuration, WLM

RunningQueriesusw.). Wenn Sie also den Namen einer Warteschlange ändern, müssen Sie möglicherweise CloudWatch Alarme ändern, die Sie eingerichtet haben.

JSON-Eigenschaft: `name`

Concurrency Scaling mode (Nebenläufigkeitsskalierungsmodus)

Zur Aktivierung der Nebenläufigkeitsskalierung für eine Warteschlange setzen Sie Concurrency Scaling mode (Nebenläufigkeitsskalierungsmodus) auf `auto`. Wenn die Anzahl der an eine Warteschlange geleiteten Abfragen die konfigurierte Nebenläufigkeit der Warteschlange überschreitet, werden berechtigte Abfragen an den Skalierungs-Cluster gesendet. Wenn Slots verfügbar werden, werden Abfragen auf dem Haupt-Cluster ausgeführt. Der Standardwert ist `off`.

JSON-Eigenschaft: `concurrency_scaling`

Concurrency (Nebenläufigkeit)

Die Anzahl der Abfragen, die gleichzeitig in einer manuellen WLM-Warteschlange ausgeführt werden können. Diese Eigenschaft gilt nur für manuelles WLM. Wenn für eine Warteschlange die Nebenläufigkeitsskalierung aktiviert ist, werden berechtigte Abfragen an einen Skalierungs-Cluster gesendet, wenn eine Warteschlange die Nebenläufigkeitsstufe (Abfrageslots) erreicht hat. Wenn die Nebenläufigkeitsskalierung nicht aktiviert ist, warten Abfragen in der Warteschlange, bis ein Slot verfügbar wird. Der Bereich liegt zwischen 1 und 50.

JSON-Eigenschaft: `query_concurrency`

User Groups (Benutzergruppen)

Eine durch Kommata getrennte Liste von Benutzergruppennamen. Wenn Mitglieder der Benutzergruppe Abfragen in der Datenbank ausführen, werden deren Abfragen zu der Warteschlange geleitet, die zu der Benutzergruppe gehört.

JSON-Eigenschaft: `user_group`

User Group Wildcard (Benutzergruppenplatzhalter)

Ein boolescher Wert, der angibt, ob Platzhalter für Benutzergruppen aktiviert werden sollen. Beim Wert 0 werden Platzhalter deaktiviert, beim Wert 1 werden sie aktiviert. Wenn Platzhalter aktiviert sind, können Sie „*“ oder „?“ verwenden, um beim Ausführen von Abfragen mehrere Benutzergruppen anzugeben. Weitere Informationen finden Sie unter Platzhalter.

JSON-Eigenschaft: `user_group_wild_card`

Query Groups (Abfragegruppen)

Eine durch Kommata abgeteilte Liste von Abfragegruppen. Wenn Mitglieder der Abfragegruppe Abfragen in der Datenbank ausführen, werden deren Abfragen zu der Warteschlange geleitet, die zu der Abfragegruppe gehört.

JSON-Eigenschaft: `query_group`

Query Group Wildcard (Abfragegruppenplatzhalter)

Ein boolescher Wert, der angibt, ob Platzhalter für Abfragegruppen aktiviert werden sollen. Beim Wert 0 werden Platzhalter deaktiviert, beim Wert 1 werden sie aktiviert. Wenn Platzhalter aktiviert sind, können Sie „*“ oder „?“ verwenden, um beim Ausführen von Abfragen mehrere Abfragegruppen anzugeben. Weitere Informationen finden Sie unter Platzhalter.

JSON-Eigenschaft: `query_group_wild_card`

Benutzerrollen

Eine durch Kommata getrennte Liste von Benutzerrollen. Wenn Mitglieder mit dieser Benutzerrolle Abfragen in der Datenbank ausführen, werden deren Abfragen zu der Warteschlange geleitet, die zu ihrer Benutzerrolle gehört. Weitere Informationen zu Benutzerrollen finden Sie unter Rollenbasierte Zugriffskontrolle (RBAC).

JSON-Eigenschaft: `user_role`

Platzhalter für die Benutzerrolle

Ein boolescher Wert, der angibt, ob Platzhalter für Abfragegruppen aktiviert werden sollen. Beim Wert 0 werden Platzhalter deaktiviert, beim Wert 1 werden sie aktiviert. Wenn Platzhalter aktiviert sind, können Sie „*“ oder „?“ verwenden, um beim Ausführen von Abfragen mehrere Abfragegruppen anzugeben. Weitere Informationen finden Sie unter Platzhalter.

JSON-Eigenschaft: `user_role_wild_card`

Timeout (ms)

WLM-Timeout (`max_execution_time`) ist veraltet. Die Funktion ist bei Verwendung von automatischem WLM nicht verfügbar. Erstellen Sie stattdessen eine Abfrageüberwachungsregel (Query Monitoring Rule, QMR) `query_execution_time` zur Begrenzung der Ausführungszeit für eine Abfrage. Weitere Informationen finden Sie unter WLM-Abfrageüberwachungsregeln.

Die maximale Zeit, in Millisekunden, für die Abfragen ausgeführt werden können, bevor sie abgebrochen werden. In einigen Fällen wird eine schreibgeschützte Abfrage, z. B. eine

SELECT-Anweisung, aufgrund einer WLM-Zeitüberschreitung abgebrochen. In diesen Fällen versucht WLM, die Abfrage auf Grundlage der WLM-Warteschlangenzuweisungsregeln an die nächste übereinstimmende Warteschlange weiterzuleiten. Wenn die Abfrage keiner anderen Warteschlangendefinition entspricht, wird sie abgebrochen und nicht der Standardwarteschlange zugewiesen. Weitere Informationen finden Sie unter WLM-Abfragewarteschlangen-Hopping. Das WLM-Timeout gilt nicht für eine Abfrage, die den Status `returning` erreicht hat. Den Status einer Abfrage finden Sie in der Systemtabelle STV_WLM_QUERY_STATE.

JSON-Eigenschaft: `max_execution_time`

Memory (%) (Arbeitsspeicher)

Der Prozentsatz des Speicherplatzes, der der Warteschlange zuzuweisen ist. Wenn Sie für mindestens eine der Warteschlangen einen Speicherprozentsatz festlegen, müssen Sie einen Prozentsatz für alle weiteren Warteschlangen bis zu einem Gesamtwert von 100 Prozent angeben. Wenn die Speicherzuweisung für alle Warteschlangen unter 100 Prozent liegt, wird der nicht zugewiesene Speicher vom Service verwaltet. Der Service kann den nicht zugewiesenen Speicher vorübergehend der Warteschlange zur Verfügung stellen, die zusätzlichen Speicher zur Verarbeitung benötigt.

JSON-Eigenschaft: `memory_percent_to_use`

Query Monitoring Rules (Abfrageüberwachungsregeln)

Mit WLM-Abfrageüberwachungsregeln können Sie Ihre WLM-Warteschlangen kontinuierlich auf der Grundlage von Kriterien bzw. Prädikaten, die Sie angeben, auf Abfragen überwachen. Sie können beispielsweise Abfragen überwachen, die dazu neigen, ein Übermaß an Systemressourcen zu beanspruchen, und dann eine angegebene Aktion initiieren, wenn eine Anfrage die von Ihnen angegebenen Leistungsgrenzen verletzt.

> **Note**
>
> Wenn Sie Regeln auf programmatischen Wege erstellen, empfehlen wir nachdrücklich, die Konsole zu verwenden, um die JSON-Elemente zu erstellen, die Sie in der Parametergruppendefinition verwenden.

Sie weisen eine Abfrageüberwachungsregel einer bestimmten Abfragewarteschlange zu. Sie können bis zu 25 Regeln pro Warteschlange und insgesamt 25 Regeln für alle Warteschlangen festlegen.

JSON-Eigenschaft: `rules`

Hierarchie der JSON-Eigenschaften:

```
rules
    rule_name
    predicate
        metric_name
        operator
        value
    action
        value
```

Für jede Regel geben Sie die folgenden Eigenschaften an:

- `rule_name` – Regelnamen müssen innerhalb einer WLM-Konfiguration eindeutig sein. Regelnamen können aus bis zu 32 alphanumerischen Zeichen oder Unterstrichen bestehen und dürfen keine Leerzeichen oder Anführungszeichen enthalten. Sie können bis zu acht Regeln pro Warteschlange und insgesamt acht Regeln für alle Warteschlangen einrichten.
  - `predicate` – Sie können bis zu drei Prädikate pro Regel verwenden. Für jedes Prädikat geben Sie die folgenden Eigenschaften an.
    - `metric_name` – Eine Liste der Metriken finden Sie unter Abfrageüberwachungsmetriken im Datenbankentwicklerhandbuch zu Amazon Redshift.
    - `operator` – Vorgänge sind =, < und >.
    - `value` – Der Schwellenwert für die angegebene Metrik, der eine Aktion auslöst.
- `action` – Jede Regel ist einer einzigen Aktion zugeordnet. Gültige Aktionen sind:
  - `log`
  - hop (nur bei Verwendung von manuellem WLM verfügbar)
  - `abort`
  - `change_query_priority` (nur bei Verwendung von automatischem WLM verfügbar)

Das folgende Beispiel zeigt den JSON-Code für eine WLM-Abfrageüberwachungsregel mit der Bezeichnung `rule_1`, mit zwei Prädikaten und der Aktion 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"
        }
      ]
```

Weitere Informationen zu den einzelnen Eigenschaften und Strategien für die Konfiguration von Abfragewarteschlangen finden Sie unter Implementierung von Workload Management im Datenbankentwicklerhandbuch zu Amazon Redshift.

Konfiguration des Parameters wlm_json_configuration mit der AWS CLI

Zur Konfiguration von WLM modifizieren Sie den Parameter `wlm_json_configuration`. Die maximale Größe des `wlm_json_configuration`-Eigenschaftswerts beträgt 8 000 Zeichen. Der Wert ist in JavaScript Object Notation (JSON) formatiert. Wenn Sie WLM mit der AWS CLI, der Amazon Redshift API oder einem der AWS-SDKs konfigurieren, lesen Sie den Rest dieses Abschnitts, um zu erfahren, wie Sie die JSON-Struktur für den Parameter `wlm_json_configuration` aufbauen.

> **Note**
>
> Wenn Sie WLM mit der Amazon-Redshift-Konsole konfigurieren, müssen Sie nicht mit der JSON-Formatierung vertraut sein, da die Konsole eine einfache Möglichkeit zum Hinzufügen von Warteschlangen und zur Konfiguration ihrer Eigenschaften bietet. Weitere Informationen zur Konfiguration von WLM mit der Konsole finden Sie unter Modifizieren einer Parametergruppe.

Beispiel

Das folgende Beispiel ist die WLM-Standardkonfiguration, die eine Warteschlange mit automatischem WLM definiert.

```
{
   "auto_wlm": true
}
```

Beispiel

Das folgende Beispiel ist eine benutzerdefinierte WLM-Konfiguration, die eine manuelle WLM-Warteschlange mit der Nebenläufigkeitsstufe fünf (Abfrageslots) definiert.

```
{
   "query_concurrency":5
}
```

Syntax

Die Standard-WLM-Konfiguration ist sehr einfach, mit nur einer Warteschlange und einer Eigenschaft. Sie können weitere Warteschlangen hinzufügen und für jede Warteschlange in der JSON-Struktur mehrere Eigenschaften konfigurieren. Die folgende Syntax zeigt die JSON-Struktur, die Sie für die Konfiguration mehrerer Warteschlangen mit mehreren Eigenschaften verwenden:

```
[
   {
      "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",
                ...
             }
             ...

         ]"
   }
```

```
]
```

Im vorherigen Beispiel sind die repräsentativen Eigenschaften, die mit q1 beginnen, Objekte in einem Array für die erste Warteschlange. Jedes dieser Objekte ist ein Name-/Wert-Paar; `name` und `value` richten gemeinsam die WLM-Eigenschaften für die erste Warteschlange ein. Die repräsentativen Eigenschaften, die mit q2 beginnen, sind Objekte in einem Array für die zweite Warteschlange. Wenn Sie mehr Warteschlangen benötigen, fügen Sie ein weiteres Array für jede weitere Warteschlange hinzu und richten die Eigenschaften für jedes Objekt ein.

Wenn Sie die WLM-Konfiguration modifizieren, müssen Sie die gesamte Struktur für Ihre Warteschlangen einschließen, selbst wenn Sie nur eine Eigenschaft in einer Warteschlange ändern möchten. Der Grund dafür ist, dass die gesamte JSON-Struktur als Zeichenfolge als Wert für den Parameter `wlm_json_configuration` übergeben wird.

Formatieren des AWS CLI-Befehls

Der Parameter `wlm_json_configuration` muss ein spezifisches Format haben, wenn Sie die AWS CLI verwenden. Das verwendete Format hängt von Ihrem Client-Betriebssystem ab. Betriebssysteme schließen die JSON-Struktur auf unterschiedliche Weise ein, damit sie korrekt von der Befehlszeile übergeben wird. Für Einzelheiten zur Konstruktion des korrekten Befehls unter Linux, Mac OS X und Windows vgl. die folgenden Abschnitte. Weitere Informationen zu den Unterschieden beim Einschließen von JSON-Datenstrukturen in der AWS CLI im Allgemeinen finden Sie unter Setzen von Anführungszeichen für Zeichenfolgen im AWS Command Line Interface-Benutzerhandbuch.

Beispiele

Mit dem folgenden Beispielbefehl wird für eine Parametergruppe mit dem Namen `example-parameter-group` manuelles WLM konfiguriert. Die Konfiguration lässt die Beschleunigung für kurze Abfragen mit einer maximalen Laufzeit von 0 Sekunden zu. Dadurch wird WLM angewiesen, den Wert dynamisch festzulegen. Die `ApplyType`-Einstellung lautet `dynamic`. Diese Einstellung bedeutet, dass alle an dynamischen Eigenschaften in dem Parameter vorgenommenen Änderungen sofort angewendet werden, sofern keine anderen statischen Änderungen an der Konfiguration vorgenommen wurden. Die Konfiguration definiert drei Warteschlangen mit:

- Die erste Warteschlange ermöglicht Benutzern, `report` als Beschriftung (wie in der Eigenschaft `query_group` angegeben) in ihren Abfragen anzugeben, um die Abfragen leichter zu dieser Warteschlange weiterleiten zu können. Platzhaltersuchen sind für die Beschriftung `report*` aktiviert, so dass die Beschriftung nicht exakt sein muss, damit Abfragen zur Warteschlange

geleitet werden. Beispielsweise entsprechen sowohl `reports` als auch `reporting` dieser Abfragegruppe. Der Warteschlange sind 25 Prozent des gesamten Speicherplatzes für alle Warteschlangen zugewiesen, und es können bis zu vier Abfragen gleichzeitig ausgeführt werden. Abfragen sind auf eine maximale Ausführungszeit von 20 000 Millisekunden (ms) begrenzt. Der Modus ist auf automatisch festgelegt. Berechtigte Abfragen werden daher an ein Skalierungs-Cluster gesendet, wenn die Abfrage-Slots der Warteschlange gefüllt sind.

- Die zweite Warteschlange ermöglicht Benutzern, die Mitglieder der Gruppe `admin` oder `dba` in der Datenbank sind, ihre Abfragen zur Verarbeitung zu der Warteschlange weiterzuleiten. Platzhaltersuchen sind für Benutzergruppen deaktiviert, die Benutzer müssen daher exakt Gruppen in der Datenbank entsprechen, damit ihre Abfragen zu der Warteschlange geleitet werden. Der Warteschlange werden 40 Prozent des gesamten Speicherplatzes für alle Warteschlangen zugeteilt. Sie kann bis zu fünf Abfragen gleichzeitig ausführen. Der Modus ist auf „Off“ (Aus) festgelegt. Daher werden alle Abfragen, die von Mitgliedern der Administrator- oder DBA-Gruppe gesendet werden, auf dem Haupt-Cluster ausgeführt.
- Die letzte Warteschlange in der Konfiguration ist die Standard-Warteschlange. Dieser Warteschlange sind 35 Prozent des gesamten Speicherplatzes für alle Warteschlangen zugewiesen. Sie kann bis zu fünf Abfragen gleichzeitig verarbeiten. Der Modus ist auf „Auto“ (Automatisch) festgelegt.

> **Note**
>
> Das Beispiel wird zu Demonstrationszwecken auf mehreren Zeilen angezeigt. Die tatsächlichen Befehle haben jedoch keine Zeilenumbrüche.

```
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}
]'
```

Im Folgenden sehen Sie ein Beispiel für die Konfiguration von WLM-Abfrageüberwachungsregeln für eine automatische WLM-Konfiguration. In diesem Beispiel wird eine Parametergruppe mit dem Namen `example-monitoring-rules` erstellt. Die Konfiguration definiert die gleichen drei Warteschlangen wie im vorherigen Beispiel. `query_concurrency` und `memory_percent_to_use` werden jedoch nicht mehr angegeben. Die Konfiguration fügt darüber hinaus die folgenden Regeln und Abfrageprioritäten hinzu:

- Die erste Warteschlange definiert eine Regel mit der Bezeichnung `rule_1`. Die Regel hat zwei Prädikate: `query_cpu_time > 10000000` und `query_blocks_read > 1000`. Die Regelaktion ist `log` . Diese Warteschlange hat die Priorität `Normal`.
- Die zweite Warteschlange definiert eine Regel mit dem Namen `rule_2`. Die Regel hat zwei Prädikate: `query_execution_time > 600000000` und `scan_row_count > 1000000000`. Die Regelaktion ist `abort` . Diese Warteschlange hat die Priorität `Highest`.
- Die letzte Warteschlange in der Konfiguration ist die Standard-Warteschlange. Diese Warteschlange hat die Priorität `Low`.

> **Note**
>
> Das Beispiel wird zu Demonstrationszwecken auf mehreren Zeilen angezeigt. Die tatsächlichen Befehle haben jedoch keine Zeilenumbrüche.

```
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
} ]'
```

Konfigurieren von WLM mithilfe der AWS CLI in der Befehlszeile mit einer JSON-Datei

Sie können den Parameter `wlm_json_configuration` mithilfe der AWS CLI ändern und den Wert des Arguments `parameters` als JSON-Datei übergeben.

```
aws redshift modify-cluster-parameter-group --parameter-group-name
 myclusterparaametergroup --parameters file://modify_pg.json
```

Die Argumente für `--parameters` werden in der Datei `modify_pg.json` gespeichert: Der Speicherort der Datei wird in dem Format für Ihr Betriebssystem angegeben. Weitere Informationen finden Sie unter Laden von Parametern aus einer Datei. Es folgen Beispiele für den Inhalt der JSON–Datei `modify_pg.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"
    }
]
```

Regeln für die Konfiguration von WLM mit der AWS CLI in der Befehlszeile unter Linux und macOS X

Beachten Sie die folgenden Regeln, wenn Sie einen AWS CLI-Befehl mit Parametern in einer Zeile ausführen möchten:

- Die gesamte JSON-Struktur muss in einfache Anführungszeichen (') und einem Satz Klammern ([ ]) eingeschlossen werden.
- Alle Parameternamen und Parameterwerte müssen in doppelte Anführungszeichen (") eingeschlossen werden.
- Innerhalb des `ParameterValue`-Werts müssen Sie die gesamte eingebettete Struktur in doppelte Anführungszeichen (") und Klammern ([ ]) einschließen.
- Innerhalb der eingebetteten Struktur müssen alle Eigenschaften und Werte für jede Warteschlange in geschweifte Klammern ({ }) eingeschlossen werden.

- Innerhalb der eingebetteten Struktur müssen Sie den umgekehrten Schrägstrich (\) als Escape-Zeichen vor jedem doppelten Anführungszeichen (") verwenden.
- Für Name-/Wert-Paare trennt ein Doppelpunkt (:) jede Eigenschaft von ihrem Wert.
- Alle Name-/Wert-Paare werden voneinander durch Kommata (,) getrennt.
- Mehrere Warteschlangen werden durch ein Komma (,) zwischen der schließenden geschweiften Klammer einer Warteschlange (}) und der öffnenden geschweiften Klammer der nächsten Warteschlange getrennt.

Regeln für die Konfiguration von WLM unter Verwendung der AWS CLI unter Windows PowerShell unter Microsoft Windows-Betriebssystemen

Beachten Sie die folgenden Regeln, wenn Sie einen AWS CLI-Befehl mit Parametern in einer Zeile ausführen möchten:

- Die gesamte JSON-Struktur muss in einfache Anführungszeichen (') und einem Satz Klammern ([ ]) eingeschlossen werden.
- Alle Parameternamen und Parameterwerte müssen in doppelte Anführungszeichen (") eingeschlossen werden.
- Innerhalb des `ParameterValue`-Werts müssen Sie die gesamte eingebettete Struktur in doppelte Anführungszeichen (") und Klammern ([ ]) einschließen.
- Innerhalb der eingebetteten Struktur müssen alle Eigenschaften und Werte für jede Warteschlange in geschweifte Klammern ({ }) eingeschlossen werden.
- Innerhalb der eingebetteten Struktur müssen Sie den umgekehrten Schrägstrich (\) als Escape-Zeichen vor jedem doppelten Anführungszeichen (") und dessen Escape-Zeichen (umgekehrter Schrägstrich (\)) verwenden. Dies bedeutet, dass Sie drei umgekehrte Schrägstriche und ein doppeltes Anführungszeichen verwenden müssen, um sicherzustellen, dass die Eigenschaften korrekt übergeben werden („\\\“).
- Für Name-/Wert-Paare trennt ein Doppelpunkt (:) jede Eigenschaft von ihrem Wert.
- Alle Name-/Wert-Paare werden voneinander durch Kommata (,) getrennt.
- Mehrere Warteschlangen werden durch ein Komma (,) zwischen der schließenden geschweiften Klammer einer Warteschlange (}) und der öffnenden geschweiften Klammer der nächsten Warteschlange getrennt.

Regeln für die Konfiguration von WLM mit der Befehlszeile in Windows-Betriebssystemen

Beachten Sie die folgenden Regeln, wenn Sie einen AWS CLI-Befehl mit Parametern in einer Zeile ausführen möchten:

- Die gesamte JSON-Struktur muss in doppelte Anführungszeichen (") und einem Satz Klammern ([ ]) eingeschlossen werden.
- Alle Parameternamen und Parameterwerte müssen in doppelte Anführungszeichen (") eingeschlossen werden.
- Innerhalb des `ParameterValue`-Werts müssen Sie die gesamte eingebettete Struktur in doppelte Anführungszeichen (") und Klammern ([ ]) einschließen.
- Innerhalb der eingebetteten Struktur müssen alle Eigenschaften und Werte für jede Warteschlange in geschweifte Klammern ({ }) eingeschlossen werden.
- Innerhalb der eingebetteten Struktur müssen Sie den umgekehrten Schrägstrich (\) als Escape-Zeichen vor jedem doppelten Anführungszeichen (") und dessen Escape-Zeichen (umgekehrter Schrägstrich (\)) verwenden. Dies bedeutet, dass Sie drei umgekehrte Schrägstriche und ein doppeltes Anführungszeichen verwenden müssen, um sicherzustellen, dass die Eigenschaften korrekt übergeben werden („\\\“).
- Für Name-/Wert-Paare trennt ein Doppelpunkt (:) jede Eigenschaft von ihrem Wert.
- Alle Name-/Wert-Paare werden voneinander durch Kommata (,) getrennt.
- Mehrere Warteschlangen werden durch ein Komma (,) zwischen der schließenden geschweiften Klammer einer Warteschlange (}) und der öffnenden geschweiften Klammer der nächsten Warteschlange getrennt.

Verwaltung von Parametergruppen mit der Konsole

Sie können Parametergruppen in der Amazon-Redshift-Konsole anzeigen, erstellen, ändern und löschen.

Sie können jede Ihrer Parametergruppen anzeigen, um eine Zusammenfassung der Werte für die Konfiguration von Parametern und Workload Management (WLM) zu erhalten. Gruppenparameter werden auf der Registerkarte Parameters (Parameter) und Workload queues (Workload-Warteschlagen) auf der Registerkarte Workload Management (Workload-Management) angezeigt.

Erstellen einer Parametergruppe

Wenn Sie Parameterwerte einstellen möchten, die sich von der Standardparametergruppe unterscheiden, können Sie eine eigene Parametergruppe anlegen,

So erstellen Sie eine Parametergruppe:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Configurations (Konfigurationen) und dann Workload management (Workload-Management) aus, um die Seite Workload management (Workload-Management) anzuzeigen.
3. Wählen Sie Create (Erstellen) aus, um das Fenster Create parameter group (Parametergruppe erstellen) anzuzeigen.
4. Geben Sie einen Wert für Parameter group name (Parametergruppenname) und Description (Beschreibung) ein.
5. Wählen Sie Create (Erstellen) aus, um die Parametergruppe zu erstellen.

Modifizieren einer Parametergruppe

Sie können Parameter modifizieren, um die Parametereinstellungen und die WLM-Konfigurationseigenschaften zu ändern.

> **Note**
>
> Die Standard-Parametergruppe kann nicht modifiziert werden.

So ändern Sie eine Parametergruppe:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Configurations (Konfigurationen) und dann Workload management (Workload-Management) aus, um die Seite Workload management (Workload-Management) anzuzeigen.

3. Wählen Sie die Parametergruppe aus, die Sie ändern möchten, um die Detailseite mit Registerkarten für Parameters (Parameter) und Workload management (Workload-Management) anzuzeigen.
4. Wählen Sie die Registerkarte Parameters (Parameter) aus, um die aktuellen Parametereinstellungen anzuzeigen.
5. Wählen Sie Edit parameters (Parameter bearbeiten) aus, um die Änderung der Einstellungen für diese Parameter zu aktivieren:

   - `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`

   Weitere Informationen zu diesen Parametern finden Sie unter Amazon-Redshift-Parametergruppen.
6. Geben Sie Ihre Änderungen ein und wählen Sie dann Save (Speichern) aus, um die Parametergruppe zu aktualisieren.

So ändern Sie die WLM-Konfiguration für eine Parametergruppe:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.

2. Wählen Sie im Navigationsmenü Configurations (Konfigurationen) und dann Workload management (Workload-Management) aus, um die Seite Workload management (Workload-Management) anzuzeigen.
3. Wählen Sie die Parametergruppe aus, die Sie ändern möchten, um die Detailseite mit Registerkarten für Parameters (Parameter) und Workload management (Workload-Management) anzuzeigen.
4. Wählen Sie die Registerkarte Workload management (Workload-Management) aus, um die aktuelle WLM-Konfiguration anzuzeigen.
5. Wählen Sie Edit workload queues (Workload-Warteschlangen bearbeiten) aus, um die WLM-Konfiguration zu bearbeiten,
6. (Optional) Wählen Sie Enable short query acceleration (Beschleunigen von kurzen Abfragen aktivieren) aus, um Short Query Acceleration (SQA) zu aktivieren.

   Wenn Sie SQA aktivieren, wird Maximum run time for short queries (1 to 20 seconds) (Maximale Laufzeit für kurze Abfragen (1 bis 20 Sekunden)) auf Dynamic (Dynamisch) festgelegt. Um die maximale Laufzeit auf einen festen Wert festzulegen, wählen Sie einen Wert zwischen 1 und 20.
7. Nehmen Sie eine der folgenden Aktionen vor, um die Warteschlangenkonfiguration zu modifizieren:

   - Wählen Sie Switch WLM mode (WLM-Modus wechseln) aus, um zwischen Automatic WLM (Automatisches WLM) und Manual WLM (Manuelles WLM) zu wählen.

     Mit Automatic WLM (Automatisches WLM) werden die Werte Memory (Arbeitsspeicher) und Concurrency on main (Parallelität auf Main) auf Auto gesetzt.
   - Um eine Warteschlange zu erstellen, wählen Sie Edit workload queues (Workload-Warteschlangen bearbeiten) und dann Add Queue (Warteschlange hinzufügen) aus.
   - Um eine Warteschlange zu modifizieren, ändern Sie Eigenschaftenwerte in der Tabelle. Je nach Warteschlangentyp können die folgenden Eigenschaften vorhanden sein:
     - Der Warteschlangenname kann geändert werden.
     - Memory (%) (Arbeitsspeicher)
     - Gleichzeitigkeit auf dem Haupt-Cluster
     - Concurrency scaling mode (Parallelitätsskalierungsmodus) kann off (aus) oder Auto sein.
     - Timeout (ms)
     - Benutzergruppen
     - Abfragegruppen

- Benutzerrollen

Weitere Informationen zu diesen Eigenschaften finden Sie unter Eigenschaften des Parameters wlm_json_configuration.

> **Important**
>
> Wenn Sie einen Warteschlangennamen ändern, ändert sich auch der `QueueName` Dimensionswert der WLM-Warteschlangenmetriken (wie WLMQueueLength, WLMQueueWaitTime, WLMQueriesCompletedPerSecond, WLMQueryDuration, WLM usw.)RunningQueries. Wenn Sie also den Namen einer Warteschlange ändern, müssen Sie möglicherweise die von Ihnen eingerichteten Alarme ändern CloudWatch .

- Um die Reihenfolge der Warteschlangen zu ändern, wählen Sie die Hoch- und Runter-Pfeilschaltflächen aus.
- Um eine Warteschlange zu löschen, wählen Sie Delete (Löschen) in der Zeile der Warteschlange in der Tabelle aus.

8. (Optional) Wählen Sie Defer dynamic changes until reboot (Dynamische Änderungen bis zum Neustart verschieben) aus, damit die Änderungen nach dem nächsten Neustart auf die Cluster angewendet werden.

> **Note**
>
> Einige Änderungen erfordern auch unabhängig von dieser Einstellung einen Neustart des Clusters. Weitere Informationen finden Sie unter Dynamische und statische WLM-Eigenschaften.

9. Wählen Sie Save (Speichern) aus.

Erstellen oder Modifizieren einer Abfrageüberwachungsregel mit der Konsole

Sie können die Amazon-Redshift-Konsole verwenden, um WLM-Abfrageüberwachungsregeln zu erstellen und zu ändern. Abfrageüberwachungsregeln sind Teil des WLM-Konfigurationsparameters für eine Parametergruppe. Wenn Sie eine Abfrageüberwachungsregel (Query Monitoring Rule, QMR) ändern, erfolgt die Änderung automatisch, ohne dass der Cluster geändert werden muss. Weitere Informationen finden Sie unter WLM-Abfrageüberwachungsregeln.

Wenn Sie eine Regel erstellen, definieren Sie den Namen der Regel, ein oder mehrere Prädikate und eine Aktion.

Wenn Sie eine WLM-Konfiguration speichern, die eine Regel enthält, können Sie den JSON-Code für die Regeldefinition als JSON-Teil für den WLM-Konfigurationsparameter anzeigen.

So erstellen Sie eine Abfrageüberwachungsregel:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Configurations (Konfigurationen) und dann Workload management (Workload-Management) aus, um die Seite Workload management (Workload-Management) anzuzeigen.
3. Wählen Sie die Parametergruppe aus, die Sie ändern möchten, um die Detailseite mit Registerkarten für Parameters (Parameter) und Workload management (Workload-Management) anzuzeigen.
4. Wählen Sie die Registerkarte Workload management (Workload-Management) aus und wählen Sie Edit workload queues (Workload-Warteschlangen bearbeiten) aus, um die WLM-Konfiguration zu bearbeiten,
5. Fügen Sie eine neue Regel hinzu (entweder mit Hilfe einer vordefinierten Vorlage oder von Grund auf neu).

   Um eine vordefinierte Vorlage zu verwenden, gehen Sie wie folgt vor:

   1. Wählen Sie Add rule from template (Regel aus Vorlage hinzufügen) in der Gruppe Query monitoring rules (Überwachungsregeln abfragen) aus. Die Liste der Regelvorlagen wird angezeigt.
   2. Wählen Sie eine oder mehrere Regelvorlagen. Wenn Sie Save (Speichern) auswählen, erstellt WLM eine Regel für jede ausgewählte Vorlage.
   3. Geben Sie Werte für die Regel ein oder bestätigen Sie diese, einschließlich Rule name (Regelname), Predicates (Prädikate) und Actions (Aktionen).
   4. Wählen Sie Speichern.

   Um eine neue Regel von Grund auf neu hinzuzufügen, gehen Sie wie folgt vor:

1. Um weitere Prädikate hinzuzufügen, wählen Sie Add predicate (Prädikat hinzufügen) aus. Sie können bis zu drei Prädikate für jede Regel haben. Wenn alle Prädikate erfüllt sind, löst WLM die zugehörige Aktion aus.
2. Wählen Sie eine Action (Aktion) aus. Zu jeder Regel gehört eine Aktion.
3. Wählen Sie Speichern.

Amazon Redshift generiert Ihren WLM-Konfigurationsparameter im JSON-Format und zeigt ihn im Bereich JSON an.

Löschen einer Parametergruppe

Sie können eine Parametergruppe löschen, wenn Sie sie nicht mehr benötigen und sie nicht mit einem Cluster verbunden ist. Sie können nur benutzerdefinierte Parametergruppen löschen.

So löschen Sie eine Parametergruppe:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Configurations (Konfigurationen) und dann Workload management (Workload-Management) aus, um die Seite Workload management (Workload-Management) anzuzeigen.
3. Wählen Sie unter Parameter groups (Parametergruppen) die Parametergruppe aus, die Sie ändern möchten.

   > **Note**
   >
   > Die Standard-Parametergruppe kann nicht gelöscht werden.

4. Wählen Sie Delete (Löschen) aus und bestätigen Sie, dass Sie die Parametergruppe löschen möchten.

Zuordnung einer Parametergruppe zu einem Cluster

Wenn Sie einen Cluster starten, müssen Sie ihn mit einer Parametergruppe verbinden. Wenn Sie die Parametergruppe später ändern möchten, können Sie den Cluster modifizieren und eine andere Parametergruppe auswählen.

Verwalten von Parametergruppen mit der AWS CLI und der Amazon Redshift API

Sie können zur Verwaltung von Parametergruppen die folgenden Amazon-Redshift-Vorgänge in der AWS CLI verwenden.

- 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

Sie können zur Verwaltung von Parametergruppen die folgenden Amazon Redshift API-Vorgänge verwenden.

- CreateClusterParameterGroup
- DeleteClusterParameterGroup
- DescribeClusterParameters
- DescribeClusterParameterGroups
- DescribeDefaultClusterParameters
- ModifyClusterParameterGroup
- ResetClusterParameterGroup

Integration von Amazon Redshift mit einem Partner AWS

Wenn Sie mit Amazon Redshift arbeiten, können Sie über die Seite mit den Cluster-Details in der Amazon Redshift Redshift-Konsole eine Integration mit AWS Partnern durchführen. Auf der Seite mit den Cluster-Details können Sie das Onboarding Ihrer Daten in Ihr Amazon Redshift Redshift-Data Warehouse mit AWS Partneranwendungen beschleunigen. Sie können auch Daten aus verschiedenen Quellen zusammen mit vorhandenen Daten in Ihrem Cluster verknüpfen und analysieren. Vor Abschluss der Integration in Informatica müssen Sie die IP-Adressen des Partners der Zulassungsliste für eingehenden Datenverkehr hinzufügen. Die folgenden AWS Partner können Amazon Redshift integrieren:

- Datacoral
- Etleap
- Fivetran
- SnapLogic
- Stitch
- Upsolver
- Matillion (Vorversion)
- Sisense (Vorversion)
- Thoughtspot

AWS Partner können Amazon Redshift mithilfe der API-Operationen AWS CLI oder Amazon Redshift integrieren. Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz oder der Amazon-Redshift-API-Referenz.

Integration mit einem AWS Partner über die Amazon Redshift Redshift-Konsole

Gehen Sie wie folgt vor, um einen Cluster mit einem AWS Partner zu integrieren.

Um einen Amazon Redshift Redshift-Cluster mit einem AWS Partner zu integrieren

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.

2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus.
3. Wählen Sie den Cluster aus, den Sie integrieren möchten.
4. Klicken Sie auf Add partner integration (Partnerintegration hinzufügen). Die Seite Partner auswählen wird mit Details zu den verfügbaren AWS Partnern geöffnet.
5. Wählen Sie einen AWS Partner aus und klicken Sie dann auf Weiter.

   Weitere Details zum ausgewählten AWS Partner werden angezeigt, zusammen mit Details zu dem Cluster, den Sie integrieren. Der Abschnitt Clusterdetails enthält Informationen, die Sie auf der AWS Partner-Website angeben, z. B. die Cluster-ID, den Endpunkt, den Datenbanknamen und den Benutzernamen (bei dem es sich um einen Datenbankbenutzernamen handelt). Diese Informationen werden an den von Ihnen ausgewählten Partner gesendet.
6. Wählen Sie Partner hinzufügen, um die Website des AWS Partners zu öffnen.
7. Konfigurieren Sie die Integration mit Ihrem Amazon-Redshift-Cluster auf der Website des Partners. Auf der Website des Partners können Sie die Datenquellen auswählen und konfigurieren, die in Ihren Amazon-Redshift-Cluster geladen werden. Sie können auch zusätzliche ELT-Transformationen (Extract, Load and Transform) definieren, um Ihre Geschäftsdaten zu verarbeiten, sie mit anderen Datensätzen zu verknüpfen und konsolidierte Ansichten für Analysen und Berichte zu erstellen.

Sie können AWS Partnerintegrationen auf der Registerkarte Eigenschaften der Clusterdetails anzeigen und verwalten. Im Abschnitt Integrationen sind der Partnername aufgeführt, mit dem Sie auf die AWS Partner-Website verlinken können, der Status der Integration, die Datenbank, die die Daten empfängt, und die letzte erfolgreiche Verbindung, die den Cluster möglicherweise aktualisiert hat.

Die möglichen Statuswerte lauten wie folgt:

- Aktiv — Der AWS Partner kann eine Verbindung zum Cluster herstellen und konfigurierte Aufgaben ausführen.
- Inaktiv — Die AWS Partnerintegration ist nicht vorhanden.
- Laufzeitfehler — Der AWS Partner kann eine Verbindung zum Cluster herstellen, aber konfigurierte Aufgaben nicht abschließen.
- Verbindungsfehler — Der AWS Partner kann keine Verbindung zum Cluster herstellen.

Nachdem Sie eine AWS Partnerintegration aus Amazon Redshift gelöscht haben, fließen weiterhin Daten in Ihren Cluster. Schließen Sie den Löschvorgang auf der Website des Partners ab.

Daten mit AWS Partnern werden geladen

Neben der Integration eines Partners in einen Amazon-Redshift-Cluster haben Sie auch die Möglichkeit, mithilfe der Datenladetools unseres Partners Daten aus mehr als 30 Quellen in Ihren Amazon-Redshift-Cluster zu verschieben. Bevor Sie dies tun, müssen Sie die IP-Adressen des Partners (siehe unten) der Zulassungsliste der Regeln für eingehenden Datenverkehr hinzufügen. Informationen zum Hinzufügen von Regeln zu einer Amazon-EC2-Sicherheitsgruppe finden Sie unter Autorisieren von eingehendem Datenverkehr für Ihre Instances im Amazon-EC2-Benutzerhandbuch für Linux-Instances. Beachten Sie, dass das Tool Informatica Data Loader zwar kostenlos ist, jedoch Gebühren für den Dateneingang anfallen können, je nachdem, welche Datenquellen und -ziele Sie auswählen.

Sie können Daten von folgenden Partnern laden:

- Informatica – IP-Adressen

So integrieren Sie einen Amazon-Redshift-Cluster mit Informatica

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü AWS Partnerintegration und dann den Partner aus, mit dem Sie Ihren Cluster integrieren möchten.
3. Wählen Sie Complete <partner-name> integration (Integration von <Partnername> durchführen) aus. Sie werden auf die Integrationssite des Partners weitergeleitet.
4. Geben Sie die erforderlichen Details auf der Website des Partners ein und führen Sie die Integration durch.

Kaufen reservierter Amazon-Redshift-Knoten

Übersicht

In AWS, die Gebühren, die Ihnen für die Nutzung von Amazon Redshift anfallen, basieren auf Rechenknoten. Jeder Datenverarbeitungsknoten wird auf stündlicher Basis abgerechnet. Der stündliche Preis ist von Faktoren wie Region, Knotentyp und davon abhängig, ob für den Knoten On-Demand-Preise oder Preise für reservierte Knoten gelten.

On-Demand-Knotenpreise sind die teuerste, aber flexibelste Option in Amazon Redshift. Bei On-Demand-Preisen werden Ihnen nur Datenverarbeitungsknoten in ausgeführten Clustern berechnet. Wenn Sie ein Cluster abschalten oder löschen, werden Ihnen Datenverarbeitungsknoten in diesem Cluster nicht mehr berechnet. Ihnen werden nur Datenverarbeitungsknoten berechnet, die Sie nutzen, und keine weiteren. Der stündliche Preis, die Ihnen für die einzelnen Datenverarbeitungsknoten berechnet wird, ist von Faktoren wie Region und Knotentyp abhängig.

Reserved Node-Preise sind günstiger als On-Demand-Preise, da die Datenverarbeitungsknoten zu rabattierten stündlichen Preisen berechnet werden. Um diese rabattierten Preise zu erhalten, müssen Sie jedoch Lösungen mit reservierten Knoten kaufen. Wenn Sie eine Lösung kaufen, führen Sie eine Reservierung aus. Die Reservierung legt für jeden von Ihnen reservierten Knoten während der Dauer der Reservierung einen rabattierten Preis fest. Der rabattierte Preis für eine Lösung ist von Faktoren wie Region, Knotentyp, Dauer und Zahlungsoptionen abhängig.

Sie können einen Knoten als reservierten Knoten festlegen, indem Sie den API-Vorgang `PurchaseReservedNodeOffering` aufrufen oder in der Amazon Redshift-Konsole Purchase reserved nodes (Reservierte Knoten erwerben) auswählen. Wenn Sie einen reservierten Knoten kaufen, müssen Sie eine AWS Region, einen Knotentyp, eine Laufzeit, die Anzahl der Knoten und den Angebotstyp für den jeweiligen reservierten Knotentyp angeben. Der reservierte Knoten darf nur in der angegebenen AWS Region verwendet werden.

In diesem Thema wird beschrieben, was unter Angeboten reservierter Knoten verstanden wird und wie Sie diese kaufen können, um die Kosten Ihrer Amazon-Redshift-Cluster zu reduzieren. In diesem Thema werden die Preise in allgemeiner Weise als bedarfsbasiert (on-demand) oder rabattiert beschrieben, sodass Sie die Preiskonzepte und die Auswirkungen von Preisen auf die Abrechnung verstehen können. Weitere Informationen zu spezifischen Preisen finden Sie unter Amazon-Redshift-Preise.

Über Angebote reservierter Knoten

Wenn Ihr Amazon-Redshift-Cluster kontinuierlich über einen längeren Zeitraum ausgeführt werden soll, sollten Sie den Kauf von Angeboten reservierter Knoten in Betracht ziehen. Diese Lösungen bieten im Vergleich zu On-Demand-Preisen deutliche Einsparungen. Sie erfordern jedoch die Reservierung von Datenverarbeitungsknoten und die Verpflichtung, für ein Jahr oder drei Jahre für diese Knoten zu bezahlen.

Reservierte Knoten sind ein Abrechnungskonzept, das ausschließlich dazu verwendet wird, den Preis festzulegen, der Ihnen für Knoten berechnet wird. Durch die Reservierung eines Knotens wird dieser nicht für Sie erstellt. Reservierte Knoten werden Ihnen unabhängig von der Nutzung berechnet. Das bedeutet, dass Sie für jeden Knoten, den Sie während der Dauer der Reservierung reservieren, bezahlen müssen, unabhängig davon, ob Sie Knoten in einem ausgeführten Cluster ausführen, für das der rabattierte Preis gilt.

Während der Evaluierungsphase Ihres Projekts oder der Entwicklung eines Machbarkeitsnachweises, erhalten Sie mit On-Demand-Preisen die nötige Flexibilität, um nur für das zu bezahlen, was Sie verwenden. Sie können die Zahlung jederzeit einstellen, indem Sie Cluster abschalten oder löschen. Nachdem Sie die Anforderungen Ihrer Produktionsumgebung festgelegt und die Implementierungsphase begonnen haben, sollten Sie die Reservierung von Datenverarbeitungsknoten in Betracht ziehen, indem Sie eine oder mehrere Lösungen kaufen.

Eine Lösung kann für einen oder mehrere Datenverarbeitungsknoten gelten. Sie geben beim Kauf der Lösung die Anzahl der Datenverarbeitungsknoten an, die reserviert werden sollen. Sie können eine einzelne Lösung für mehrere Datenverarbeitungsknoten kaufen oder mehrere Lösungen kaufen und in jeder Lösung eine bestimmte Anzahl von Datenverarbeitungsknoten angeben.

Jede der folgenden Möglichkeiten ist für den Kauf einer Lösung für drei Datenverarbeitungsknoten zulässig:

- Kauf einer einzelnen Lösung und Angabe von drei Datenverarbeitungsknoten.
- Kauf von zwei Lösungen und Angabe eines einzelnen Datenverarbeitungsknotens für die erste Lösung und von zwei Datenverarbeitungsknoten für die zweite Lösung.
- Kauf von drei Lösungen und Angabe eines einzelnen Datenverarbeitungsknotens für jede der drei Lösungen.

Vergleich der Preise für Lösungen mit reservierten Knoten

Amazon Redshift stellt verschiedene Zahlungsoptionen für Angebote bereit. Die von Ihnen gewählte Zahlungsoption wirkt sich auf den Zahlungsplan und den rabattierten Preis aus, der Ihnen für die Reservierung berechnet wird. Je mehr Sie im Voraus für die Reservierung zahlen, desto größer sind die Einsparungen insgesamt.

Für die Lösungen stehen folgende Zahlungsoptionen zur Verfügung: Die Lösungen werden in der Reihenfolge der Höhe der Einsparungen im Vergleich zu On-Demand-Preisen angezeigt, von den niedrigsten bis zu den höchsten Einsparungen.

> **Note**
>
> Ihnen wird der jeweilige Stundensatz für jede Stunde in der angegebenen Dauer der Reservierung berechnet, unabhängig davon, ob Sie den reservierten Knoten verwenden oder nicht. Die Zahlungsoption legt lediglich die Häufigkeit der Zahlungen und den jeweils gültigen Rabatt fest. Weitere Informationen finden Sie unter Über Angebote reservierter Knoten.

Vergleich von Angeboten reservierter Knoten

Zahlungsoption	Zahlungsplan	Vergleich der Einsparungen	Dauer	Vorabkosten	Wiederkehrende monatliche Kosten
Keine Vorabzahlung	Monatliche Teilzahlungen für die Dauer der Reservierung. Keine Vorauszahlung.	Ein Rabatt von ungefähr 20 Prozent im Vergleich zu On-Demand-Preisen.	Laufzeit von einem Jahr oder drei Jahren	None	Ja
Teilweise Vorauszahlung	Zum Teil Vorauszahlung, zum Teil monatliche Teilzahlungen für die Dauer der Reservierung.	Zwischen 41 Prozent und 73 Prozent Rabatt, abhängig von der Dauer.	Laufzeit von einem Jahr oder drei Jahren	Ja	Ja

Zahlungsoption	Zahlungsplan	Vergleich der Einsparungen	Dauer	Vorabkosten	Wiederkehrende monatliche Kosten
Komplette Vorauszahlung	Reservierung wird vollständig im Voraus bezahlt. Keine monatliche Kosten.	Zwischen 42 Prozent und 76 Prozent Rabatt, abhängig von der Dauer.	Laufzeit von einem Jahr oder drei Jahren	Ja	None

Die spezifischen Optionen und Laufzeiten sind abhängig von der Verfügbarkeit.

> **Note**
>
> Wenn Sie zuvor Heavy Utilization (Starke Auslastung)-Angebote für Amazon Redshift gekauft haben, ist das Angebot Partial Upfront (Teilweise im Voraus) vergleichbar.

So funktionieren reservierte Knoten:

Im Fall von Lösungen mit reservierten Knoten zahlen Sie entsprechend den Zahlungsbedingungen, die im vorherigen Abschnitt beschrieben wurden. Sie zahlen auf diese Weise unabhängig davon, ob Sie bereits ein Cluster ausführen oder nach einer Reservierung ein Cluster starten.

Wenn Sie eine Lösung kaufen, hat Ihre Reservierung den Status payment-pending (Zahlung ausstehend), bis die Reservierung verarbeitet wurde. Wenn die Reservierung nicht verarbeitet werden kann, wird der Status als payment-failed (Zahlung nicht erfolgreich) angezeigt und Sie können den Vorgang wiederholen. Wenn die Reservierung erfolgreich verarbeitet wurde, wird der Status in active (aktiv) geändert. Der jeweilige rabattierte Preis in Ihrer Reservierung wird erst auf Ihre Rechnung angewendet, wenn der Status in active (aktiv) geändert wird. Wenn die Reservierungsdauer abgelaufen ist, wird der Status in retired (abgelaufen) geändert. Sie können jedoch weiterhin auf Informationen zur Reservierung zugreifen, um den Verlauf zu überprüfen. Wenn sich eine Reservierung im Status retired (abgelaufen) befindet, werden Ihre Cluster weiter ausgeführt. Ihnen wird jedoch möglicherweise der On-Demand-Preis berechnet, wenn Sie keine andere Reservierung besitzen, durch die rabattierte Preise auf die Knoten angewendet werden.

Reservierte Knoten sind für die Region spezifisch, in der Sie die Lösung gekauft haben. Wenn Sie ein Angebot mithilfe der Amazon Redshift Redshift-Konsole erwerben, wählen Sie die AWS Region aus, in der Sie ein Angebot erwerben möchten, und schließen Sie dann den Reservierungsvorgang ab. Wenn Sie ein Angebot programmgesteuert kaufen, wird die Region durch den Amazon-Redshift-Endpunkt festgelegt, mit dem Sie sich verbinden. Weitere Informationen zu Amazon-Redshift-Regionen finden Sie unter Regionen und Endpunkte in der Allgemeine Amazon Web Services-Referenz.

Um sicherzustellen, dass der rabattierte Preis auf alle Knoten angewendet wird, wenn Sie ein Cluster starten, müssen die Region, der Knotentyp und die Zahl der von Ihnen ausgewählten Knoten mit mindestens einer aktiven Reservierung übereinstimmen. Andernfalls wird Ihnen der On-Demand-Preis für Knoten berechnet, die mit keiner aktiven Reservierung übereinstimmen.

Wenn Sie in einem ausgeführten Cluster die Anzahl der Knoten überschreiten, die Sie reserviert haben, wird Ihnen für diese zusätzlichen Knoten der On-Demand-Preis berechnet. Das bedeutet, dass es möglich ist, dass Ihnen für Knoten im selben Cluster unterschiedliche Preise berechnet werden, abhängig davon, wie viele Knoten Sie reserviert haben. Sie können eine weitere Lösung kaufen, um diese zusätzlichen Knoten abzudecken. Anschließend wird der rabattierte Preis für die restliche Dauer der Reservierung auf diese Knoten angewendet, sobald der Reservierungsstatus in active (aktiv) geändert wird.

Wenn Sie Ihr Cluster in einen anderen Knotentyp ändern und Sie keine Knoten dieses Typs reserviert haben, wird Ihnen der On-Demand-Preis berechnet. Sie können eine weitere Lösung mit dem neuen Knotentyp kaufen, wenn Sie für Ihr Cluster mit dem neuen Knotentyp rabattierte Preise erhalten möchten. Sie zahlen jedoch weiter für die ursprüngliche Reservierung, bis diese abgelaufen ist. Wenn Sie Ihre Reservierungen vor ihrem Ablauf ändern müssen, erstellen Sie bitte in der AWS -Konsole einen Supportfall.

Reservierte Knoten und konsolidierte Fakturierung

Die Preisvorteile von reservierten Knoten werden geteilt, wenn das kaufende Konto Teil eines Satzes von Konten ist, die unter einem einzigen, konsolidierten Zahlerkonto abgerechnet werden. Der Stundensatz für alle Unterkonten wird jeden Monat im Zahlerkonto zusammengefasst. Dies ist in der Regel für Unternehmen nützlich, in denen es verschiedene Funktionsteams oder -gruppen gibt. Zur Berechnung der Abrechnung wird die normale Logik für reservierte Konten angewendet. Weitere Informationen finden Sie unter Konsolidierte Fakturierung im AWS Billing Benutzerhandbuch.

Beispiele für reservierte Knoten

Die Szenarien in diesem Abschnitt zeigen, wie für Knoten Kosten auf der Basis von On-Demand-Preisen und rabattierten Preisen entstehen können. Dabei werden die folgenden Reservierungsdetails verwendet:

- Region: USA West (Oregon)
- Knotentyp: ra3.xlplus
- Zahlungsoption: keine Vorauszahlung
- Dauer: ein Jahr
- Anzahl der reservierten Knoten: 16

Beispiel 1

Sie haben einen Cluster in der Region USA West (Oregon) mit 20 Knoten.

In diesem Szenario erhalten 16 Knoten den rabattierten Preis aus der Reservierung. Die zusätzlichen 4 Knoten im Cluster werden jedoch zum On-Demand-Preis abgerechnet.

Beispiel 2

Sie haben einen Cluster in der Region USA West (Oregon) mit 12 Knoten.

In diesem Szenario werden alle 12 Knoten im Cluster zum rabattierten Preis aus der Reservierung abgerechnet. Sie zahlen jedoch auch für die übrigen reservierten Knoten in der Reservierung, auch wenn Sie zurzeit kein Cluster ausführen, für das sie verwendet werden.

Beispiel 3

Sie haben einen Cluster in der Region USA West (Oregon) mit 12 Knoten. Sie führen den Cluster über mehrere Monate mit dieser Konfiguration aus und müssen dem Cluster anschließend Knoten hinzufügen. Sie ändern die Größe des Clusters, wählen den gleichen Knotentyp aus und geben insgesamt 16 Knoten an.

In diesem Szenario wird Ihnen der rabattierte Preis für 16 Knoten berechnet. Ihre Kosten bleiben für das gesamte Jahr gleich, da die Zahl der Knoten im Cluster gleich der Zahl der von Ihnen reservierten Knoten ist.

Beispiel 4

Sie haben einen Cluster in der Region USA West (Oregon) mit 16 Knoten. Sie führen den Cluster über mehrere Monate mit dieser Konfiguration aus und müssen anschließend Knoten hinzufügen. Sie ändern die Größe des Clusters, wählen den gleichen Knotentyp aus und geben insgesamt 20 Knoten an.

In diesem Szenario wird Ihnen vor der Änderung der Größe für alle Knoten der rabattierte Preis berechnet. Nach der Änderung der Größe wird Ihnen für den Rest des Jahres der rabattierte Preis für 16 Knoten berechnet. Für die zusätzlichen 4 Knoten, die Sie dem Cluster hinzugefügt haben, wird Ihnen der On-Demand-Preis berechnet.

Beispiel 5

Sie haben zwei Cluster in der Region USA West (Oregon). Ein Cluster hat 6 Knoten und das andere Cluster hat 10 Knoten.

In diesem Szenario wird Ihnen für alle Knoten der rabattierte Preis berechnet, da die Gesamtzahl der Knoten in beiden Clustern gleich der Zahl der von Ihnen reservierten Knoten ist.

Beispiel 6

Sie haben zwei Cluster in der Region USA West (Oregon). Ein Cluster hat 4 Knoten und das andere Cluster hat 6 Knoten.

In diesem Szenario wird Ihnen für die 10 Knoten in den ausgeführten Clustern der rabattierte Preis berechnet. Für die zusätzlichen 6 von Ihnen reservierten Knoten zahlen Sie ebenfalls den rabattierten Preis, obwohl Sie zurzeit keine Cluster ausführen, in denen sie verwendet werden.

Kaufen eines Angebots reservierter Knoten mit der Amazon-Redshift-Konsole

Auf der Seite Reserved Nodes (Reservierte Knoten) in der Amazon-Redshift-Konsole können Sie Angebote reservierter Knoten kaufen und aktuelle und frühere Reservierungen anzeigen.

Nach dem Kauf einer Lösung werden in der Liste Reserved Nodes (Reserved Nodes) Ihre Reservierungen und die jeweiligen Details angezeigt, wie Knotentyp, Anzahl der Knoten und Status der Reservierung. Weitere Informationen zu den Reservierungsdetails finden Sie unter So funktionieren reservierte Knoten:.

So kaufen Sie einen reservierten Knoten:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann Reserved nodes (Reservierte Knoten) aus, um die Liste der reservierten Knoten anzuzeigen.
3. Wählen Sie Purchase reserved nodes (Reservierte Knoten kaufen) aus, um die Seite anzuzeigen, auf der Sie die Eigenschaften des Knotens auswählen können, den Sie kaufen möchten.
4. Geben Sie die Eigenschaften des Knotens ein und wählen Sie dann Purchase reserved nodes (Reservierte Knoten kaufen) aus.

Verwenden Sie zum Aktualisieren eines reservierten Knotens die AWS CLI.

Sie können nicht alle Knotentypen in reservierte Knoten konvertieren. Es ist auch möglich, dass ein vorhandener reservierter Knoten zur Verlängerung nicht verfügbar ist. Dies könnte daran liegen, dass der Knotentyp eingestellt wurde. Wenden Sie sich an den Kundensupport, um einen eingestellten Knotentyp zu verlängern.

Aktualisierung reservierter Knoten mit dem AWS CLI

Um eine Reservierung für reservierte Knoten zu aktualisieren mit dem AWS CLI

1. Besorgen Sie sich eine Liste ReservedNodeOffering mit IDs für Angebote, die Ihren Anforderungen in Bezug auf Zahlungsart, Laufzeit und Gebühren entsprechen. Das folgende Beispiel veranschaulicht diesen Schritt:

```
aws redshift get-reserved-node-exchange-offerings --reserved-node-id xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxx
{
    "ReservedNodeOfferings": [
        {
            "Duration": 31536000,
            "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
            "UsagePrice": 0.0,
            "NodeType": "dc2.large",
            "RecurringCharges": [
                {
```

```
                    "RecurringChargeFrequency": "Hourly",
                    "RecurringChargeAmount": 0.2
                }
            ],
            "CurrencyCode": "USD",
            "OfferingType": "No Upfront",
            "ReservedNodeOfferingType": "Regular",
            "FixedPrice": 0.0
        }
    ]
}
```

2. Rufen Sie an `accept-reserved-node-exchange` und geben Sie die ID für den reservierten DC1-Knoten an, den Sie austauschen möchten, sowie die ReservedNodeOffering ID, die Sie im vorherigen Schritt erhalten haben.

   Das folgende Beispiel veranschaulicht diesen Schritt:

```
aws redshift accept-reserved-node-exchange --reserved-node-id xxxxxxxx-xxxx-xxxx-
xxxx-xxxxxxxxxxxx --target-reserved-node-offering-id yyyyyyyy-yyyy-yyyy-yyyy-
yyyyyyyyyyyy
{
    "ExchangedReservedNode": {
        "UsagePrice": 0.0,
        "OfferingType": "No Upfront",
        "State": "exchanging",
        "FixedPrice": 0.0,
        "CurrencyCode": "USD",
        "ReservedNodeId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzz",
        "NodeType": "dc2.large",
        "NodeCount": 1,
        "RecurringCharges": [
            {
                "RecurringChargeFrequency": "Hourly",
                "RecurringChargeAmount": 0.2
            }
        ],
        "ReservedNodeOfferingType": "Regular",
        "StartTime": "2018-06-27T18:02:58Z",
        "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
        "Duration": 31536000
    }
```

```
}
```

Sie können bestätigen, dass der Austausch abgeschlossen ist, indem Sie anrufen describe-reserved-nodesund den Wert für `Node type` überprüfen.

Kaufen eines Angebots reservierter Knoten über die AWS CLI und die Amazon-Redshift-API

Zum Erwerb von Reserved Node-Angeboten können Sie die folgenden AWS CLI-Operationen verwenden.

- purchase-reserved-node-offering
- describe-reserved-node-offerings
- describe-orderable-cluster-options

Zum Kaufen von Angeboten reservierter Knoten können Sie die folgenden Amazon-Redshift-API-Vorgänge verwenden.

- PurchaseReservedNodeOffering
- DescribeReservedNodeOfferings
- DescribeOrderableClusterOptions

Sie können nicht alle Knotentypen in reservierte Knoten konvertieren. Es ist auch möglich, dass ein vorhandener reservierter Knoten zur Verlängerung nicht verfügbar ist. Dies könnte daran liegen, dass der Knotentyp eingestellt wurde.

Sicherheit in Amazon Redshift

Die Sicherheit in der Cloud hat für AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud: AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen des AWS-Compliance-Programms getestet und überprüft. Weitere Informationen zu den für Amazon Redshift geltenden Compliance-Programmen finden Sie unter Durch das Compliance-Programm abgedeckte AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Der Zugriff auf Amazon-Redshift-Ressourcen wird auf vier Ebenen gesteuert:

- Clusterverwaltung – Die Fähigkeit, Cluster zu erstellen, zu konfigurieren und zu löschen, wird durch die Berechtigungen gesteuert, die der Benutzer oder das Konto, der bzw. das Ihren AWS-Sicherheitsanmeldeinformationen zugeordnet ist, erhalten hat. Benutzer mit den geeigneten Berechtigungen können die AWS Management Console, AWS Command Line Interface (CLI) oder Amazon-Redshift-Programmierschnittstelle (API) zum Verwalten ihrer Cluster verwenden. Dieser Zugriff wird mit IAM-Richtlinien gesteuert.

> **Important**
>
> Amazon Redshift verfügt über eine Sammlung bewährter Methoden für die Verwaltung von Berechtigungen, Identitäten und einem sicheren Zugriff. Wir empfehlen Ihnen, sich mit diesen vertraut zu machen, wenn Sie mit der Verwendung von Amazon Redshift beginnen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

- Cluster-Konnektivität – Amazon-Redshift-Sicherheitsgruppen geben die AWS-Instances, die zur Verbindung mit einem Amazon-Redshift-Cluster berechtigt sind, im Classless Inter-Domain Routing (CIDR)-Format an. Informationen zum Erstellen von Amazon-Redshift-, Amazon-EC2- und Amazon-VPC-Sicherheitsgruppen und ihrer Zuweisung zu Clustern finden Sie unter Amazon-Redshift-Cluster-Sicherheitsgruppen.
- Datenbankzugriff – Die Möglichkeit zum Zugreifen auf Datenbankobjekte wie Tabellen oder Ansichten wird durch Datenbank-Benutzerkonten in der Amazon-Redshift-Datenbank gesteuert. Benutzer können nur auf Ressourcen in der Datenbank zugreifen, für die ihre Benutzerkonten Zugriffsberechtigungen erhalten haben. Sie erstellen diese Amazon-Redshift-Benutzerkonten und verwalten die Berechtigungen mithilfe der SQL-Anweisungen CREATE USER, CREATE GROUP, GRANT und REVOKE. Weitere Informationen finden Sie unter Verwalten der Datenbanksicherheit im Datenbankentwicklerhandbuch zu Amazon Redshift.
- Temporäre Datenbank-Anmeldeinformationen und Single Sign-On – Zusätzlich zum Erstellen und Verwalten von Datenbankbenutzern mithilfe von SQL-Befehlen wie CREATE USER und ALTER USER können Sie Ihren SQL-Client mit benutzerdefinierten Amazon-Redshift-JDBC- oder -ODBC-Treibern konfigurieren. Diese Treiber verwalten die Erstellung von Datenbankbenutzern und temporären Passwörtern als Teil der Datenbankanmeldung.

  Die Treiber authentifizieren Datenbankbenutzer basierend auf der Authentifizierung durch AWS Identity and Access Management (IAM). Wenn Sie bereits Benutzeridentitäten außerhalb von AWS verwalten, können Sie einen SAML-2.0-konformen Identitätsanbieter für die Verwaltung des Zugriffs auf Amazon-Redshift-Ressourcen verwenden. Sie verwenden eine IAM-Rolle, um den Identitätsanbieter zu konfigurieren, und AWS, um Ihren Verbundbenutzern zu ermöglichen, temporäre Datenbankanmeldeinformationen zu erstellen und sich bei Amazon-Redshift-Datenbanken anzumelden. Weitere Informationen finden Sie unter Verwenden der IAM-Authentifizierung zur Erstellung von Anmeldeinformationen für Datenbankbenutzern.

Diese Dokumentation zeigt, wie Sie bei der Nutzung von Amazon Redshift das Modell der geteilten Verantwortung anwenden können. Die folgenden Themen zeigen, wie Sie Amazon Redshift zur Erreichung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie lernen auch, wie Sie andere AWS-Services verwenden, die Sie bei der Überwachung und Sicherung Ihrer Amazon-Redshift-Ressourcen unterstützen.

Themen

- Datenschutz in Amazon Redshift
- Identity and Access Management in Amazon Redshift

- Verwaltung von Amazon Redshift Redshift-Administratorkennwörtern mit AWS Secrets Manager
- Protokollierung und Überwachung in Amazon Redshift
- Compliance-Validierung für Amazon Redshift
- Ausfallsicherheit in Amazon Redshift
- Infrastruktursicherheit in Amazon Redshift
- Konfigurations- und Schwachstellenanalyse in Amazon Redshift

Datenschutz in Amazon Redshift

Dieses AWSModell der geteilten Verantwortung wird auch auf den Datenschutz in Amazon Redshift angewendet. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon Redshift oder anderen AWS-Services über die Konsole, API, AWS CLI oder AWS-SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung

Dieser Datenschutz bezieht sich auf Daten bei der Übertragung (während sie in Amazon Redshift oder daraus übertragen werden) sowie im Ruhezustand (während sie in Amazon-Redshift-Rechenzentren auf Datenträgern gespeichert sind). Sie können Daten während der Übertragung durch SSL oder eine clientseitige Verschlüsselung sichern. Sie haben folgende Optionen, um Data-at-Rest in Amazon Redshift zu schützen.

- Verwenden serverseitiger Verschlüsselung – Sie fordern an, dass Amazon Redshift Ihre Daten verschlüsselt, bevor sie auf Datenträgern in den Rechenzentren des Services gespeichert werden, und die Daten entschlüsselt, wenn Sie die Objekte herunterladen.
- Verwenden clientseitiger Verschlüsselung – Sie können Daten clientseitig verschlüsseln und die verschlüsselten Daten in Amazon Redshift hochladen. In diesem Fall verwalten Sie den Verschlüsselungsprozess, die Verschlüsselungsschlüssel und die zugehörigen Tools.

Verschlüsselung im Ruhezustand

Serverseitige Verschlüsselung betrifft Datenverschlüsselung im Ruhezustand – das heißt, Amazon Redshift verschlüsselt optional Ihre Daten, wenn sie in die Rechenzentren des Services geschrieben werden, und entschlüsselt sie für Sie, wenn Sie darauf zugreifen. Wenn Sie Ihre Anfrage authentifizieren und Zugriffsberechtigungen besitzen, gibt es in Bezug auf die Art und Weise, wie Sie auf verschlüsselte oder nicht verschlüsselte Daten zugreifen, keinen Unterschied.

Amazon Redshift schützt Data-at-Rest durch Verschlüsselung. Optional können Sie alle auf Datenträgern gespeicherten Daten innerhalb eines Clusters und alle Backups in Amazon S3 mit Advanced Encryption Standard AES-256 schützen.

Verwenden Sie zur Verwaltung der Schlüssel für die Ver- und Entschlüsselung Ihrer Amazon-Redshift-Ressourcen AWS Key Management Service (AWS KMS). AWS KMS kombiniert sichere, hoch verfügbare Hard- und Software, um ein System für die Schlüsselverwaltung bereitzustellen,

das für die Cloud skaliert ist. Mit AWS KMS können Sie Verschlüsselungsschlüssel erstellen und Richtlinien definieren, die steuern, wie diese Schlüssel verwendet werden können. AWS KMS unterstützt AWS CloudTrail, sodass Sie die Schlüsselverwendung überprüfen und sicherstellen können, dass die Schlüssel korrekt verwendet werden. Sie können Ihre AWS KMS-Schlüssel in Kombination mit Amazon Redshift und unterstützten AWS-Services verwenden. Eine Liste der Services, die AWS KMS unterstützen, finden Sie unter Wie AWS-Services AWS KMSverwenden im AWS Key Management Service-Entwicklerhandbuch.

Wenn Sie sich für die Verwaltung des Administratorpassworts Ihres bereitgestellten Clusters oder Serverless-Namespace über AWS Secrets Manager entscheiden, akzeptiert Amazon Redshift auch einen zusätzlichen AWS-KMS-Schlüssel, den AWS Secrets Manager zur Verschlüsselung Ihrer Anmeldeinformationen verwendet. Dieser zusätzliche Schlüssel kann ein automatisch generierter Schlüssel aus AWS Secrets Manager oder ein von Ihnen bereitgestellter benutzerdefinierter Schlüssel sein.

Der Amazon-Redshift-Abfrage-Editor v2 speichert die in den Abfrage-Editor eingegebenen Informationen sicher wie folgt:

- Der Amazon-Ressourcenname (ARN) des KMS-Schlüssels zum Verschlüsseln von Daten des Abfrage-Editors v2.
- Informationen zur Datenbankverbindung.
- Namen und Inhalt von Dateien und Ordnern.

Der Amazon-Redshift-Abfrage-Editor v2 verschlüsselt Informationen mithilfe von Blockverschlüsselung entweder mit Ihrem KMS-Schlüssel oder dem KMS-Schlüssel des Servicekontos. Die Verschlüsselung Ihrer Amazon-Redshift-Redshift-Daten wird durch Ihre Amazon-Redshift-Cluster-Eigenschaften gesteuert.

Themen

- Verschlüsselung von Amazon-Redshift-Datenbanken

Verschlüsselung von Amazon-Redshift-Datenbanken

Sie können in Amazon Redshift die Datenbankverschlüsselung für Ihre Cluster aktivieren, um Data-at-Rest besser zu schützen. Wenn Sie die Verschlüsselung für einen Cluster aktivieren, werden die Datenblöcke und die Metadaten des Systems für den Cluster und Snapshots des Clusters verschlüsselt.

Sie können die Verschlüsselung aktivieren, wenn Sie Ihren Cluster starten, oder Sie können einen unverschlüsselten Cluster so ändern, dass er die Verschlüsselung AWS Key Management Service (AWS KMS) verwendet. Dazu können Sie entweder einen AWS-verwalteten Schlüssel oder einen vom Kunden verwalteten Schlüssel verwenden. Wenn Sie Ihren Cluster bearbeiten, um die AWS KMS -Verschlüsselung zu aktivieren, migriert Amazon Redshift Ihre Daten automatisch in einen neuen, verschlüsselten Cluster. Aus dem verschlüsselten Cluster erstellte Snapshots sind ebenfalls verschlüsselt. Sie können auch einen unverschlüsselten Cluster in einem verschlüsselten Cluster migrieren, indem Sie den Cluster anpassen und die Option Encrypt database (Datenbank verschlüsseln) wählen. Weitere Informationen finden Sie unter Ändern der Verschlüsselung von Clustern.

Die Verschlüsselung in Amazon Redshift ist zwar optional, wir empfehlen jedoch, sie für Cluster mit sensiblen Daten zu aktivieren. Beachten Sie außerdem, dass für Ihre Daten möglicherweise Richtlinien oder Vorschriften gelten, die eine Verschlüsselung obligatorisch machen. Beispiele für Vorschriften, die diesbezüglich Richtlinien zur Verarbeitung von bestimmten Arten von Daten haben, sind beispielsweise PCI DSS (Payment Card Industry Data Security Standard), SOX (Sarbanes-Oxley Act) und HIPAA (Health Insurance Portability and Accountability Act).

Amazon Redshift verwendet eine Schlüsselhierarchie, um die Datenbank zu verschlüsseln. Sie können AWS Key Management Service (AWS KMS) oder ein Hardwaresicherheitsmodul (HSM) verwenden, um die Verschlüsselungsschlüssel der obersten Ebene in dieser Hierarchie zu verwalten. Der Prozess, den Amazon Redshift zur Verschlüsselung verwendet, richtet sich danach, wie Sie Schlüssel verwalten. Amazon Redshift lässt sich automatisch in ein HSM integrieren AWS KMS , aber nicht in dieses. Wenn Sie ein HSM verwenden, müssen Sie Client- und Serverzertifikate verwenden, um eine vertrauenswürdige Verbindung zwischen Amazon Redshift und Ihrem HSM herzustellen.

Verbesserungen des Verschlüsselungsprozesses für höhere Leistung und Verfügbarkeit

Verschlüsselung mit RA3-Knoten

Aktualisierungen des Verschlüsselungsprozesses für RA3-Knoten führten zu erheblichen Verbesserungen. Während des Vorgangs können sowohl Lese- als auch Schreibabfragen ausgeführt werden, wobei die Verschlüsselung weniger Leistungseinbußen verursacht. Außerdem wird die Verschlüsselung viel schneller abgeschlossen. Die aktualisierten Prozessschritte umfassen einen Wiederherstellungsvorgang und die Migration von Cluster-Metadaten zu einem Zielcluster. Die verbesserte Benutzererfahrung gilt beispielsweise für Verschlüsselungstypen wie AWS KMS. Bei Datenvolumen im Petabyte-Bereich wurde die Dauer des Vorgangs von Wochen auf Tage reduziert.

Wenn Sie vor der Verschlüsselung Ihres Clusters weiterhin Datenbank-Workloads ausführen möchten, können Sie die Leistung verbessern und den Prozess beschleunigen, indem Sie Knoten mit elastischer Größenanpassung hinzufügen. Sie können die elastische Größenanpassung nicht verwenden, wenn die Verschlüsselung läuft. Verwenden Sie sie daher vor dem Verschlüsseln. Beachten Sie, dass das Hinzufügen von Knoten in der Regel zu höheren Kosten führt.

Verschlüsselung mit anderen Knotentypen

Wenn Sie einen Cluster mit DC2- oder DS2-Knoten verschlüsseln, können Sie keine Schreibabfragen ausführen, wie dies bei RA3-Knoten der Fall ist. Es können nur Leseabfragen ausgeführt werden.

Nutzungshinweise für die Verschlüsselung mit RA3-Knoten

Die folgenden Erkenntnisse und Ressourcen helfen Ihnen, sich auf die Verschlüsselung vorzubereiten und den Prozess zu überwachen.

- Ausführen von Abfragen nach dem Start der Verschlüsselung – Nach dem Start der Verschlüsselung sind Lese- und Schreibvorgänge innerhalb von etwa fünfzehn Minuten verfügbar. Wie lange es dauert, bis der vollständige Verschlüsselungsprozess abgeschlossen ist, hängt von der Datenmenge im Cluster und den Workload-Ebenen ab.
- Wie lange dauert die Verschlüsselung? – Wie lange die Verschlüsselung Ihrer Daten dauert, hängt von mehreren Faktoren ab: Dazu gehören die Anzahl der laufenden Workloads, die verwendeten Rechenressourcen sowie die Anzahl und die Art der Knoten. Wir empfehlen, die Verschlüsselung zunächst in einer Testumgebung durchzuführen. Als Faustregel gilt: Wenn Sie mit Datenvolumen im Petabyte-Bereich arbeiten, kann es wahrscheinlich 1–3 Tage dauern, bis die Verschlüsselung abgeschlossen ist.
- Woher weiß ich, dass die Verschlüsselung abgeschlossen ist? — Nachdem Sie die Verschlüsselung aktiviert haben, bestätigt der Abschluss des ersten Snapshots, dass die Verschlüsselung abgeschlossen ist.
- Zurücksetzen der Verschlüsselung – Wenn Sie den Verschlüsselungsvorgang rückgängig machen müssen, ist es am besten, die Wiederherstellung anhand des letzten Backups durchzuführen, das vor der Initiierung der Verschlüsselung erstellt wurde. Sie müssen alle neuen Updates (Aktualisierungen/Löschungen/Einfügungen) nach dem letzten Backup erneut anwenden.
- Durchführen einer Tabellenwiederherstellung – Beachten Sie, dass Sie eine Tabelle aus einem unverschlüsselten Cluster nicht in einem verschlüsselten Cluster wiederherstellen können.
- Verschlüsselung eines Clusters mit einem Knoten – Die Verschlüsselung eines Clusters mit einem Knoten ist mit Leistungseinschränkungen verbunden. Dieser Vorgang dauert länger als die Verschlüsselung eines Clusters mit mehreren Knoten.

- Erstellen eines Backups nach der Verschlüsselung – Wenn Sie die Daten in Ihrem Cluster verschlüsseln, wird erst dann ein Backup erstellt, wenn der Cluster vollständig verschlüsselt ist. Der Zeitaufwand dafür kann variieren. Die für das Backup benötigte Zeit kann je nach Clustergröße Stunden bis Tage betragen. Nach Abschluss der Verschlüsselung kann es zu einer Verzögerung kommen, bevor Sie ein Backup erstellen können.

  Beachten Sie, dass Tabellen oder Materialized Views, die mit erstellt wurden, `BACKUP NO` nicht beibehalten werden, da während des Verschlüsselungsvorgangs ein Vorgang ausgeführt wird. backup-and-restore Weitere Informationen finden Sie unter CREATE TABLE oder CREATE MATERIALIZED VIEW.

Themen

- Datenbankverschlüsselung für Amazon Redshift mithilfe von AWS KMS
- Verschlüsselung für Amazon Redshift mit Hardwaresicherheitsmodulen
- Rotation von Verschlüsselungsschlüsseln in Amazon Redshift
- Ändern der Verschlüsselung von Clustern
- Konfigurieren der Datenbankverschlüsselung mit der Konsole
- Konfigurieren der Datenbankverschlüsselung mit der Amazon Redshift API und AWS CLI

Datenbankverschlüsselung für Amazon Redshift mithilfe von AWS KMS

Wenn Sie sich AWS KMS für die Schlüsselverwaltung mit Amazon Redshift entscheiden, gibt es eine vierstufige Hierarchie von Verschlüsselungsschlüsseln. Diese Schlüssel sind (in der Abfolge der Hierarchie) der Root-Schlüssel, ein Clusterschlüssel (CEK, Cluster Encryption Key), ein Datenbankschlüssel (DEK, Database Encryption Key) und Schlüssel zur Datenverschlüsselung.

Wenn Sie Ihren Cluster starten, gibt Amazon Redshift eine Liste der Cluster zurück AWS KMS keys , die Ihr AWS Konto erstellt hat oder zu deren Verwendung Ihr Konto berechtigt ist. AWS KMS Sie wählen einen KMS-Schlüssel zur Verwendung als Root-Schlüssel in der Verschlüsselungshierarchie aus.

Standardmäßig verwendet Amazon Redshift Ihren Standardschlüssel als Root-Schlüssel. Ihr Standardschlüssel ist ein AWS verwalteter Schlüssel, der für Ihr AWS Konto zur Verwendung in Amazon Redshift erstellt wurde. AWS KMS erstellt diesen Schlüssel, wenn Sie zum ersten Mal einen verschlüsselten Cluster in einer AWS Region starten und den Standardschlüssel wählen.

Wenn Sie den Standardschlüssel nicht verwenden möchten, müssen Sie einen vom Kunden verwalteten KMS-Schlüssel separat haben (oder erstellen), AWS KMS bevor Sie Ihren Cluster in Amazon Redshift starten. Vom Kunden verwaltete Schlüssel gewähren Ihnen größere Flexibilität, einschließlich der Möglichkeit, eine Zugriffssteuerung zu erstellen, zu rotieren, zu deaktivieren und zu definieren sowie die Verschlüsselungsschlüssel zu prüfen, um Ihre Daten besser zu schützen. Weitere Informationen zum Erstellen von KMS-Schlüsseln finden Sie unter Erstellen von Schlüsseln im AWS Key Management Service -Entwicklerhandbuch.

Wenn Sie einen AWS KMS Schlüssel von einem anderen AWS Konto verwenden möchten, müssen Sie über die Berechtigung zur Verwendung des Schlüssels verfügen und seinen Amazon-Ressourcennamen (ARN) in Amazon Redshift angeben. Weitere Informationen zum Zugriff auf Schlüssel finden Sie unter Steuern des Zugriffs auf Ihre Schlüssel im AWS Key Management Service Entwicklerhandbuch. AWS KMS

Nachdem Sie einen Root-Schlüssel ausgewählt haben, fordert Amazon Redshift an, einen Datenschlüssel AWS KMS zu generieren und ihn mit dem ausgewählten Root-Schlüssel zu verschlüsseln. Dieser Datenschlüssel wird in Amazon Redshift als CEK verwendet. AWS KMS exportiert den verschlüsselten CEK nach Amazon Redshift. Hier wird er in einem vom Cluster getrennten Netzwerk intern auf einem Datenträger gespeichert, zusammen mit der Genehmigung für den KMS-Schlüssel und dem Verschlüsselungskontext für den CEK. Nur der verschlüsselte CEK wird nach Amazon Redshift exportiert; der KMS-Schlüssel bleibt in AWS KMS. Außerdem übergibt Amazon Redshift den verschlüsselten CEK über einen sicheren Kanal an den Cluster und lädt ihn in den Arbeitsspeicher. Dann ruft Amazon Redshift auf, um das CEK AWS KMS zu entschlüsseln, und lädt das entschlüsselte CEK in den Speicher. Weitere Informationen zu Zuschüssen, Verschlüsselungskontext und anderen verwandten Konzepten finden Sie AWS KMS unter Konzepte im Entwicklerhandbuch.AWS Key Management Service

Anschließend generiert Amazon Redshift nach dem Zufallsprinzip einen Schlüssel zur Verwendung als DEK und lädt ihn im Cluster in den Arbeitsspeicher. Der entschlüsselte CEK wird zum Verschlüsseln des DEK verwendet, der dann über eine gesicherte Verbindung vom Cluster übergeben wird und von Amazon Redshift intern in einem vom Cluster getrennten Netzwerk auf Datenträger gespeichert wird. Wie bei dem CEK werden sowohl die verschlüsselte als auch die entschlüsselte Version des in dem Cluster in den Arbeitsspeicher geladen. Mit dem entschlüsselten DEK werden anschließend die einzelnen Verschlüsselungsschlüssel verschlüsselt, die nach dem Zufallsprinzip für die einzelnen Blöcke in der Datenbank generiert werden.

Wenn der Cluster neu gestartet wird, beginnt Amazon Redshift mit den intern gespeicherten, verschlüsselten Versionen von CEK und DEK, lädt sie erneut in den Speicher und ruft dann auf, um

das CEK erneut mit dem KMS-Schlüssel AWS KMS zu entschlüsseln, sodass es in den Speicher geladen werden kann. Anschließend wird der entschlüsselte CEK verwendet, um den DEK wieder zu entschlüsseln, der entschlüsselte DEK wird in den Arbeitsspeicher geladen und kann dazu verwendet werden, Datenblöcke wie gewünscht zu verschlüsseln und zu entschlüsseln.

Weitere Informationen zum Erstellen von Amazon-Redshift-Clustern, die mit AWS KMS -Schlüsseln verschlüsselt sind, finden Sie unter Erstellen eines Clusters und Verwaltung von Clustern mithilfe der AWS CLI und der Amazon Redshift Redshift-API.

Kopieren von —verschlüsselten Snapshots in eine andere Region AWS KMSAWS

AWS KMS Schlüssel sind spezifisch für eine AWS Region. Wenn Sie das Kopieren von Amazon Redshift-Snapshots in eine andere AWS Region aktivieren und der Quell-Cluster und seine Snapshots mit einem Root-Schlüssel von verschlüsselt sind AWS KMS, müssen Sie eine Genehmigung für Amazon Redshift konfigurieren, um einen Root-Schlüssel in der Zielregion zu verwenden. AWS Dieser Zuschuss ermöglicht es Amazon Redshift, Snapshots in der Zielregion zu verschlüsseln. AWS Weitere Informationen zum regionenübergreifenden Kopieren von Snapshots finden Sie unter Kopieren von Snapshots in eine andere AWS -Region.

> **Note**
>
> Wenn Sie das Kopieren von Snapshots aus einem verschlüsselten Cluster und deren Verwendung AWS KMS für Ihren Root-Schlüssel aktivieren, können Sie Ihren Cluster nicht umbenennen, da der Clustername Teil des Verschlüsselungskontextes ist. Wenn Sie Ihren Cluster umbenennen müssen, können Sie das Kopieren von Snapshots in der AWS Quellregion deaktivieren, den Cluster umbenennen und dann das Kopieren von Snapshots erneut konfigurieren und aktivieren.

Der Prozess zum Konfigurieren der Berechtigung zum Kopieren von Snapshots sieht wie folgt aus.

1. Gehen Sie wie folgt vor, um in der AWS Zielregion eine Genehmigung für Snapshot-Kopien zu erstellen:
   - Wenn Sie noch keinen AWS KMS Schlüssel haben, den Sie verwenden können, erstellen Sie einen. Weitere Informationen zum Erstellen von AWS KMS Schlüsseln finden Sie unter Schlüssel erstellen im AWS Key Management Service Entwicklerhandbuch.
   - Geben Sie einen Namen für die Berechtigung zum Kopien von Snapshots an. Dieser Name muss in dieser AWS Region für Ihr AWS Konto eindeutig sein.

- Geben Sie die AWS KMS Schlüssel-ID an, für die Sie den Zuschuss erstellen. Wenn Sie keine Schlüssel-ID angeben, wird die Berechtigung für Ihren Standardschlüssel übernommen.

2. Aktivieren Sie in der AWS Quellregion das Kopieren von Snapshots und geben Sie den Namen des Snapshot-Kopierzuschusses an, den Sie in der AWS Zielregion erstellt haben.

Dieser vorherige Vorgang ist nur erforderlich, wenn Sie das Kopieren von Snapshots mithilfe der AWS CLI Amazon Redshift Redshift-API oder SDKs aktivieren. Wenn Sie die Konsole verwenden, stellt Amazon Redshift den richtigen Workflow zum Konfigurieren der Berechtigung bereit, wenn Sie das regionenübergreifende Kopieren von Snapshots aktivieren. Weitere Informationen zum Konfigurieren von regionenübergreifenden Snapshot-Kopien für AWS KMS-verschlüsselte Cluster unter Verwendung der Konsole finden Sie unter Konfigurieren Sie die regionsübergreifende Snapshot-Kopie für einen AWS KMS—verschlüsselten Cluster.

Bevor der Snapshot in die AWS Zielregion kopiert wird, entschlüsselt Amazon Redshift den Snapshot mithilfe des Stammschlüssels in der AWS Quellregion und verschlüsselt ihn vorübergehend erneut mit einem zufällig generierten RSA-Schlüssel, den Amazon Redshift intern verwaltet. Amazon Redshift kopiert dann den Snapshot über einen sicheren Kanal in die AWS Zielregion, entschlüsselt den Snapshot mit dem intern verwalteten RSA-Schlüssel und verschlüsselt den Snapshot anschließend erneut mit dem Stammschlüssel in der Zielregion. AWS

Weitere Informationen zur Konfiguration von Snapshot-Kopierberechtigungen für AWS KMS-verschlüsselte Cluster finden Sie unter. Konfigurieren von Amazon Redshift zur Verwendung von AWS KMS-Verschlüsselungsschlüsseln mit der Amazon Redshift API und AWS CLI

Verschlüsselung für Amazon Redshift mit Hardwaresicherheitsmodulen

Wenn Sie es nicht AWS KMS für die Schlüsselverwaltung verwenden, können Sie ein Hardware-Sicherheitsmodul (HSM) für die Schlüsselverwaltung mit Amazon Redshift verwenden.

> **Important**
>
> Die HSM-Verschlüsselung wird für DC2- und RA3-Knotentypen nicht unterstützt.

HSMs sind Geräte zur direkten Steuerung der Erzeugung und Verwaltung von Schlüsseln. Sie bieten eine höhere Sicherheit, da die Schlüsselverwaltung getrennt von den Anwendungs- und Datenbankebenen erfolgt. Amazon Redshift unterstützt AWS CloudHSM Classic für die

Schlüsselverwaltung. Wenn Sie zur Verwaltung Ihrer Verschlüsselungsschlüssel anstelle von HSMs verwenden, ändert sich der Verschlüsselungsprozess AWS KMS.

> **Important**
>
> Amazon Redshift unterstützt nur AWS CloudHSM Classic. Wir unterstützen nicht den neueren AWS CloudHSM -Service.
> AWS CloudHSM Classic ist für Neukunden geschlossen. Weitere Informationen finden Sie unter CloudHSM Classic-Preise. AWS CloudHSM Classic ist nicht in allen AWS Regionen verfügbar. Weitere Informationen zu den verfügbaren AWS Regionen finden Sie AWS in der Regionentabelle.

Wenn Sie Ihren Cluster zur Verwendung eines HSM konfigurieren, sendet Amazon Redshift eine Anforderung an das HSM, einen Schlüssel zur Verwendung als CEK zu generieren und zu speichern. Im Gegensatz AWS KMS dazu exportiert das HSM das CEK jedoch nicht nach Amazon Redshift. Stattdessen generiert Amazon Redshift den DEK nach dem Zufallsprinzip im Cluster und übergibt ihn an das HSM, um vom CEK verschlüsselt zu werden. Das HSM gibt den verschlüsselten DEK an Amazon Redshift zurück. Hier wird er mittels eines nach dem Zufallsprinzip generierten internen Root-Schlüssels weiter verschlüsselt und intern auf einem Datenträger in einem vom Cluster getrennten Netzwerk gespeichert. Außerdem lädt Amazon Redshift die entschlüsselte Version des DEK in den Arbeitsspeicher im Cluster, sodass der DEK zur Verschlüsselung und Entschlüsselung der einzelnen Schlüssel für die Datenblöcke verwendet werden kann.

Wenn der Cluster neu gestartet wird, entschlüsselt Amazon Redshift den intern gespeicherten, doppelt verschlüsselten DEK mit dem internen Root-Schlüssel, um den intern gespeicherten DEK wieder in den CEK-verschlüsselten Zustand zurückzuversetzen. Anschließend wird der CEK-verschlüsselte DEK an das HSM übergeben, wo er entschlüsselt und an Amazon Redshift zurückgegeben wird. Dort kann er wieder in den Arbeitsspeicher geladen und für die einzelnen Datenblockschlüssel verwendet werden.

Konfigurieren einer vertrauenswürdigen Verbindung zwischen Amazon Redshift und einem HSM

Wenn Sie sich bei der Verwaltung Ihres Clusterschlüssels für ein HSM entscheiden, müssen Sie eine vertrauenswürdige Netzwerkverbindung zwischen Amazon Redshift und Ihrem HSM herstellen. Hierzu müssen Client- und Serverzertifikate konfiguriert werden. Über die vertrauenswürdige Verbindung werden bei Verschlüsselungs- und Entschlüsselungsoperationen die Verschlüsselungsschlüssel zwischen dem HSM und Amazon Redshift übergeben.

Amazon Redshift erstellt anhand eines nach dem Zufallsprinzip erzeugten privaten und öffentlichen Schlüsselpaars ein öffentliches Clientzertifikat. Dieses Schlüsselpaar wird verschlüsselt und intern gespeichert. Sie laden das öffentliche Clientzertifikat in Ihr HSM herunter, registrieren es in dem HSM und weisen es der betreffenden HSM-Partition zu.

Sie stellen Amazon Redshift die IP-Adresse des HSM, den Namen der HSM-Partition, das Passwort der HSM-Partition und ein öffentliches HSM-Serverzertifikat bereit, das mit einem internen Root-Schlüssel verschlüsselt wird. Amazon Redshift schließt den Konfigurationsprozess ab und verifiziert, ob eine Verbindung zum HSM hergestellt werden kann. Falls diese Verbindung nicht hergestellt werden kann, wechselt der Cluster in den Zustand INCOMPATIBLE_HSM und wird nicht erstellt. Wenn dies der Fall ist, müssen Sie den unvollständigen Cluster löschen und den Vorgang wiederholen.

> **Important**
>
> Wenn Sie Ihren Cluster so ändern, dass eine andere HSM-Partition verwendet wird, überprüft Amazon Redshift, ob eine Verbindung zur neuen Partition hergestellt werden kann, verifiziert jedoch nicht, ob ein gültiger Verschlüsselungsschlüssel vorhanden ist. Um diese andere Partition verwenden zu können, müssen Sie Ihre Schlüssel in die neue Partition replizieren. Wenn der Cluster neu gestartet wird und Amazon Redshift keinen gültigen Schlüssel findet, schlägt der Neustart fehl. Weitere Informationen finden Sie unter Replizieren von Schlüsseln über mehrere HSMs.

Wenn Amazon Redshift nach der erstmaligen Konfiguration keine Verbindung zu dem HSM herstellen kann, wird ein Ereignis protokolliert. Weitere Informationen zu diesen Ereignissen finden Sie unter Amazon-Redshift-Ereignisbenachrichtigungen.

Rotation von Verschlüsselungsschlüsseln in Amazon Redshift

Sie können in Amazon Redshift Verschlüsselungsschlüssel für verschlüsselte Cluster rotieren. Wenn Sie die Schlüsselrotation starten, rotiert Amazon Redshift den CEK für das angegebene Cluster sowie alle automatisierten oder manuellen Snapshots des Clusters. Außerdem rotiert Amazon Redshift den DEK für das angegebene Cluster, kann jedoch den DEK für die Snapshots nicht rotieren, während sie intern in Amazon Simple Storage Service (Amazon S3) gespeichert und mithilfe des vorhandenen DEK verschlüsselt sind.

Während des Rotationsvorgangs wird der Cluster in den Zustand ROTATING_KEYS versetzt. Nach Abschluss des Vorgangs kehrt der Cluster wieder in den Zustand AVAILABLE zurück. Amazon Redshift verarbeitet die Entschlüsselung und Neuverschlüsselung während der Schlüsselrotation.

> **Note**
>
> Bei Snapshots ohne Quellcluster können die Schlüssel nicht rotiert werden. Wenn Sie einen Cluster löschen möchten, überlegen Sie zuerst, ob für die zugehörigen Snapshots die Schlüssel rotiert werden müssen.

Da der Cluster während des Rotierens der Schlüssel kurzweilig nicht verfügbar ist, sollten Sie die Schlüssel nur so oft rotieren, wie es die Anforderungen an Ihre Daten erforderlich machen, oder wenn Sie den Verdacht haben, dass die Schlüssel möglicherweise kompromittiert wurden. es hat sich als Methode bewährt, zu überprüfen, welche Arten von Daten gespeichert werden, und zu planen, wie häufig die Schlüssel zur Verschlüsselung dieser Daten rotiert werden sollen. Die Häufigkeit von Schlüsselrotationen richtet sich nach Ihren Unternehmensrichtlinien zur Datensicherheit, nach den Industriestandards für sensible Daten sowie nach der erforderlichen Konformität gegenüber geltenden Vorschriften. Stellen Sie sicher, dass in Ihrem Plan ein sorgfältig abgewogen wird zwischen Sicherheitsanforderungen einerseits und Aspekten der Verfügbarkeit Ihres Clusters andererseits.

Weitere Informationen zum Rotieren der Schlüssel finden Sie unter Rotieren der Verschlüsselungsschlüssel mithilfe der Amazon-Redshift-Konsole und Rotieren von Verschlüsselungsschlüsseln mithilfe der Amazon Redshift API und AWS CLI.

Ändern der Verschlüsselung von Clustern

Sie können einen unverschlüsselten Cluster so ändern, dass er die Verschlüsselung AWS Key Management Service (AWS KMS) verwendet, indem Sie entweder einen AWS-verwalteten Schlüssel oder einen vom Kunden verwalteten Schlüssel verwenden. Wenn Sie Ihren Cluster ändern, um die AWS KMS Verschlüsselung zu aktivieren, migriert Amazon Redshift Ihre Daten automatisch auf einen neuen verschlüsselten Cluster. Sie können auch einen unverschlüsselten Cluster in einem verschlüsselten Cluster migrieren, indem Sie den Cluster anpassen.

Während des Migrationsprozesses ist der Cluster im schreibgeschützten Modus verfügbar, und der Clusterstatus wird als Größenanpassung angezeigt.

Wenn Ihr Cluster so konfiguriert ist, dass das regionsübergreifende Kopieren von AWS Snapshots aktiviert wird, müssen Sie ihn deaktivieren, bevor Sie die Verschlüsselung ändern. Weitere

Informationen erhalten Sie unter Kopieren von Snapshots in eine andere AWS -Region und Konfigurieren Sie die regionsübergreifende Snapshot-Kopie für einen AWS KMS—verschlüsselten Cluster. Wenn Sie eine Verschlüsselung per Hardwaresicherheitsmodul (HSM) aktivieren möchten, können Sie dies nicht erreichen, indem Sie das Cluster ändern. Sie müssen stattdessen ein neues, HSM-verschlüsseltes Cluster erstellen und die Daten in das neue Cluster migrieren. Weitere Informationen finden Sie unter Migrieren zu einem HSM-verschlüsselten Cluster.

So ändern Sie die Datenbankverschlüsselung in einem Cluster:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster aus, für den Sie die Verschlüsselung ändern möchten.
3. Wählen Sie Properties (Eigenschaften).
4. Wählen Sie im Bereich Database configurations (Datenbankkonfigurationen) Edit (Bearbeiten) und anschließend Edit encryption (Verschlüsselung bearbeiten) aus.
5. Wählen Sie eine der Verschlüsselungsoptionen und dann Save changes (Änderungen speichern) aus.

So ändern Sie die Verschlüsselung von Clustern mithilfe der CLI

Um den zu verwendenden unverschlüsselten Cluster zu ändern AWS KMS, führen Sie den `modify-cluster` CLI-Befehl aus und geben Sie Folgendes an`--encrypted`, wie im Folgenden gezeigt. Standardmäßig wird Ihr Standard-KMS-Schlüssel verwendet. Um einen vom Kunden verwalteten Schlüssel anzugeben, geben Sie auch die Option `--kms-key-id` an.

```
aws redshift modify-cluster --cluster-identifier <value> --encrypted --kms-key-id
 <value>
```

Führen Sie zum Entfernen der Verschlüsselung von einem Cluster den folgenden CLI-Befehl aus.

```
aws redshift modify-cluster --cluster-identifier <value> --no-encrypted
```

Migrieren zu einem HSM-verschlüsselten Cluster

Um von einem unverschlüsselten Cluster zu einem mit einem Hardwaresicherheitsmodul (HSM) verschlüsselten Cluster zu migrieren, müssen Sie ein neues verschlüsseltes Cluster erstellen und

anschließend Ihre Daten in das neue Cluster migrieren. Sie können zu keinen HSM-verschlüsselten Cluster migrieren, indem Sie den Cluster anpassen.

Um von einem unverschlüsselten Cluster zu einem HSM-verschlüsselten Cluster zu migrieren, müssen Sie zuerst Ihre Daten aus dem vorhandenen Quellcluster entladen. Anschließend laden Sie die Daten in einen neuen Ziel-Cluster mit der gewünschten Verschlüsselungseinstellung. Weitere Informationen zum Starten eines verschlüsselten Clusters finden Sie unter Verschlüsselung von Amazon-Redshift-Datenbanken.

Während des Migrationsprozesses steht Ihr Quell-Cluster bis zum letzten Schritt für schreibgeschützte Abfragen zur Verfügung. Im letzten Schritt werden der Ziel- und der Quell-Cluster umbenannt. Damit werden die Endpunkte vertauscht, sodass Datenverkehr an den neuen Ziel-Cluster weitergeleitet wird. Der Ziel-Cluster steht erst zur Verfügung, wenn Sie nach der Umbenennung einen Neustart durchgeführt haben. Unterbrechen Sie das Laden von Daten und andere Schreiboperationen für den Quell-Cluster, während Daten übertragen werden.

Vorbereitung der Migration

1. Identifizieren Sie alle abhängigen Systeme, die mit Amazon Redshift interagieren, z. B. Business Intelligence (BI)-Tools und ETL-Systeme (Extract, Transform, Load).
2. Identifizieren Sie Prüfabfragen, um die Migration zu testen.

   Beispielsweise können Sie die folgende Abfrage verwenden, um die Anzahl der benutzerdefinieren Tabellen zu ermitteln.

   ```
   select count(*)
   from pg_table_def
   where schemaname != 'pg_catalog';
   ```

   Die folgende Abfrage gibt eine Liste aller benutzerdefinierten Tabellen und die Anzahl der Zeilen für jede Tabelle zurück.

   ```
   select "table", tbl_rows
   from svv_table_info;
   ```

3. Wählen Sie einen sinnvollen Zeitpunkt für Ihre Migration aus. Um einen Zeitpunkt zu finden, zu dem der Cluster möglichst wenig genutzt wird, überwachen Sie Cluster-Metriken, wie beispielsweise die CPU-Nutzung oder die Anzahl der Datenbankverbindungen. Weitere Informationen finden Sie unter Anzeigen von Cluster-Leistungsdaten.

4. Verwerfen Sie nicht genutzte Tabellen.

   Um eine Liste der Tabellen zu erstellen, die angibt, wie oft jede Tabelle abgefragt wurde, führen Sie die folgende Anfrage aus.

```
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. Starte Sie einen neuen, verschlüsselten Cluster.

   Verwenden Sie dieselbe Port-Nummer für den Ziel-Cluster wie für den Quell-Cluster. Weitere Informationen zum Starten eines verschlüsselten Clusters finden Sie unter Verschlüsselung von Amazon-Redshift-Datenbanken.

6. Richten Sie den Prozess zum Entladen und Laden ein.

   Das Dienstprogramm Amazon Redshift Unload/Copy unterstützt Sie bei der Migration von Daten zwischen Clustern. Das Dienstprogramm exportiert Daten aus dem Quell-Cluster an einen Speicherort auf Amazon S3. Die Daten sind verschlüsselt mit AWS KMS. Anschließend importiert das Dienstprogramm die Daten automatisch in das Ziel. Optional können Sie das Dienstprogramm verwenden, um Amazon S3 zu bereinigen, nachdem die Migration abgeschlossen ist.

7. Führen Sie einen Test aus, um Ihren Prozess zu überprüfen und zu schätzen, wie lange Schreiboperationen ausgesetzt werden müssen.

   Während der Entlade- und Ladeoperationen bewahren Sie die Datenkonsistenz, indem Sie das Laden von Daten und andere Schreiboperationen aussetzen. Führen Sie unter Verwendung

einer Ihrer größten Tabellen den Entlade- und Ladeprozess aus, um die Zeit abschätzen zu können.

8. Erstellen Sie Datenbankenobjekte, wie Schemas, Tabellen und Ansichten. Um Ihnen bei der Generierung der erforderlichen DDL-Anweisungen (Data Definition Language) zu helfen, können Sie die Skripts AdminViewsim AWS GitHub Repository verwenden.

So migrieren Sie Ihren Cluster

1. Halten Sie alle ETL-Prozesse auf dem Quellcluster an.

   Um sicherzustellen, dass derzeit keine Schreibvorgänge ausgeführt werden, überwachen Sie die Schreib-IOPS mithilfe der Amazon-Redshift-Managementkonsole. Weitere Informationen finden Sie unter Anzeigen von Cluster-Leistungsdaten.
2. Führen sie die Prüfabfragen aus, die Sie zuvor identifiziert haben, um Informationen über den unverschlüsselten Quellcluster vor der Migration zu erfassen.
3. (Optional) Erstellen Sie eine WLM-Warteschlange (Workload Management), um im Quell- und im Zielcluster die maximal verfügbaren Ressourcen zu nutzen. Erstellen Sie beispielsweise eine Warteschlange namens `data_migrate` und konfigurieren Sie diese mit einem Speicher von 95 Prozent und einer Nebenläufigkeit von 4. Weitere Informationen finden Sie unter Weiterleiten von Abfragen zu Warteschlangen auf der Grundlage von Benutzergruppen und Abfragegruppen im Datenbankentwicklerhandbuch zu Amazon Redshift.
4. Führen Sie mithilfe der `data_migrate` Warteschlange den UnloadCopyUtility aus.

   Überwachen Sie den UNLOAD- und COPY-Vorgang mit der Amazon-Redshift-Konsole.
5. Führen Sie die Prüfabfragen erneut aus und stellen Sie sicher, dass die Ergebnisse mit den Ergebnissen des Quellclusters übereinstimmen.
6. Benennen Sie Ihre Quell- und Zielcluster um, um die Endpunkte zu vertauschen. Um Störungen zu vermeiden, führen Sie diese Operation außerhalb der Geschäftszeiten aus.
7. Stellen Sie sicher, dass Sie mit allen Ihren SQL-Clients eine Verbindung zum Zielcluster herstellen können, z. B. für ETL und Berichtswerkzeuge.
8. Schließen Sie den unverschlüsselten Quellcluster.

Konfigurieren der Datenbankverschlüsselung mit der Konsole

Sie können die Amazon-Redshift-Konsole verwenden, um Amazon Redshift für die Verwendung eines HSM zu konfigurieren und Verschlüsselungsschlüssel zu rotieren. Hinweise zum Erstellen von

Clustern mithilfe von AWS KMS Verschlüsselungsschlüsseln finden Sie unter Erstellen eines Clusters undVerwaltung von Clustern mithilfe der AWS CLI und der Amazon Redshift Redshift-API.

So ändern Sie die Datenbankverschlüsselung in einem Cluster:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster aus, für den Sie Snapshots verschieben möchten.
3. Wählen Sie für Actions (Aktionen) Modify (Ändern) aus, um die Konfigurationsseite anzuzeigen.
4. Wählen Sie im Abschnitt Database configuration (Datenbankkonfiguration eine Einstellung für Encryption (Verschlüsselung und dann Modify cluster (Cluster ändern) aus.

Rotieren der Verschlüsselungsschlüssel mithilfe der Amazon-Redshift-Konsole

Sie können das folgende Verfahren verwenden, um über die Amazon-Redshift-Konsole Verschlüsselungsschlüssel zu rotieren.

So rotieren Sie die Verschlüsselungscodes für einen Cluster:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster aus, der die Verschlüsselungsschlüssel aktualisieren soll.
3. Wählen Sie für Actions (Aktionen) Rotate encryption (Verschlüsselung rotieren) aus, um die Seite Rotate encryption keys (Verschlüsselungsschlüssel rotieren) anzuzeigen.
4. Wählen Sie auf der Seite Rotate encryption keys (Schlüssel rotieren) die Option Rotate encryption keys (Schlüssel rotieren) aus.

Konfigurieren der Datenbankverschlüsselung mit der Amazon Redshift API und AWS CLI

Verwenden Sie die Amazon Redshift API und AWS Command Line Interface (AWS CLI), um Optionen für Verschlüsselungsschlüssel für Amazon-Redshift-Datenbanken zu konfigurieren. Weitere Informationen zum Thema Datenbankverschlüsselung finden Sie unter Verschlüsselung von Amazon-Redshift-Datenbanken.

Konfigurieren von Amazon Redshift zur Verwendung von AWS KMS-Verschlüsselungsschlüsseln mit der Amazon Redshift API und AWS CLI

Sie können die folgenden Amazon Redshift API-Aktionen verwenden, um Amazon Redshift zur Verwendung von AWS KMS-Verschlüsselungsschlüsseln zu konfigurieren.

- CreateCluster
- CreateSnapshotCopyGrant
- DescribeSnapshotCopyGrants
- DeleteSnapshotCopyGrant
- DisableSnapshotCopy
- EnableSnapshotCopy

Sie können die folgenden Amazon-Redshift-CLI-Vorgänge verwenden, um Amazon Redshift zur Verwendung von AWS KMS-Verschlüsselungsschlüsseln zu konfigurieren.

- create-cluster
- create-snapshot-copy-grant
- describe-snapshot-copy-grants
- delete-snapshot-copy-grant
- disable-snapshot-copy
- enable-snapshot-copy

Konfigurieren von Amazon Redshift zur Verwendung eines HSM mit der Amazon Redshift API und AWS CLI

Sie können zur Verwaltung von Hardwaresicherheitsmodulen die folgenden Amazon Redshift API-Aktionen verwenden.

- CreateHsmClientCertificate
- CreateHsmConfiguration
- DeleteHsmClientCertificate
- DeleteHsmConfiguration
- DescribeHsmClientCertificates

- DescribeHsmConfigurations

Sie können zur Verwaltung von Hardwaresicherheitsmodulen die folgenden AWS CLI-Operationen verwenden.

- create-hsm-client-certificate
- create-hsm-configuration
- delete-hsm-client-certificate
- delete-hsm-configuration
- describe-hsm-client-certificates
- describe-hsm-configurations

Rotieren von Verschlüsselungsschlüsseln mithilfe der Amazon Redshift API und AWS CLI

Sie können zum Rotieren von Verschlüsselungsschlüsseln die folgenden Amazon Redshift API-Aktionen verwenden.

- RotateEncryptionKey

Sie können zum Rotieren der Verschlüsselungsschlüssel die folgenden AWS CLI-Operationen verwenden.

- rotate-encryption-key

Verschlüsselung während der Übertragung

Sie können Ihre Umgebung so konfigurieren, dass die Vertraulichkeit und Integrität von Daten während der Übertragung geschützt sind.

Verschlüsselung von Daten während der Übertragung zwischen einem Amazon-Redshift-Cluster und SQL-Clients über JDBC/ODBC:

- Sie können Verbindungen von SQL-Client-Tools zu Amazon-Redshift-Clustern über Java Database Connectivity (JDBC)- und Open Database Connectivity (ODBC)-Verbindungen herstellen.
- Amazon Redshift unterstützt Secure Sockets Layer (SSL)-Verbindungen, um Daten und Serverzertifikate zu verschlüsseln, um das Zertifikat des Servers zu validieren, mit dem der

Client die Verbindung herstellt. Der Client stellt die Verbindung zum Führungsknoten eines Amazon-Redshift-Clusters her. Weitere Informationen finden Sie unter Konfigurieren von Sicherheitsoptionen für Verbindungen.

- Um SSL-Verbindungen zu unterstützen, erstellt und installiert Amazon Redshift auf jedem Cluster von AWS Certificate Manager (ACM) ausgegebene Zertifikate. Weitere Informationen finden Sie unter Umstellung auf ACM-Zertifikate für SSL-Verbindungen.
- Damit Ihre Daten während der Übertragung innerhalb der AWS Cloud geschützt sind, verwendet Amazon Redshift zur Kommunikation mit Amazon S3 oder Amazon DynamoDB bei COPY-, UNLOAD-, Backup- und Wiederherstellungsoperationen eine hardwarebeschleunigte SSL-Verbindung.

Verschlüsselung von Daten während der Übertragung zwischen einem Amazon-Redshift-Cluster und Amazon S3 oder DynamoDB:

- Amazon Redshift verwendet zur Kommunikation mit Amazon S3 oder DynamoDB für COPY-, UNLOAD-, Backup- und Wiederherstellungsvorgänge hardwarebeschleunigtes SSL.
- Redshift Spectrum unterstützt die serverseitige Verschlüsselung (SSE) von Amazon S3 mithilfe des von AWS Key Management Service (KMS) verwalteten Standardschlüssels Ihres Kontos.
- Verschlüsseln Sie Amazon-Redshift-Lasten mit Amazon S3 und AWS KMS. Weitere Informationen finden Sie unter Verschlüsseln von Amazon-Redshift-Lasten mit Amazon S3 und AWS KMS.

Verschlüsseln und Signieren von Daten während der Übertragung zwischen AWS CLI, SDK oder API-Clients und Amazon-Redshift-Endpunkten:

- Amazon Redshift stellt HTTPS-Endpunkte zum Verschlüsseln von Daten während der Übertragung bereit.
- Um die Integrität von API-Anforderungen an Amazon Redshift zu schützen, müssen API-Aufrufe vom Aufrufer signiert werden. Die Aufrufe werden von einem X.509-Zertifikat oder vom geheimen AWS-Zugriffsschlüssel des Kunden gemäß dem Signaturprozess von Signature Version 4 (Sigv4) signiert. Weitere Informationen finden Sie unter Signaturprozess mit Signaturversion 4 im Allgemeine AWS-Referenz.
- Verwenden Sie die AWS CLI oder eines der AWS-SDKs, um Anforderungen an AWS zu senden. Diese Tools signieren automatisch die Anforderungen für Sie mit dem Zugriffsschlüssel, den Sie bei der Konfiguration der Tools angegeben haben.

Verschlüsselung von Daten während der Übertragung zwischen Amazon-Redshift-Clustern und dem Amazon-Redshift-Abfrage-Editor v2:

- Daten werden zwischen dem Abfrage-Editor v2 und Amazon-Redshift-Clustern über einen TLS-verschlüsselten Kanal übertragen.

Schlüsselverwaltung

Sie können Ihre Umgebung so konfigurieren, dass Daten mit Schlüsseln geschützt werden.

- Amazon Redshift integriert sich zur Schlüsselverwaltung automatisch in AWS Key Management Service (AWS KMS). AWS KMS nutzt Envelope-Verschlüsselung. Weitere Informationen finden Sie unter Envelope-Verschlüsselung.
- Wenn Verschlüsselungsschlüssel in AWS KMS verwaltet werden, verwendet Amazon Redshift zur Verschlüsselung eine schlüsselbasierte Architektur mit vier Ebenen. Diese Architektur besteht aus nach dem Zufallsprinzip generierten AES-256-Datenverschlüsselungsschlüsseln, einem Datenbankschlüssel, einem Clusterschlüssel und einem Root-Schlüssel. Weitere Informationen dazu finden Sie unter Verwendung von AWS KMS durch Amazon Redshift.
- Sie können Ihren eigenen vom Kunden verwalteten Schlüssel in AWS KMS erstellen. Weitere Informationen finden Sie unter Erstellen von Schlüsseln.
- Sie können außerdem Ihr eigenes Schlüsselmaterial für neue AWS KMS keys importieren. Weitere Informationen finden Sie unter Importieren von Schlüsselmaterial in AWS Key Management Service (AWS KMS).
- Amazon Redshift unterstützt die Verwaltung von Verschlüsselungsschlüsseln in externen Hardwaresicherheitsmodulen (HSMs). Das HSM kann ein lokales HSM oder sein AWS CloudHSM. Wenn Sie ein HSM verwenden, müssen Sie Client- und Serverzertifikate verwenden, um eine vertrauenswürdige Verbindung zwischen Amazon Redshift und Ihrem HSM herzustellen. Amazon Redshift unterstützt zur Schlüsselverwaltung nur AWS CloudHSM Classic. Weitere Informationen finden Sie unter Verschlüsselung für Amazon Redshift mit Hardwaresicherheitsmodulen. Weitere Informationen zu AWS CloudHSM finden Sie unter Was ist AWS CloudHSM?.
- Sie können Verschlüsselungsschlüssel für verschlüsselte Cluster rotieren. Weitere Informationen finden Sie unter Rotation von Verschlüsselungsschlüsseln in Amazon Redshift.

Datenaufgliederung in Token

Aufgliederung in Token ist der Vorgang der Ersetzung tatsächlicher Werte durch nicht transparente Werte zu Datensicherheitszwecken. Sicherheitssensible Anwendungen verwenden eine Aufgliederung in Token, um sensible Daten wie persönlich identifizierbare Informationen (PII) oder geschützte Gesundheitsinformationen (PHI) durch Token zu ersetzen, um Sicherheitsrisiken zu mindern. Die Aufhebung der Aufgliederung in Token ersetzt Token für autorisierte Benutzer mit entsprechenden Sicherheitsrichtlinien wieder durch tatsächliche Werte.

Zur Integration mit Drittanbieterservices zur Aufgliederung in Token können Sie benutzerdefinierte Funktionen (User-Defined Functions, UDFs) von Amazon Redshift verwenden, die Sie mit erstellen AWS Lambda. Weitere Informationen finden Sie unter Benutzerdefinierte Lambda-Funktionen im Datenbankentwicklerhandbuch zu Amazon Redshift. Ein Beispiel finden Sie unter Protegrity.

Amazon Redshift sendet Anforderungen zur Aufgliederung in Token an einen Tokenisierungsserver, auf den über eine REST API oder einen vordefinierten Endpunkt zugegriffen wird. Zwei oder mehr ergänzende Lambda-Funktionen verarbeiten die Anforderungen zur Aufgliederung in Token und zur Aufhebung der Aufgliederung in Token. Für diese Verarbeitung können Sie Lambda Funktionen verwenden, die von einem Drittanbieter für Aufgliederung in Token bereitgestellt werden. Sie können auch Lambda Funktionen verwenden, die Sie als Lambda-UDFs in Amazon Redshift registrieren.

Angenommen, eine Abfrage wird gesendet, die eine UDF zur Aufgliederung in Token oder zur Aufhebung der Aufgliederung in Token für eine Spalte aufruft. Der Amazon-Redshift-Cluster spoolt die entsprechenden Argumentzeilen und sendet diese Zeilen parallel in Batches an die Lambda-Funktion. Die Daten zwischen den Amazon-Redshift-Rechenknoten und Lambda werden in einer separaten, isolierten Netzwerkverbindung übertragen, auf die Clients nicht zugreifen können.
Die Lambda-Funktion übergibt die Daten an den Endpunkt des Tokenisierungsservers. Der Tokenisierungsserver gliedert die Daten nach Bedarf auf bzw. hebt ihre Aufgliederung auf und gibt sie zurück. Die Lambda-Funktionen übermitteln dann die Ergebnisse zur weiteren Verarbeitung an den Amazon-Redshift-Cluster, falls erforderlich, und geben dann die Abfrageergebnisse zurück.

Richtlinie für den Datenverkehr zwischen Netzwerken

So leiten Sie Datenverkehr zwischen Amazon Redshift und Clients und Anwendungen in einem Unternehmensnetzwerk weiter:

- Richten Sie eine private Verbindung zwischen Ihrer Virtual Private Cloud (VPC) und Ihrem Unternehmensnetzwerk ein. Richten Sie entweder eine IPsec-VPN-Verbindung über das Internet oder eine private physische Verbindung per AWS Direct Connect-Verbindung ein. Mit AWS

Direct Connect können Sie eine private, virtuelle Schnittstelle von Ihrem lokalen Netzwerk direkt zur Amazon VPC einrichten, sodass Sie eine private Netzwerkverbindung mit hoher Bandbreite zwischen Ihrem Netzwerk und Ihrer VPC erhalten. Mit mehreren virtuellen Schnittstellen können Sie sogar eine private Konnektivität mit mehreren VPCs aufbauen und trotzdem die Netzwerkisolierung aufrechterhalten. Weitere Informationen finden Sie unter Was ist AWS Site-to-Site VPN? und Was ist AWS Direct Connect?

So leiten Sie Datenverkehr zwischen einem Amazon-Redshift-Cluster in einer VPC und Amazon-S3-Buckets in derselben AWS-Region weiter:

- Richten Sie einen privaten Amazon-S3-VPC-Endpunkt ein, um privat auf Amazon-S3-Daten von einem ETL-Lade- oder -Entladevorgang zuzugreifen. Weitere Informationen finden Sie unter Endpunkte für Amazon S3.
- Aktivieren Sie „Enhanced VPC routing“ (Erweitertes VPC-Routing) für einen Amazon-Redshift-Cluster und geben Sie einen Amazon-S3-VPC-Zielendpunkt an. Von COPY-, UNLOAD- oder CREATE LIBRARY-Befehlen in Amazon Redshift generierter Datenverkehr wird dann über den privaten Endpunkt geleitet. Weitere Informationen finden Sie unter Enhanced VPC routing (Erweitertes VPC-Routing.

Identity and Access Management in Amazon Redshift

Für den Zugriff auf Amazon Redshift sind Anmeldeinformationen erforderlich, mit denen Sie Ihre Anfragen authentifizieren AWS können. Diese Anmeldeinformationen müssen über Berechtigungen für den Zugriff auf AWS Ressourcen wie einen Amazon Redshift Redshift-Cluster verfügen. In den folgenden Abschnitten erfahren Sie, wie Sie Ihre Ressourcen mithilfe von AWS Identity and Access Management (IAM) und Amazon Redshift sichern können, indem Sie den Zugriff auf sie kontrollieren:

- Authentifizierung mit Identitäten
- Zugriffskontrolle

> **Important**
>
> Dieses Thema enthält eine Sammlung bewährter Methoden für die Verwaltung von Berechtigungen, Identitäten und sicherem Zugriff. Wir empfehlen Ihnen, sich mit den bewährten Methoden für die Verwendung von IAM mit Amazon Redshift vertraut zu machen. Hierzu gehört auch die Verwendung von IAM-Rollen zur Anwendung von Berechtigungen.

Wenn Sie die Informationen in diesen Abschnitten gut verstehen, sind Sie besser in der Lage, ein sichereres Amazon Redshift Data Warehouse zu verwalten.

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-

Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb von Ihnen AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff: Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen: Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

  - Servicerolle: Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon EC2 ausgeführte Anwendungen — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Zugriffskontrolle

Auch wenn Sie über gültige Anmeldeinformationen zur Authentifizierung Ihrer Anforderungen verfügen, können Sie nur dann Amazon-Redshift-Ressourcen erstellen oder aufrufen, wenn Sie die entsprechenden Berechtigungen haben. Sie müssen beispielsweise über eine Berechtigung zum Erstellen eines Amazon-Redshift-Clusters, zum Erstellen eines Snapshots, zum Hinzufügen eines Ereignisabonnements usw. verfügen.

In den folgenden Abschnitten wird die Verwaltung von Berechtigungen für Amazon Redshift beschrieben. Wir empfehlen Ihnen, zunächst die Übersicht zu lesen.

- Übersicht zur Verwaltung der Zugriffsberechtigungen für Amazon-Redshift-Ressourcen
- Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon Redshift

Übersicht zur Verwaltung der Zugriffsberechtigungen für Amazon-Redshift-Ressourcen

Jede AWS Ressource gehört einem AWS Konto, und die Berechtigungen zum Erstellen oder Zugreifen auf die Ressourcen werden durch Berechtigungsrichtlinien geregelt. Ein Kontoadministrator kann IAM-Identitäten (d. h. Benutzern, Gruppen und Rollen) Berechtigungsrichtlinien zuordnen, und einige Dienste (z. B. AWS Lambda) unterstützen auch das Anhängen von Berechtigungsrichtlinien an Ressourcen.

> **Note**
>
> Ein Kontoadministrator (oder Administratorbenutzer) ist ein Benutzer mit Administratorrechten. Weitere Informationen finden Sie unter Bewährte Methoden für IAM im IAM-Benutzerhandbuch.

Beim Erteilen von Berechtigungen entscheiden Sie, wer die Berechtigungen erhält, für welche Ressourcen die Berechtigungen gelten und welche Aktionen an diesen Ressourcen gestattet werden sollen.

Amazon-Redshift-Ressourcen und -Operationen

Amazon Redshift stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Benutzung in IAM-Berechtigungsrichtlinien bereit.

Zugriffsberechtigungen von Amazon Redshift, Amazon Redshift Serverless, der Amazon-Redshift-Daten-API und Amazon Redshift Query Editor v2

Beim Einrichten von Zugriffskontrolle schreiben Sie Berechtigungsrichtlinien, die Sie einer IAM-Identität zuweisen können (identitätsbasierte Richtlinien). Weitere Informationen finden Sie in den folgenden Themen in der Service-Authorization-Referenz:

- Für Amazon Redshift siehe Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Redshift, die das Präfix `redshift:` benutzen.
- Für Amazon Redshift Serverless siehe Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Redshift Serverless, die das Präfix `redshift-serverless:` benutzen.
- Für die Amazon-Redshift-Daten-API siehe Aktionen, Ressourcen und Bedingungsschlüssel für die Amazon-Redshift-Daten-API, die das Präfix `redshift-data:` benutzen.

- Informationen zum Amazon Redshift-Abfrage-Editor v2 finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS SQL Workbench (Amazon Redshift Query Editor v2), die das Präfix verwenden. `sqlworkbench:`

  Der Abfrage-Editor v2 enthält „nur mit Berechtigung“-Aktionen, die nicht direkt einer API-Operation entsprechen. Diese Aktionen sind in der Service-Authorization-Referenz mit „`[permission only]`“ angegeben.

Die Service-Authorization-Referenz enthält Informationen darüber, welche API-Operationen in einer IAM-Richtlinie verwendet werden können. Es enthält auch die AWS Ressource, für die Sie die Berechtigungen erteilen können, sowie Bedingungsschlüssel, die Sie für eine detaillierte Zugriffskontrolle einbeziehen können. Weitere Informationen über Bedingungen finden Sie unter Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle.

Sie geben die Aktionen im Feld `Action` der Richtlinie, den Ressourcenwert im Feld `Resource` der Richtlinie und die Bedingungen im Feld `Condition` der Richtlinie an. Um eine Aktion für Amazon Redshift anzugeben, verwenden Sie das Präfix `redshift:` gefolgt vom Namen der API-Operation (z. B. `redshift:CreateCluster`).

Grundlegendes zum Eigentum an Ressourcen

Ein Ressourcenbesitzer ist das AWS Konto, das eine Ressource erstellt hat. Das heißt, der Ressourcenbesitzer ist das AWS Konto der Prinzipalentität (das Root-Konto, ein IAM-Benutzer oder eine IAM-Rolle), das die Anforderung authentifiziert, mit der die Ressource erstellt wird. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn Sie die Root-Kontoanmeldeinformationen Ihres AWS Kontos verwenden, um einen DB-Cluster zu erstellen, ist Ihr AWS Konto der Eigentümer der Amazon Redshift Redshift-Ressource.
- Wenn Sie in Ihrem AWS Konto eine IAM-Rolle mit Berechtigungen zum Erstellen von Amazon Redshift Redshift-Ressourcen erstellen, kann jeder, der diese Rolle übernehmen kann, Amazon Redshift Redshift-Ressourcen erstellen. Ihr AWS -Konto, zu dem die Rolle gehört, ist der Inhaber der Amazon-Redshift-Ressourcen.
- Wenn Sie in Ihrem AWS Konto einen IAM-Benutzer erstellen und diesem Benutzer Berechtigungen zum Erstellen von Amazon Redshift Redshift-Ressourcen gewähren, kann der Benutzer Amazon Redshift Redshift-Ressourcen erstellen. Ihr AWS Konto, zu dem der Benutzer gehört, besitzt jedoch die Amazon Redshift Redshift-Ressourcen. In den meisten Fällen wird diese Methode nicht empfohlen. Wir empfehlen, eine IAM-Rolle zu erstellen, der Rolle Berechtigungen anzufügen und die Rolle dann einem Benutzer zuzuweisen.

Verwalten des Zugriffs auf Ressourcen

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf was hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

> **Note**
>
> Dieser Abschnitt behandelt die Verwendung von IAM im Zusammenhang mit Amazon Redshift. Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie unter Was ist IAM? im IAM-Benutzerhandbuch. Informationen über die Syntax und Beschreibungen von IAM-Richtlinien finden Sie in der AWS -IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Richtlinien, die einer IAM-Identität zugeordnet sind, werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet, während Richtlinien, die einer Ressource zugeordnet sind, ressourcenbasierte Richtlinien genannt werden. Amazon Redshift unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Identitätsbasierte Richtlinien (IAM-Richtlinien)

Sie können Berechtigungen zuweisen, indem Sie Richtlinien an eine IAM-Rolle anfügen und diese Rolle dann einem Benutzer oder einer Gruppe zuweisen. Im Folgenden finden Sie eine Beispielrichtlinie, die Berechtigungen zum Erstellen, Löschen, Ändern und Neustarten von Amazon Redshift Redshift-Clustern für Ihr AWS Konto enthält.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowManageClusters",
      "Effect":"Allow",
      "Action": [
        "redshift:CreateCluster",
        "redshift:DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource":"*"
    }
  ]
```

```
}
```

Weitere Informationen zur Verwendung identitätsbasierter Richtlinien mit Amazon Redshift finden Sie unter Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon Redshift. Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie unter Identitäten (Benutzer, Gruppen und Rollen) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Andere Services, z. B. Amazon S3, unterstützen auch ressourcenbasierte Berechtigungsrichtlinien. Beispielsweise können Sie einem S3 Bucket eine Richtlinie zuweisen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. Amazon Redshift unterstützt keine ressourcenbasierten Richtlinien.

Angeben der Richtlinienelemente: Aktionen, Effekte, Ressourcen und Prinzipale

Für jede Amazon-Redshift-Ressource (siehe Amazon-Redshift-Ressourcen und -Operationen) definiert der Service eine Reihe von API-Vorgängen (siehe Aktionen). Zur Erteilung von Berechtigungen für diese API-Vorgänge definiert Amazon Redshift eine Reihe von Aktionen, die Sie in einer Richtlinie angeben können. Für das Durchführen einer API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein.

Grundlegende Richtlinienelemente:

- Ressource – In einer Richtlinie wird der Amazon-Ressourcenname (ARN) zur Identifizierung der Ressource verwendet, für die die Richtlinie gilt. Weitere Informationen finden Sie unter Amazon-Redshift-Ressourcen und -Operationen.
- Aktion – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten. Die `redshift:DescribeClusters`-Berechtigung erteilt dem Benutzer zum Beispiel Berechtigungen zum Durchführen des Amazon-Redshift-`DescribeClusters`-Vorgangs.
- Auswirkung – Die von Ihnen festgelegte Auswirkung, wenn der Benutzer die jeweilige Aktion anfordert – entweder „allow“ (Zugriffserlaubnis) oder „deny“ (Zugriffsverweigerung). Wenn Sie den Zugriff auf eine Ressource nicht ausdrücklich gestatten ("Allow"), wird er automatisch verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern. So können Sie sicherstellen, dass Benutzer nicht darauf zugreifen können, auch wenn der Zugriff durch eine andere Richtlinie gestattet wird.
- Prinzipal – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. In ressourcenbasierten Richtlinien müssen Sie den

Benutzer, das Konto, den Service oder die sonstige Entität angeben, die die Berechtigungen erhalten soll (gilt nur für ressourcenbasierte Richtlinien). Amazon Redshift unterstützt keine ressourcenbasierten Richtlinien.

Weitere Informationen zur Syntax und zu Beschreibungen von IAM-Richtlinien finden Sie in der AWS -IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Eine Tabelle mit allen Amazon-Redshift-API-Aktionen und den Ressourcen, für die sie gelten, finden Sie unter Zugriffsberechtigungen von Amazon Redshift, Amazon Redshift Serverless, der Amazon-Redshift-Daten-API und Amazon Redshift Query Editor v2.

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der Sprache der Zugriffsrichtlinie die Bedingungen angeben, wann die Richtlinie wirksam werden soll. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben von Bedingungen in der Sprache der Zugriffsrichtlinie finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Um Bedingungen zu identifizieren, unter denen eine Berechtigungsrichtlinie gilt, fügen Sie ein `Condition`-Element in Ihre IAM-Berechtigungsrichtlinie ein. Sie können beispielsweise eine Richtlinie erstellen, die einem Benutzer erlaubt, einen Cluster mit der Aktion `redshift:CreateCluster` zu erstellen, und Sie können ein `Condition`-Element hinzufügen, um die Einschränkung zu machen, dass dieser Benutzer den Cluster nur in einer bestimmten Region erstellen kann. Details hierzu finden Sie unter Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle. Eine Liste mit allen Bedingungsschlüsselwerten sowie den Amazon-Redshift-Aktionen und -Ressourcen, für die sie gelten, finden Sie unter Zugriffsberechtigungen von Amazon Redshift, Amazon Redshift Serverless, der Amazon-Redshift-Daten-API und Amazon Redshift Query Editor v2.

Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle

In Amazon Redshift können Sie Bedingungsschlüssel verwenden, um den Zugriff auf Ressourcen basierend auf den Tags dieser Ressourcen einzuschränken. Die folgenden Elemente sind gängige Amazon-Redshift-Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung
`aws:RequestTag`	Erfordert, dass Benutzer einen Tag-Schlüssel (Name) und einen Wert angeben, wenn sie eine Ressource erstellen. Weitere Informationen finden Sie unter aws: RequestTag im IAM-Benutzerhandbuch.
`aws:ResourceTag`	Beschränkt den Benutzerzugriff auf Ressourcen auf der Grundlage bestimmter Tag-Schlüssel und Werte. Weitere Informationen finden Sie unter aws: ResourceTag im IAM-Benutzerhandbuch.
`aws:TagKeys`	Verwenden Sie diesen Schlüssel, um die Tag-Schlüssel in einer Anforderung mit den Schlüsseln zu vergleichen, die Sie in der Richtlinie angeben. Weitere Informationen finden Sie unter aws: TagKeys im IAM-Benutzerhandbuch.

Weitere Informationen zu Tags finden Sie unter Markieren – Übersicht.

Eine Liste der API-Aktionen, die die Bedingungsschlüssel `redshift:RequestTag` und `redshift:ResourceTag` unterstützen, finden Sie unter Zugriffsberechtigungen von Amazon Redshift, Amazon Redshift Serverless, der Amazon-Redshift-Daten-API und Amazon Redshift Query Editor v2.

Die folgenden Bedingungsschlüssel können mit der Amazon Redshift GetClusterCredentials Redshift-Aktion verwendet werden.

Bedingungsschlüssel	Beschreibung
`redshift:DurationSeconds`	Begrenzt die Anzahl der Sekunden, die für die Dauer angegeben werden können.
`redshift:DbName`	Schränkt ein, welche Datenbanknamen angegeben werden können.
`redshift:DbUser`	Schränkt ein, welche Datenbankbenutzernamen angegeben werden können.

Beispiel 1: Beschränkung des Zugriffs mithilfe des Bedingungsschlüssels aws: ResourceTag

Verwenden Sie die folgende IAM-Richtlinie, damit ein Benutzer einen Amazon Redshift Redshift-Cluster nur für ein bestimmtes AWS Konto in der `us-west-2` Region mit einem Tag mit einem `environment` Tag-Wert von ändern kann. `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"
            }
        }
    }
}
```

Beispiel 2: Beschränken des Zugriffs mithilfe des Bedingungsschlüssels aws: RequestTag

Verwenden Sie die folgende IAM-Richtlinie, um einem Benutzer nur dann zu erlauben, einen Amazon-Redshift-Cluster zu erstellen, wenn der Befehl zum Erstellen des Clusters einen Tag mit der Bezeichnung `usage` und einen Tag-Wert von `production` enthält. Die Bedingung mit `aws:TagKeys` und der `ForAllValues`-Modifikator geben an, dass nur die Schlüssel `costcenter` und `usage` in der Anforderung angegeben werden können.

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

Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon Redshift

In diesem Thema finden Sie Beispiele für identitätsbasierte Richtlinien, in denen ein Kontoadministrator den IAM-Identitäten (Benutzer, Gruppen und Rollen) Berechtigungsrichtlinien anfügen kann.

> **Important**
>
> Wir empfehlen Ihnen, zunächst die einführenden Themen zu lesen, in denen die Grundkonzepte und die für Sie verfügbaren Optionen zum Verwalten des Zugriffs auf Ihre Amazon-Redshift-Ressourcen erläutert werden. Weitere Informationen finden Sie unter Übersicht zur Verwaltung der Zugriffsberechtigungen für Amazon-Redshift-Ressourcen.

Dies ist ein Beispiel für eine Berechtigungsrichtlinie. Die Richtlinie ermöglicht es einem Benutzer, alle Cluster zu erstellen, zu löschen, zu ändern und neu zu starten, und verweigert dann die Erlaubnis, alle Cluster zu löschen oder zu ändern, deren Cluster-ID mit `production` in AWS-Region `us-west-2` und beginnt. AWS-Konto `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"
    }
  ]
}
```

Die Richtlinie enthält zwei Anweisungen:

- Die erste Anweisung gibt einem Benutzer die Berechtigung zum Erstellen, Löschen, Modifizieren und erneuten Starten von Clustern. Die Anweisung gibt ein Platzhalterzeichen (*) als `Resource` Wert an, sodass die Richtlinie für alle Amazon Redshift Redshift-Ressourcen gilt, die dem AWS Root-Konto gehören.
- Die zweite Anweisung verweigert die Berechtigung zum Löschen oder Modifizieren eines Clusters. Die Anweisung gibt einen Cluster-ARN (Amazon-Ressourcenname) für den `Resource`-Wert an, der ein Platzhalterzeichen (*) enthält. Daher gilt diese Aussage für alle Amazon Redshift Redshift-Cluster, die dem AWS Root-Konto gehören, mit `production` dem die Cluster-ID beginnt.

AWS verwaltete Richtlinien für Amazon Redshift

AWS adressiert viele gängige Anwendungsfälle durch die Bereitstellung eigenständiger IAM-Richtlinien, die von erstellt und verwaltet werden. AWS Die verwalteten Richtlinien erteilen die erforderlichen Berechtigungen für viele häufige Anwendungsfälle, sodass Sie nicht mühsam ermitteln müssen, welche Berechtigungen erforderlich sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Sie können auch Ihre eigenen benutzerdefinierten IAM-Richtlinien erstellen, um Berechtigungen für Amazon-Redshift-API-Operationen und -Ressourcen zu gewähren. Die benutzerdefinierten Richtlinien können Sie dann den IAM-Rollen oder -Gruppen zuweisen, die diese Berechtigungen benötigen.

In den folgenden Abschnitten AWS werden verwaltete Richtlinien beschrieben, die Sie Benutzern in Ihrem Konto zuordnen können und die speziell für Amazon Redshift gelten.

AmazonRedshiftReadOnlyAccess

Gewährt schreibgeschützten Zugriff auf alle Amazon Redshift Redshift-Ressourcen für ein Konto. AWS

Sie finden die AmazonRedshiftReadOnlyAccessRichtlinie auf der IAM-Konsole und AmazonRedshiftReadOnlyAccessim AWS Managed Policy Reference Guide.

AmazonRedshiftFullAccess

Gewährt vollen Zugriff auf alle Amazon Redshift Redshift-Ressourcen für ein AWS Konto. Darüber hinaus gewährt diese Richtlinie vollen Zugriff auf alle Ressourcen von Amazon Redshift Serverless.

Sie finden die AmazonRedshiftFullAccessRichtlinie auf der IAM-Konsole und AmazonRedshiftFullAccessim AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditor

Gewährt vollständigen Zugriff auf den Abfrage-Editor in der Amazon-Redshift-Konsole.

Sie finden die AmazonRedshiftQueryEditorRichtlinie auf der IAM-Konsole und AmazonRedshiftQueryEditorim AWS Managed Policy Reference Guide.

AmazonRedshiftDataFullAccess

Gewährt vollen Zugriff auf die Amazon Redshift Data API-Operationen und Ressourcen für ein AWS Konto.

Sie finden die AmazonRedshiftDataFullAccessRichtlinie auf der IAM-Konsole und AmazonRedshiftDataFullAccessim AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorV2 FullAccess

Gewährt vollen Zugriff auf die Vorgänge und Ressourcen des Amazon-Redshift-Abfrage-Editors v2. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste.

Sie finden die AmazonRedshiftQueryEditorFullAccessV2-Richtlinie auf der IAM-Konsole und AmazonRedshiftQueryEditorV2 FullAccess im AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorV2 NoSharing

Ermöglicht es, mit dem Amazon-Redshift-Abfrage-Editor v2 zu arbeiten, ohne Ressourcen zu teilen. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Der Prinzipal, der diese Richtlinie verwendet, kann seine Ressourcen (z. B. Abfragen) nicht markieren, um sie mit anderen Prinzipalen im selben AWS-Konto zu teilen.

Sie finden die AmazonRedshiftQueryEditorNoSharingV2-Richtlinie auf der IAM-Konsole und AmazonRedshiftQueryEditorV2 NoSharing im AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorV2 ReadSharing

Ermöglicht die eingeschränkte Freigabe von Ressourcen bei der Arbeit mit dem Amazon-Redshift-Abfrage-Editor v2. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Der Prinzipal, der diese Richtlinie verwendet, kann seine Ressourcen (z. B. Abfragen) markieren, um sie mit anderen Prinzipalen im selben AWS-Konto zu teilen. Der Prinzipal mit der entsprechenden Berechtigung kann die mit seinem Team geteilten Ressourcen lesen, kann sie jedoch nicht ändern.

Sie finden die AmazonRedshiftQueryEditorReadSharingV2-Richtlinie auf der IAM-Konsole und AmazonRedshiftQueryEditorV2 ReadSharing im AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorV2 ReadWriteSharing

Ermöglicht die Freigabe von Ressourcen bei der Arbeit mit dem Amazon-Redshift-Abfrage-Editor v2. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Der Prinzipal, der diese Richtlinie verwendet, kann seine Ressourcen (z. B. Abfragen) markieren, um sie mit anderen Prinzipalen im selben AWS-Konto zu teilen. Der Prinzipal mit den entsprechenden Berechtigungen kann die mit seinem Team geteilten Ressourcen lesen und bearbeiten.

Sie finden die AmazonRedshiftQueryEditorReadWriteSharingV2-Richtlinie auf der IAM-Konsole und AmazonRedshiftQueryEditorV2 ReadWriteSharing im AWS Managed Policy Reference Guide.

AmazonRedshiftServiceLinkedRolePolicy

Sie können keine Verbindungen AmazonRedshiftServiceLinkedRolePolicy zu Ihren IAM-Entitäten herstellen. Diese Richtlinie ist an eine dienstgebundene Rolle angehängt, mit der Amazon Redshift auf Kontoressourcen zugreifen kann. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Redshift.

Sie finden die AmazonRedshiftServiceLinkedRolePolicyRichtlinie auf der IAM-Konsole und AmazonRedshiftServiceLinkedRolePolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

AmazonRedshiftAllCommandsFullAccess

Erlaubt es, die IAM-Rolle zu verwenden, die in der Amazon-Redshift-Konsole erstellt wurde, und legt sie als Standard fest, damit der Cluster die Befehle COPY von Amazon S3 sowie UNLOAD, CREATE EXTERNAL SCHEMA, CREATE EXTERNAL FUNCTION und CREATE MODEL ausführt. Die Richtlinie gewährt auch Berechtigungen zur Ausführung von SELECT-Anweisungen für verwandte Dienste wie Amazon S3, CloudWatch Logs SageMaker, Amazon oder AWS Glue.

Sie finden die AmazonRedshiftAllCommandsFullAccessRichtlinie auf der IAM-Konsole und AmazonRedshiftAllCommandsFullAccessim AWS Managed Policy Reference Guide.

Sie können auch Ihre eigenen benutzerdefinierten IAM-Richtlinien erstellen, um Berechtigungen für Amazon-Redshift-API-Operationen und -Ressourcen zu gewähren. Die benutzerdefinierten Richtlinien können Sie dann den IAM-Rollen oder -Gruppen zuweisen, die diese Berechtigungen benötigen.

Amazon Redshift Redshift-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon Redshift an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Amazon-Redshift-Seite „Document history“ (Dokumentverlauf).

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 FullAccess – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktionen `redshift-serverless:ListNamespaces` und `redshift-serverless:ListWorkgroups` werden der verwalteten Richtlinie hinzugefügt. Wenn Sie sie	21. Februar 2024

Änderung	Beschreibung	Datum
	hinzufügen, erhalten Sie die Erlaubnis, serverlose Namespaces und serverlos e Arbeitsgruppen im Amazon Redshift Data Warehouse aufzulisten.	
AmazonRedshiftQuer yEditorV2 NoSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktionen `redshift-serverless:ListNam espaces` und `redshift-serverless:ListWor kgroups` werden der verwalteten Richtlinie hinzugefügt. Wenn Sie sie hinzufügen, erhalten Sie die Erlaubnis, serverlose Namespaces und serverlos e Arbeitsgruppen im Amazon Redshift Data Warehouse aufzulisten.	21. Februar 2024

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 ReadSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktionen `redshift-serverless:ListNamespaces` und `redshift-serverless:ListWorkgroups` werden der verwalteten Richtlinie hinzugefügt. Wenn Sie sie hinzufügen, erhalten Sie die Erlaubnis, serverlose Namespaces und serverlose Arbeitsgruppen im Amazon Redshift Data Warehouse aufzulisten.	21. Februar 2024
AmazonRedshiftQueryEditorV2 ReadWriteSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktionen `redshift-serverless:ListNamespaces` und `redshift-serverless:ListWorkgroups` werden der verwalteten Richtlinie hinzugefügt. Wenn Sie sie hinzufügen, erhalten Sie die Erlaubnis, serverlose Namespaces und serverlose Arbeitsgruppen im Amazon Redshift Data Warehouse aufzulisten.	21. Februar 2024

Änderung	Beschreibung	Datum
AmazonRedshiftReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktion `redshift:ListRecommendations` wird der verwalteten Richtlinie hinzugefügt. Dadurch wird die Erlaubnis erteilt, Amazon Redshift Advisor-Empfehlungen aufzulisten.	7. Februar 2024
AmazonRedshiftServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktionen `ec2:AssignIpv6Addresses` und `ec2:UnassignIpv6Addresses` werden der verwalteten Richtlinie hinzugefügt. Wenn Sie diese hinzufügen, erhalten Sie die Berechtigung, IP-Adressen zuzuweisen und ihre Zuweisung aufzuheben.	31. Oktober 2023

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 NoSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktionen `sqlworkbench:GetAutocompletionMetadata` und `sqlworkbench:GetAutocompletionResource` werden der verwalteten Richtlinie hinzugefügt. Wenn Sie sie hinzufügen, erhalten Sie die Berechtigung zum Generieren und Abrufen von Datenbankinformationen für die automatische Vervollständigung von SQL während der Bearbeitung von Abfragen.	16. August 2023
AmazonRedshiftQueryEditorV2 ReadSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktionen `sqlworkbench:GetAutocompletionMetadata` und `sqlworkbench:GetAutocompletionResource` werden der verwalteten Richtlinie hinzugefügt. Wenn Sie sie hinzufügen, erhalten Sie die Berechtigung zum Generieren und Abrufen von Datenbankinformationen für die automatische Vervollständigung von SQL während der Bearbeitung von Abfragen.	16. August 2023

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 ReadWriteSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktionen `sqlworkbench:GetAutocompletionMetadata` und `sqlworkbench:GetAutocompletionResource` werden der verwalteten Richtlinie hinzugefügt. Wenn Sie sie hinzufügen, erhalten Sie die Berechtigung zum Generieren und Abrufen von Datenbankinformationen für die automatische Vervollständigung von SQL während der Bearbeitung von Abfragen.	16. August 2023

Änderung	Beschreibung	Datum
AmazonRedshiftServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Der verwalteten Richtlinie werden Berechtigungen für Aktionen AWS Secrets Manager zur Erstellung und Verwaltung von Geheimnissen hinzugefügt. Es wurden folgende Berechtigungen hinzugefügt: • `secretsmanager:GetRandomPassword` • `secretsmanager:DescribeSecret` • `secretsmanager:PutSecretValue` • `secretsmanager:UpdateSecret` • `secretsmanager:UpdateSecretVersionStage` • `secretsmanager:RotateSecret` • `secretsmanager:DeleteSecret`	14. August 2023

Änderung	Beschreibung	Datum
AmazonRedshiftServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Berechtigungen für Aktionen in Amazon EC2 zum Erstellen und Verwalten von Sicherheitsgruppen- und Routing-Regeln wurden von der verwalteten Richtlinie entfernt. Diese Berechtigungen betrafen die Erstellung von Subnetzen und VPCs. Es wurden folgende Berechtigungen entfernt: • `ec2:AuthorizeSecurityGroupEgress` • `ec2:AuthorizeSecurityGroupIngress` • `ec2:UpdateSecurityGroupRuleDescriptionsEgress` • `ec2:ReplaceRouteTableAssociation` • `ec2:CreateRouteTable` • `ec2:AttachInternetGateway` • `ec2:UpdateSecurityGroupRuleDescriptionsIngress` • `ec2:AssociateRouteTable` • `ec2:RevokeSecurityGroupIngress` • `ec2:CreateRoute`	8. Mai 2023

Änderung	Beschreibung	Datum
	• `ec2:CreateSecurityGroup` • `ec2:RevokeSecurityGroupEgress` • `ec2:ModifyVpcAttribute` • `ec2:CreateSubnet` • `ec2:CreateInternetGateway` • `ec2:CreateVpc` Diese wurden mit dem Tag Purpose: RedshiftMigrateToVpc resource verknüpft. Das Tag beschränkte den Umfang der Berechtigungen auf Aufgaben für die Migration von Amazon EC2 Classic zu Amazon EC2 VPC. Weitere Informationen über Ressourcen-Tags finden Sie unter Steuern des Zugriffs auf AWS-Ressourcen mithilfe von Ressourcen-Tags.	

Änderung	Beschreibung	Datum
AmazonRedshiftDataFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktion `redshift:GetClusterCredentialsWithIAM` wird der verwalteten Richtlinie hinzugefügt. Erteilt jetzt die Berechtigung zum Abrufen erweiterter temporärer Anmeldeinformationen für den Zugriff auf eine Amazon-Redshift-Datenbank durch das angegebene AWS-Konto.	07. April 2023
AmazonRedshiftServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Berechtigungen für Aktionen in Amazon EC2 zum Erstellen und Verwalten von Sicherheitsgruppenregeln wurden der verwalteten Richtlinie hinzugefügt. Diese Sicherheitsgruppen und Regeln sind speziell dem Amazon-Redshift-Ressourcen-Tag `aws:RequestTag/Redshift` zugeordnet. Dies beschränkt den Geltungsbereich der Berechtigungen auf bestimmte Amazon-Redshift-Ressourcen.	06. April 2023

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 NoSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktion `sqlworkbench:GetSchemaInference` wird der verwalteten Richtlinie hinzugefügt. Erteilt jetzt die Berechtigung zum Abrufen der aus einer Datei abgeleiteten Spalten und Datentypen.	21. März 2023
AmazonRedshiftQueryEditorV2 ReadSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktion `sqlworkbench:GetSchemaInference` wird der verwalteten Richtlinie hinzugefügt. Erteilt jetzt die Berechtigung zum Abrufen der aus einer Datei abgeleiteten Spalten und Datentypen.	21. März 2023
AmazonRedshiftQueryEditorV2 ReadWriteSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktion `sqlworkbench:GetSchemaInference` wird der verwalteten Richtlinie hinzugefügt. Erteilt jetzt die Berechtigung zum Abrufen der aus einer Datei abgeleiteten Spalten und Datentypen.	21. März 2023

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 NoSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktion `sqlworkbench:AssociateNotebookWithTab` wird der verwalteten Richtlinie hinzugefügt. Wenn diese hinzugefügt wird, wird damit die Berechtigung zum Erstellen und Aktualisieren von Registerkarten erteilt, die mit dem eigenen Notebook eines Benutzers verknüpft sind.	2. Februar 2023
AmazonRedshiftQueryEditorV2 ReadSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktion `sqlworkbench:AssociateNotebookWithTab` wird der verwalteten Richtlinie hinzugefügt. Wenn diese hinzugefügt wird, wird damit die Berechtigung zum Erstellen und Aktualisieren von Registerkarten erteilt, die mit dem eigenen Notebook eines Benutzers oder einem gemeinsam genutzten Notebook verknüpft sind.	2. Februar 2023

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 ReadWriteSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktion `sqlworkbench:AssociateNotebookWithTab` wird der verwalteten Richtlinie hinzugefügt. Wenn diese hinzugefügt wird, wird damit die Berechtigung zum Erstellen und Aktualisieren von Registerkarten erteilt, die mit dem eigenen Notebook eines Benutzers oder einem gemeinsam genutzten Notebook verknüpft sind.	2. Februar 2023

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 NoSharing – Aktualisierung auf eine bestehende Richtlinie	Um die Berechtigung zur Verwendung von Notebooks zu gewähren, hat Amazon Redshift die Berechtigung für die folgenden Aktionen hinzugefügt: • `sqlworkbench:ListNotebooks` • `sqlworkbench:CreateNotebook` • `sqlworkbench:DuplicateNotebook` • `sqlworkbench:CreateNotebookFromVersion` • `sqlworkbench:ImportNotebook` • `sqlworkbench:GetNotebook` • `sqlworkbench:UpdateNotebook` • `sqlworkbench:DeleteNotebook` • `sqlworkbench:CreateNotebookCell` • `sqlworkbench:DeleteNotebookCell` • `sqlworkbench:UpdateNotebookCellContent`	17. Oktober 2022

Änderung	Beschreibung	Datum
	• sqlworkbench:UpdateNotebookCellLayout • sqlworkbench:BatchGetNotebookCell • sqlworkbench:ListNotebookVersions • sqlworkbench:CreateNotebookVersion • sqlworkbench:GetNotebookVersion • sqlworkbench:DeleteNotebookVersion • sqlworkbench:RestoreNotebookVersion • sqlworkbench:ExportNotebook	

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 ReadSharing – Aktualisierung auf eine bestehende Richtlinie	Um die Berechtigung zur Verwendung von Notebooks zu gewähren, hat Amazon Redshift die Berechtigung für die folgenden Aktionen hinzugefügt: • `sqlworkbench:ListNotebooks` • `sqlworkbench:CreateNotebook` • `sqlworkbench:DuplicateNotebook` • `sqlworkbench:CreateNotebookFromVersion` • `sqlworkbench:ImportNotebook` • `sqlworkbench:GetNotebook` • `sqlworkbench:UpdateNotebook` • `sqlworkbench:DeleteNotebook` • `sqlworkbench:CreateNotebookCell` • `sqlworkbench:DeleteNotebookCell` • `sqlworkbench:UpdateNotebookCellContent`	17. Oktober 2022

Änderung	Beschreibung	Datum
	• sqlworkbench:UpdateNotebookCellLayout • sqlworkbench:BatchGetNotebookCell • sqlworkbench:ListNotebookVersions • sqlworkbench:CreateNotebookVersion • sqlworkbench:GetNotebookVersion • sqlworkbench:DeleteNotebookVersion • sqlworkbench:RestoreNotebookVersion • sqlworkbench:ExportNotebook	

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 ReadWriteSharing – Aktualisierung auf eine bestehende Richtlinie	Um die Berechtigung zur Verwendung von Notebooks zu gewähren, hat Amazon Redshift die Berechtigung für die folgenden Aktionen hinzugefügt: • `sqlworkbench:ListNotebooks` • `sqlworkbench:CreateNotebook` • `sqlworkbench:DuplicateNotebook` • `sqlworkbench:CreateNotebookFromVersion` • `sqlworkbench:ImportNotebook` • `sqlworkbench:GetNotebook` • `sqlworkbench:UpdateNotebook` • `sqlworkbench:DeleteNotebook` • `sqlworkbench:CreateNotebookCell` • `sqlworkbench:DeleteNotebookCell` • `sqlworkbench:UpdateNotebookCellContent`	17. Oktober 2022

Änderung	Beschreibung	Datum
	• `sqlworkbench:UpdateNotebookCellLayout` • `sqlworkbench:BatchGetNotebookCell` • `sqlworkbench:ListNotebookVersions` • `sqlworkbench:CreateNotebookVersion` • `sqlworkbench:GetNotebookVersion` • `sqlworkbench:DeleteNotebookVersion` • `sqlworkbench:RestoreNotebookVersion` • `sqlworkbench:ExportNotebook`	
AmazonRedshiftServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat den Namespace `AWS/Redshift` hinzugefügt, in dem Metriken veröffentlicht werden können. CloudWatch	7. September 2022

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 NoSharing – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat den Aktionen `sqlworkbench:ListQueryExecutionHistory` und `sqlworkbench:GetQueryExecutionHistory` eine Berechtigung hinzugefügt. Dadurch wird die Berechtigung erteilt, den Abfrageverlauf anzuzeigen.	30. August 2022
AmazonRedshiftQueryEditorV2 ReadSharing – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat den Aktionen `sqlworkbench:ListQueryExecutionHistory` und `sqlworkbench:GetQueryExecutionHistory` eine Berechtigung hinzugefügt. Dadurch wird die Berechtigung erteilt, den Abfrageverlauf anzuzeigen.	30. August 2022
AmazonRedshiftQueryEditorV2 ReadWriteSharing – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat den Aktionen `sqlworkbench:ListQueryExecutionHistory` und `sqlworkbench:GetQueryExecutionHistory` eine Berechtigung hinzugefügt. Dadurch wird die Berechtigung erteilt, den Abfrageverlauf anzuzeigen.	30. August 2022

Änderung	Beschreibung	Datum
AmazonRedshiftFullAccess – Aktualisierung auf eine bestehende Richtlinie	Berechtigungen für Amazon Redshift Serverless werden der bestehenden AmazonRedshiftFullAccess verwalteten Richtlinie hinzugefügt.	22. Juli 2022
AmazonRedshiftDataFullAccess – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat die Standardbedingung `redshift-serverless:GetCredentials` für den Geltungsbereich des Tags `aws:ResourceTag/RedshiftDataFullAccess` von `StringEquals` auf `StringLike` aktualisiert, um Zugriff auf Ressourcen zu gewähren, die mit dem Tag-Schlüssel `RedshiftDataFullAccess` und einem beliebigen Tag-Wert markiert sind.	11. Juli 2022
AmazonRedshiftDataFullAccess – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat neue Berechtigungen hinzugefügt, um `redshift-serverless:GetCredentials` für temporäre Anmeldeinformationen für Amazon Redshift Serverless zuzulassen.	8. Juli 2022

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 NoSharing – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat der Aktion `sqlworkbench:GetAccountSettings` die Berechtigung hinzugefügt. Damit wird die Berechtigung zum Abrufen von Kontoeinstellungen gewährt.	15. Juni 2022
AmazonRedshiftQueryEditorV2 ReadSharing – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat der Aktion `sqlworkbench:GetAccountSettings` die Berechtigung hinzugefügt. Damit wird die Berechtigung zum Abrufen von Kontoeinstellungen gewährt.	15. Juni 2022
AmazonRedshiftQueryEditorV2 ReadWriteSharing – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat der Aktion `sqlworkbench:GetAccountSettings` die Berechtigung hinzugefügt. Damit wird die Berechtigung zum Abrufen von Kontoeinstellungen gewährt.	15. Juni 2022

Änderung	Beschreibung	Datum
AmazonRedshiftServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Um den öffentlichen Zugriff auf neue Endpunkte von Amazon Redshift Serverless zu ermöglichen, weist Amazon Redshift der Elastic-Network-Schnittstelle des VPC-Endpunkts Elastic IP-Adressen im Kundenkonto zu und verknüpft sie. Dies geschieht über Berechtigungen, die über die serviceverknüpfte Rolle bereitgestellt werden. Für diesen Anwendungsfall werden der mit dem Amazon-Redshift-Serverless-Service verknüpften Rolle Aktionen zum Zuweisen und Freigeben einer Elastic IP-Adresse hinzugefügt.	26. Mai 2022
AmazonRedshiftQueryEditorV2 FullAccess – Aktualisierung auf eine bestehende Richtlinie	Berechtigungen für die Aktion `sqlworkbench:ListTaggedResources` . Speziell auf Ressourcen des Abfrage-Editors v2 von Amazon Redshift ausgerichtet. Durch dieses Richtlinienupdate wird die Berechtigung erteilt, `tag:GetResources` nur über den Abfrage-Editor v2 aufzurufen.	22. Februar 2022

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 NoSharing – Aktualisierung auf eine bestehende Richtlinie	Berechtigungen für die Aktion `sqlworkbench:ListTaggedResources` . Speziell auf Ressourcen des Abfrage-Editors v2 von Amazon Redshift ausgerichtet. Durch dieses Richtlinienupdate wird die Berechtigung erteilt, `tag:GetResources` nur über den Abfrage-Editor v2 aufzurufen.	22. Februar 2022
AmazonRedshiftQueryEditorV2 ReadSharing – Aktualisierung auf eine bestehende Richtlinie	Berechtigungen für die Aktion `sqlworkbench:ListTaggedResources` . Speziell auf Ressourcen des Abfrage-Editors v2 von Amazon Redshift ausgerichtet. Durch dieses Richtlinienupdate wird die Berechtigung erteilt, `tag:GetResources` nur über den Abfrage-Editor v2 aufzurufen.	22. Februar 2022
AmazonRedshiftQueryEditorV2 ReadWriteSharing – Aktualisierung auf eine bestehende Richtlinie	Berechtigungen für die Aktion `sqlworkbench:ListTaggedResources` . Speziell auf Ressourcen des Abfrage-Editors v2 von Amazon Redshift ausgerichtet. Durch dieses Richtlinienupdate wird die Berechtigung erteilt, `tag:GetResources` nur über den Abfrage-Editor v2 aufzurufen.	22. Februar 2022

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 ReadSharing – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung für die Aktion `sqlworkbench:AssociateQueryWithTab` wurde der verwalteten Richtlinie hinzugefügt. Dadurch können Kunden Editor-Registerkarten erstellen, die mit einer für sie freigegebenen Abfrage verknüpft sind.	22. Februar 2022
AmazonRedshiftServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Für Amazon Redshift gibt es jetzt neue Berechtigungen für neue Aktionen, mit denen Sie Amazon-Redshift-Netzwerk- und Amazon-Redshift-VPC-Ressourcen verwalten können.	22. November 2021
AmazonRedshiftAllCommandsFullAccess – Neue Richtlinie.	Für Amazon Redshift gibt es jetzt eine neue Richtlinie, mit der Sie die IAM-Rolle verwenden können, die in der Amazon-Redshift-Konsole erstellt wurde, und hat sie als Standard festgelegt, damit der Cluster die Befehle COPY von Amazon S3 sowie UNLOAD, CREATE EXTERNAL SCHEMA, CREATE EXTERNAL FUNCTION, CREATE MODEL und CREATE LIBRARY ausführt.	18. November 2021

Änderung	Beschreibung	Datum
AmazonRedshiftServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat Berechtigungen für neue Aktionen hinzugefügt, um die Verwaltung von Amazon Redshift CloudWatch Redshift-Protokollgruppen und Protokoll streams, einschließlich Audit-Log-Export, zu ermöglichen.	15. November 2021
AmazonRedshiftFullAccess – Aktualisierung auf eine bestehende Richtlinie	Für Amazon Redshift gibt es jetzt neue Berechtig ungen für Modellerklärbarkei t, DynamoDB, Redshift Spectrum und Amazon-RDS-Verbund.	7. Oktober 2021
AmazonRedshiftQuer yEditorV2 FullAccess – Neue Richtlinie.	Für Amazon Redshift gibt es jetzt eine neue Richtlinie für vollen Zugriff auf den Amazon-Redshift-Abfrage-Editor v2.	24. September 2021
AmazonRedshiftQuer yEditorV2 NoSharing – Neue Richtlinie.	Für Amazon Redshift gibt es jetzt eine neue Richtlinie, die die Verwendung des Amazon-Redshift-Abfrage-Editors v2 ohne Freigabe von Ressource n erlaubt.	24. September 2021
AmazonRedshiftQuer yEditorV2 ReadSharing – Neue Richtlinie.	Für Amazon Redshift gibt es jetzt eine neue Richtlinie, die das Lesen der Freigabe innerhalb des Amazon-Re dshift-Abfrage-Editors v2 erlaubt.	24. September 2021

Änderung	Beschreibung	Datum
AmazonRedshiftQueryEditorV2 ReadWriteSharing – Neue Richtlinie.	Für Amazon Redshift gibt es jetzt eine neue Richtlinie, die das Lesen und Aktualisieren der Freigabe im Amazon-Redshift-Abfrage-Editor v2 erlaubt.	24. September 2021
AmazonRedshiftFullAccess – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat neue Berechtigungen zum Erlauben von hinzugefügt `sagemaker:*Job*` .	18. August 2021
AmazonRedshiftDataFullAccess – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat neue Berechtigungen zum Erlauben von hinzugefügt `AuthorizeDataShare` .	12. August 2021
AmazonRedshiftDataFullAccess – Aktualisierung auf eine bestehende Richtlinie	Amazon Redshift hat neue Berechtigungen zum Erlauben von hinzugefügt `BatchExecuteStatement` .	27. Juli 2021
Amazon Redshift begann Nachverfolgung von Änderungen	Amazon Redshift hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	27. Juli 2021

Erforderliche Berechtigungen zur Verwendung von Redshift Spectrum

Amazon Redshift Spectrum benötigt für den Zugriff auf Ressourcen Berechtigungen für andere AWS Services. Detaillierte Informationen über Berechtigungen in IAM-Richtlinien für Redshift Spectrum finden Sie unter IAM-Richtlinien für Amazon Redshift Spectrum im Datenbankentwicklerhandbuch zu Amazon Redshift.

Erforderliche Berechtigungen zur Verwendung der Amazon-Redshift-Konsole

Damit ein Benutzer mit der Amazon Redshift Redshift-Konsole arbeiten kann, muss er über Mindestberechtigungen verfügen, die es dem Benutzer ermöglichen, die Amazon Redshift Redshift-Ressourcen für sein AWS Konto zu beschreiben. Diese Berechtigungen müssen es dem Benutzer auch ermöglichen, andere verwandte Informationen zu beschreiben, darunter Amazon EC2-Sicherheit, Amazon CloudWatch, Amazon SNS und Netzwerkinformationen.

Wenn Sie eine IAM-Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Benutzer mit dieser IAM-Richtlinie. Um sicherzustellen, dass diese Benutzer die Amazon-Redshift-Konsole weiterhin verwenden können, weisen Sie ihnen auch die von `AmazonRedshiftReadOnlyAccess` verwaltete Richtlinie zu. Die Vorgehensweise ist in beschrieben AWS verwaltete Richtlinien für Amazon Redshift.

Informationen dazu, wie Sie einem Benutzer Zugriff auf den Abfrage-Editor in der Amazon-Redshift-Konsole geben, finden Sie unter Erforderliche Berechtigungen zur Verwendung des Abfrage-Editors der Amazon-Redshift-Konsole.

Sie müssen Benutzern, die nur die Amazon Redshift-API AWS CLI oder die Amazon Redshift Redshift-API aufrufen, keine Mindestberechtigungen für die Konsole gewähren.

Erforderliche Berechtigungen zur Verwendung des Abfrage-Editors der Amazon-Redshift-Konsole

Damit Benutzer mit dem Amazon-Redshift-Abfrage-Editor arbeiten können, müssen sie über einen Mindestsatz von Berechtigungen für Amazon Redshift und Amazon-Redshift-Data-API-Vorgänge verfügen. Um sich über ein Secret mit einer Datenbank zu verbinden, müssen Sie auch über Secrets-Manager-Berechtigungen verfügen.

Um einem Benutzer Zugriff auf den Abfrage-Editor auf der Amazon Redshift Redshift-Konsole zu gewähren, hängen Sie die `AmazonRedshiftQueryEditor` und die `AmazonRedshiftReadOnlyAccess` AWS verwalteten Richtlinien an. Die `AmazonRedshiftQueryEditor`-Richtlinie erlaubt Benutzern, nur die Ergebnisse ihrer eigenen SQL-Anweisungen abzurufen – Das sind Aussagen, die von derselben Person eingereicht wurden, `aws:userid` wie in diesem Abschnitt der `AmazonRedshiftQueryEditor` AWS verwalteten Richtlinie dargestellt.

```
{
    "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:userid}"
        }
    }
}
```

Damit ein Benutzer die Ergebnisse von SQL-Anweisungen anderer Benutzer in derselben IAM-Rolle abrufen kann, erstellen Sie eine eigene Richtlinie ohne die Bedingung, den Zugriff auf den aktuellen Benutzer zu beschränken. Beschränken Sie auch die Berechtigung zum Ändern einer Richtlinie auf einen Administrator.

Für die Verwendung des Abfrage-Editors v2 erforderliche Berechtigungen

Damit ein Benutzer mit dem Amazon Redshift-Abfrage-Editor v2 arbeiten kann, muss er über Mindestberechtigungen für Amazon Redshift, den Abfrage-Editor v2-Operationen und andere AWS Dienste wie AWS Key Management Service AWS Secrets Manager, und Tagging-Service verfügen.

Um einem Benutzer vollen Zugriff auf den Abfrage-Editor v2 zu gewähren, fügen Sie die `AmazonRedshiftQueryEditorV2FullAccess` AWS verwaltete Richtlinie an. Die `AmazonRedshiftQueryEditorV2FullAccess`-Richtlinie erlaubt es dem Benutzer, Ressourcen des Abfrage-Editors v2 (z. B. Abfragen) mit anderen im selben Team zu teilen. Weitere Informationen darüber, wie der Zugriff auf v2-Ressourcen des Abfrage-Editors gesteuert wird, finden Sie in der Definition der bestimmten verwalteten Richtlinie für den Abfrage-Editor v2 in der IAM-Konsole.

Einige AWS verwaltete Amazon Redshift Query Editor v2-Richtlinien verwenden AWS Tags innerhalb von Bedingungen, um den Zugriff auf Ressourcen einzuschränken. Innerhalb des Abfrage-Editors v2 basiert das Teilen von Abfragen auf dem Tag-Schlüssel und dem Wert `"aws:ResourceTag/sqlworkbench-team": "${aws:PrincipalTag/sqlworkbench-team}"` in der IAM-Richtlinie, die an den Prinzipal angehängt ist (die IAM-Rolle). Principals in derselben Gruppe AWS-Konto mit demselben Tag-Wert (z. B.`accounting-team`) gehören im Abfrage-Editor v2 zum selben Team. Man kann jeweils nur mit einem Team verbunden sein. Ein Benutzer mit Administratorberechtigungen kann Teams in der IAM-Konsole einrichten, indem er allen Teammitgliedern den gleichen Wert für

das Tag `sqlworkbench-team` gibt. Wenn der Tag-Wert von `sqlworkbench-team` für einen IAM-Benutzer oder eine IAM-Rolle geändert wird, kann es eine Zeit dauern, bis die Änderung in den freigegebenen Ressourcen angezeigt wird. Wenn der Tag-Wert einer Ressource (z. B. einer Abfrage) geändert wird, kann es erneut zu einer Verzögerung kommen. Teammitglieder brauchen auch die Berechtigung `tag:GetResources` zum Teilen.

Beispiel: Das Tag **`accounting-team`** für eine IAM-Rolle hinzufügen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der Konsole Rollen aus und wählen Sie dann den Namen der Rolle aus, die Sie bearbeiten möchten.
3. Wählen Sie die Registerkarte Tags und dann Add tags (Tags hinzufügen) aus.
4. Fügen Sie den Tag-Schlüssel sqlworkbench-team und den Wert `accounting-team` hinzu.
5. Wählen Sie Save Changes.

   Wenn nun ein IAM-Prinzipal (dem diese IAM-Rolle angefügt wurde) eine Abfrage mit dem Team teilt, können andere Prinzipale mit demselben Tag-Wert bei `accounting-team` die Abfrage sehen.

Weitere Informationen darüber, wie Sie ein Tag an einen Prinzipal anhängen, einschließlich IAM-Rollen und IAM-Benutzern, finden Sie unter Markieren von IAM-Ressourcen im IAM-Benutzerhandbuch.

Sie können Teams auch auf Sitzungsebene mit einem Identitätsanbieter (IdP) einrichten. Dies ermöglicht es mehreren Benutzern, die dieselbe IAM-Rolle verwenden, ein anderes Team zu haben. Die IAM-Rollen-Vertrauensrichtlinie muss den Vorgang `sts:TagSession` erlauben. Weitere Informationen finden Sie unter Zum Hinzufügen von Sitzungstags erforderliche Berechtigungen im IAM-Benutzerhandbuch. Fügen Sie das Tag-Attribut des Prinzipals zur SAML-Assertion hinzu, die von Ihrem IdP bereitgestellt wird.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:sqlworkbench-
team">
    <AttributeValue>accounting-team</AttributeValue>
</Attribute>
```

Folgen Sie den Anweisungen für Ihren Identitätsanbieter (IdP), um das SAML-Attribut mit dem Inhalt zu füllen, der aus Ihrem Verzeichnis stammt. Weitere Informationen zu Identity Providers

(IdPs) und Amazon Redshift finden Sie unter Verwenden der IAM-Authentifizierung zur Erstellung von Anmeldeinformationen für Datenbankbenutzern Identity providers and federation im IAM-Benutzerhandbuch.

`sqlworkbench:CreateNotebookVersion` erteilt die Berechtigung, den aktuellen Inhalt von Notebook-Zellen abzurufen und eine Notebook-Version in Ihrem Konto zu erstellen. Dies bedeutet, dass der aktuelle Inhalt des Notebooks zum Zeitpunkt der Versionserstellung dem Inhalt der Version entspricht. Später bleibt der Inhalt der Zellen in der Version unverändert, wenn das aktuelle Notebook aktualisiert wird. `sqlworkbench:GetNotebookVersion` erteilt die Berechtigung, eine Version des Notebooks abzurufen. Ein Benutzer, der nicht über die Berechtigung `sqlworkbench:BatchGetNotebookCell`, jedoch über die Berechtigungen `sqlworkbench:CreateNotebookVersion` und `sqlworkbench:GetNotebookVersion` für ein Notebook verfügt, hat Zugriff auf Notebook-Zellen in der Version. Dieser Benutzer ohne die Berechtigung `sqlworkbench:BatchGetNotebookCell` kann immer noch den Inhalt der Zellen eines Notebooks abrufen, indem er zuerst eine Version erstellt und dann diese erstellte Version abruft.

Erforderliche Berechtigungen zur Verwendung des Amazon-Redshift-Schedulers

Wenn Sie den Amazon-Redshift-Scheduler verwenden, richten Sie eine IAM-Rolle mit einer Vertrauensstellung zum Amazon-Redshift-Scheduler (**`scheduler.redshift.amazonaws.com`**) ein, damit der Scheduler in Ihrem Namen Berechtigungen übernehmen kann. Sie weisen der Rolle auch eine Richtlinie (Berechtigungen) für die Amazon-Redshift-API-Vorgänge zu, die Sie planen möchten.

Das folgende Beispiel zeigt das Richtliniendokument im JSON-Format zum Einrichten einer Vertrauensstellung mit dem Amazon-Redshift-Scheduler und Amazon Redshift.

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

```
        }
    ]
}
```

Weitere Informationen zu vertrauenswürdigen Entitäten finden Sie im IAM-Benutzerhandbuch unter Creating a role to delegate permissions to a AWS service.

Sie müssen außerdem eine Berechtigung für die Amazon-Redshift-Vorgänge hinzufügen, die Sie planen möchten.

Damit der Scheduler die `ResizeCluster`-Operation verwenden kann, fügen Sie Ihrer IAM-Richtlinie eine Berechtigung hinzu, die der folgenden ähnlich ist. Abhängig von Ihrer Umgebung sollten Sie die Richtlinie möglicherweise restriktiver gestalten.

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

Die Schritte zum Erstellen einer Rolle für den Amazon Redshift Redshift-Scheduler finden Sie unter Creating a role for an AWS service (console) im IAM-Benutzerhandbuch. Treffen Sie diese Entscheidungen, wenn Sie eine Rolle in der IAM-Konsole erstellen:

- Für Choose the service that will use this role (Einen Service auswählen, der diese Rolle verwenden soll): Wählen Sie Redshift aus.
- Für Select your use case (Wählen Sie Ihren Anwendungsfall) Folgendes aus: Wählen Sie Redshift - Scheduler aus.
- Erstellen Sie eine Richtlinie oder weisen Sie diese der Rolle zu, die das Planen eines Amazon-Redshift-Vorgangs zulässt. Wählen Sie Create policy (Richtlinie erstellen) aus oder ändern Sie die Rolle, um eine Richtlinie zuzuweisen. Geben Sie die JSON-Richtlinie für die Operation ein, die geplant werden soll.
- Nachdem Sie die Rolle erstellt haben, bearbeiten Sie die Trust Relationship (Vertrauensbeziehung) der IAM-Rolle, um den `redshift.amazonaws.com`-Service aufzunehmen.

Die von Ihnen erstellte IAM-Rolle hat vertrauenswürdige Entitäten von `scheduler.redshift.amazonaws.com` und `redshift.amazonaws.com`. Sie weist außerdem eine angefügte Richtlinie auf, die eine unterstützte Amazon-Redshift-API-Aktion wie zulässt., `"redshift:ResizeCluster"`.

Für die Verwendung des Amazon EventBridge Schedulers sind Berechtigungen erforderlich

Wenn Sie den EventBridge Amazon-Scheduler verwenden, richten Sie eine IAM-Rolle mit einer Vertrauensbeziehung zum EventBridge Scheduler (**`events.amazonaws.com`**) ein, damit der Scheduler in Ihrem Namen Berechtigungen übernehmen kann. Außerdem fügen Sie der Rolle eine Richtlinie (Berechtigungen) für die Amazon Redshift Data API-Operationen, die Sie planen möchten, und eine Richtlinie für EventBridge Amazon-Operationen hinzu.

Sie verwenden den EventBridge Scheduler, wenn Sie geplante Abfragen mit dem Amazon Redshift Redshift-Abfrage-Editor auf der Konsole erstellen.

Sie können eine IAM-Rolle erstellen, um geplante Abfragen in der IAM-Konsole auszuführen. Fügen Sie in dieser IAM-Rolle `AmazonEventBridgeFullAccess` und `AmazonRedshiftDataFullAccess` an.

Das folgende Beispiel zeigt das Richtliniendokument im JSON-Format, um eine Vertrauensbeziehung mit dem EventBridge Scheduler einzurichten.

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

Weitere Informationen zu vertrauenswürdigen Entitäten finden Sie im IAM-Benutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS Dienst.

Die Schritte zum Erstellen einer Rolle für den EventBridge Scheduler finden Sie unter Erstellen einer Rolle für einen AWS Dienst (Konsole) im IAM-Benutzerhandbuch. Treffen Sie diese Entscheidungen, wenn Sie eine Rolle in der IAM-Konsole erstellen:

- Für Wählen Sie den Dienst aus, der diese Rolle verwenden soll: Wählen Sie CloudWatch Ereignisse.
- Für Wählen Sie Ihren Anwendungsfall aus: Wählen Sie CloudWatch Ereignisse.
- Fügen Sie die folgenden Berechtigungsrichtlinien an: `AmazonEventBridgeFullAccess` und `AmazonRedshiftDataFullAccess`.

Die von Ihnen erstellte IAM-Rolle hat eine vertrauenswürdige Entität von `events.amazonaws.com`. Sie weist außerdem eine angefügte Richtlinie auf, die unterstützte Amazon-Redshift-Data-API-Aktionen wie zulässt., `"redshift-data:*"`.

Für die Verwendung von Amazon Redshift Machine Learning (ML) erforderliche Berechtigungen

Nachfolgend finden Sie eine Beschreibung der Berechtigungen, die zur Nutzung von Amazon Redshift Machine Learning (ML) für verschiedene Anwendungsfälle erforderlich sind.

Damit Ihre Benutzer Amazon Redshift ML mit Amazon verwenden können SageMaker, erstellen Sie eine IAM-Rolle mit einer restriktiveren Richtlinie als der Standardrichtlinie. Sie können die folgende Richtlinie verwenden. Sie können diese Richtlinie auch entsprechend Ihren Anforderungen anpassen.

Die folgende Richtlinie zeigt die Berechtigungen, die für die Ausführung von SageMaker Autopilot mit Modellerklärbarkeit von Amazon Redshift erforderlich sind.

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

```
    ]
}
```

Die folgende Richtlinie zeigt die vollständigen Mindestberechtigungen für den Zugriff auf Amazon DynamoDB, Redshift Spectrum und Amazon-RDS-Verbund.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateAutoMLJob",
                "sagemaker:CreateCompilationJob",
                "sagemaker:CreateEndpoint",
                "sagemaker:DescribeAutoMLJob",
                "sagemaker:DescribeTrainingJob",
                "sagemaker:DescribeCompilationJob",
                "sagemaker:DescribeProcessingJob",
                "sagemaker:DescribeTransformJob",
                "sagemaker:ListCandidatesForAutoMLJob",
                "sagemaker:StopAutoMLJob",
                "sagemaker:StopCompilationJob",
                "sagemaker:StopTrainingJob",
                "sagemaker:DescribeEndpoint",
                "sagemaker:InvokeEndpoint",
                "sagemaker:StopProcessingJob",
                "sagemaker:CreateModel",
                "sagemaker:CreateProcessingJob"
            ],
            "Resource": [
                "arn:aws:sagemaker:*:*:model/*redshift*",
                "arn:aws:sagemaker:*:*:training-job/*redshift*",
                "arn:aws:sagemaker:*:*:automl-job/*redshift*",
                "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
                "arn:aws:sagemaker:*:*:processing-job/*redshift*",
                "arn:aws:sagemaker:*:*:transform-job/*redshift*",
                "arn:aws:sagemaker:*:*:endpoint/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "SageMaker",
                        "/aws/sagemaker/Endpoints",
                        "/aws/sagemaker/ProcessingJobs",
                        "/aws/sagemaker/TrainingJobs",
                        "/aws/sagemaker/TransformJobs"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:BatchGetImage",
                "ecr:GetAuthorizationToken",
                "ecr:GetDownloadUrlForLayer"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": [
                "arn:aws:s3:::redshift-downloads",
                "arn:aws:s3:::redshift-downloads/*",
                "arn:aws:s3:::*redshift*",
                "arn:aws:s3:::*redshift*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringEqualsIgnoreCase": {
                    "s3:ExistingObjectTag/Redshift": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:Scan",
                "dynamodb:DescribeTable",
                "dynamodb:Getitem"
            ],
            "Resource": [
                "arn:aws:dynamodb:*:*:table/*redshift*",
                "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticmapreduce:ListInstances"
            ],
            "Resource": [
                "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticmapreduce:ListInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "elasticmapreduce:ResourceTag/Redshift": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:*:*:function:*redshift*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:BatchDeleteTable",
                "glue:UpdateTable",
                "glue:GetTable",
                "glue:GetTables",
                "glue:BatchCreatePartition",
                "glue:CreatePartition",
                "glue:DeletePartition",
                "glue:BatchDeletePartition",
                "glue:UpdatePartition",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:BatchGetPartition"
            ],
            "Resource": [
                "arn:aws:glue:*:*:table/*redshift*/*",
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:*redshift*"
            ]
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "secretsmanager:GetRandomPassword",
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "secretsmanager:ResourceTag/Redshift": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "redshift.amazonaws.com",
                        "glue.amazonaws.com",
                        "sagemaker.amazonaws.com",
                        "athena.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Um optional einen AWS KMS Schlüssel für die Verschlüsselung zu verwenden, fügen Sie der Richtlinie die folgenden Berechtigungen hinzu.

```
{
    "Effect": "Allow",
    "Action": [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:GenerateDataKey*"
    ],
```

```
    "Resource": [
        "arn:aws:kms:<your-region>:<your-account-id>:key/<your-kms-key>"
    ]
}
```

Um Amazon Redshift die Interaktion mit anderen Diensten SageMaker zu ermöglichen und die vorherige IAM-Rolle anzunehmen, fügen Sie der Rolle die folgende Vertrauensrichtlinie hinzu.

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

In der vorhergehenden ist der Amazon S3 Bucket `redshift-downloads/redshift-ml/` der Ort, an dem die Beispieldaten für andere Schritte und Beispiele gespeichert werden. Sie können ihn entfernen, wenn Sie keine Daten aus Amazon S3 laden müssen. Sie können ihn auch durch andere Amazon S3 Buckets ersetzen, die Sie zum Laden von Daten in Amazon Redshift verwenden.

Die Werte **`your-account-id`**, **`your-role`** und **`your-s3-bucket`** sind die Konto-ID, die Rolle und der Bucket, die Sie in Ihrem Befehl CREATE MODEL angeben.

Optional können Sie den Abschnitt AWS KMS Schlüssel der Beispielrichtlinie verwenden, wenn Sie einen AWS KMS Schlüssel für die Verwendung mit Amazon Redshift ML angeben. Der Wert **`your-kms-key`** ist der Schlüssel, den Sie als Teil Ihres CREATE-MODEL-Befehls verwenden.

Wenn Sie eine private Virtual Private Cloud (VPC) für den Hyperparameter-Optimierungsauftrag angeben, fügen Sie die folgenden Berechtigungen hinzu.

```
{
```

```
            "Effect": "Allow",
            "Action": [
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeVpcs",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups"
            ]
}
```

Um mit der Modellerklärung arbeiten zu können, stellen Sie sicher, dass Sie über die Berechtigungen zum Aufrufen von SageMaker API-Operationen verfügen. Wir empfehlen Ihnen dazu die verwaltete Richtlinie `AmazonSageMakerFullAccess`. Wenn Sie eine IAM-Rolle mit einer restriktiveren Richtlinie erstellen möchten, können Sie die folgende verwenden.

```
{
  "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": "*"
    }
  ]
}
```

Weitere Informationen zur `AmazonSageMakerFullAccess` verwalteten Richtlinie finden Sie AmazonSageMakerFullAccessim Amazon SageMaker Developer Guide.

Wenn Sie Prognosemodelle erstellen möchten, empfehlen wir, die verwaltete Richtlinie `AmazonForecastFullAccess` zu verwenden. Wenn Sie restriktivere Richtlinie verwenden möchten, fügen Sie Ihrer IAM-Rolle die folgende Richtlinie hinzu.

```
{
    "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": "*"
        }
    ]
}
```

Weitere Informationen zum Amazon-Redshift-ML finden Sie unter Verwenden von Machine Learning in Amazon Redshift oder CREATE MODEL.

Berechtigungen für die Streaming-Erfassung

Die Streaming-Erfassung funktioniert mit zwei Services. Dies sind Kinesis Data Streams und Amazon MSK.

Erforderliche Berechtigungen für die Verwendung der Streaming-Erfassung mit Kinesis Data Streams

Ein Verfahren mit einem Beispiel für verwaltete Richtlinien finden Sie unter Erste Schritte mit der Streaming-Erfassung von Amazon Kinesis Data Streams.

Erforderliche Berechtigungen für die Verwendung der Streaming-Erfassung mit Amazon MSK

Ein Verfahren mit einem Beispiel für verwaltete Richtlinien finden Sie unter Erste Schritte mit der Streaming-Erfassung von Amazon Managed Streaming für Apache Kafka.

Für die Verwendung der API-Operationen zur Datenfreigabe erforderliche Berechtigungen

Um den Zugriff auf die API-Operationen für die Datenfreigabe zu steuern, verwenden Sie aktionsbasierte IAM-Richtlinien. Weitere Informationen zum Verwalten von IAM-Richtlinien finden Sie unter Managing IAM policies (Verwalten von IAM-Richtlinien) im IAM-Benutzerhandbuch.

Man denke an den Fall, dass ein Administrator eines Produzenten-Clusters den Aufruf `AuthorizeDataShare` verwenden muss, um die Ausgabe eines Datashares außerhalb eines AWS-Konto zu autorisieren. In diesem Fall richten Sie eine IAM-aktionsbasierte Richtlinie ein, um diese Berechtigung zu erteilen. Verwenden Sie den `DeauthorizeDataShare`-Aufruf, um die Ausgabe aufzuheben.

Wenn Sie aktionsbasierte IAM-Richtlinien verwenden, können Sie auch eine IAM-Ressource in der Richtlinie angeben, z. B. `DataShareARN`. Nachfolgend sehen Sie das Format und ein Beispiel für `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
```

Sie können `AuthorizeDataShare`-Zugriff auf einen bestimmten Datasharedurch Angabe des Datashare-Namens in der IAM-Richtlinie beschränken.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
```

```
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/SalesShare"
      ],
      "Effect": "Deny"
    }
  ]
}
```

Sie können die IAM-Richtlinie auch auf alle Datashares beschränken, die einem bestimmten Produzenten-Cluster gehören. Dazu ersetzen Sie den **`datashare-name`**-Wert in der Richtlinie mit einem Platzhalter oder einem Sternchen. Behalten Sie den Cluster-Wert `namespace-guid` bei.

```
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/
*
```

Es folgt eine IAM-Richtlinie, die verhindert, dass eine Entität in Datashares von einem bestimmten Produzenten-Cluster `AuthorizeDataShare` aufruft.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

`DataShareARN` beschränkt den Zugriff auf Grundlage des Datashare-Namens sowie der Globally Unique ID (GUID) für den Namespace des besitzenden Clusters. Dies geschieht, indem der Name als Sternchen angegeben wird.

Ressourcenrichtlinien für GetClusterCredentials

Zum Herstellen einer Verbindung mit einer Cluster-Datenbank mithilfe einer JDBC- oder ODBC-Verbindung und IAM-Datenbankanmeldeinformationen sowie zum programmgesteuerten

Aufrufen der Aktion `GetClusterCredentials` benötigen Sie einen Mindestsatz an Berechtigungen. Sie benötigen mindestens die Berechtigung zum Aufrufen der Aktion `redshift:GetClusterCredentials` mit Zugriff auf eine `dbuser`-Ressource.

Wenn Sie eine JDBC- oder ODBC-Verbindung verwenden, können Sie anstatt `server` und `port` die Optionen `cluster_id` und `region` angeben. Dazu benötigen Sie allerdings die Berechtigung zum Aufruf der Aktion `redshift:DescribeClusters` mit Zugriff auf die Ressource `cluster`.

Wenn Sie die Aktion `GetClusterCredentials` mit den optionalen Parametern `Autocreate`, `DbGroups` und `DbName` aufrufen, müssen Sie außerdem die in der folgenden Tabelle aufgeführten Aktionen und den Zugriff auf die dort aufgeführten Ressourcen erlauben.

GetClusterCredentials Parameter	Aktion	Ressource
`Autocreate`	`redshift:CreateClusterUser`	`dbuser`
`DbGroups`	`redshift:JoinGroup`	`dbgroup`
`DbName`	N/A	`dbname`

Weitere Informationen zu Ressourcen finden Sie unter Amazon-Redshift-Ressourcen und -Operationen.

Sie können auch die folgenden Bedingungen in Ihrer Richtlinie verwenden:

- `redshift:DurationSeconds`
- `redshift:DbName`
- `redshift:DbUser`

Weitere Informationen über Bedingungen finden Sie unter Angeben von Bedingungen in einer Richtlinie.

Beispiele für vom Kunden verwaltete Richtlinien

In diesem Abschnitt finden Sie Beispiele für Benutzerrichtlinien, die Berechtigungen für verschiedene Amazon-Redshift-Aktionen gewähren. Diese Richtlinien funktionieren, wenn Sie die Amazon Redshift Redshift-API, AWS SDKs oder die verwenden. AWS CLI

> **Note**
>
> In allen Beispielen werden die Region USA West (Oregon) (`us-west-2`) und fiktive Konto-IDs verwendet.

Beispiel 1: Benutzer vollen Zugriff auf alle Amazon-Redshift-Aktionen und -Ressourcen gewähren

Die folgende Richtlinie gewährt Zugriff auf alle Amazon-Redshift-Aktionen für alle Ressourcen.

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

Der Wert `redshift:*` im Element `Action` bezeichnet alle Aktionen in Amazon Redshift.

Beispiel 2: Benutzer Zugriff auf Satz von Amazon-Redshift-Aktionen verweigern

Standardmäßig werden alle Berechtigungen verweigert. Manchmal müssen Sie jedoch den Zugriff auf eine bestimmte Aktion oder einen Satz von Aktionen ausdrücklich verweigern. Die folgende Richtlinie gewährt Zugriff auf alle Amazon-Redshift-Aktionen und verweigert ausdrücklich den Zugriff auf jede Amazon-Redshift-Aktion, deren Name mit beginnt `Delete`. Diese Richtlinie gilt für alle Amazon-Redshift-Ressourcen in `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:*"
   }
  ]
}
```

Beispiel 3: Einem Benutzer die Verwaltung von Clustern gestatten

Die folgende Richtlinie erlaubt einem Benutzer, alle Cluster zu erstellen, zu löschen, zu modifizieren und neu zu starten, und verweigert die Erlaubnis, alle Cluster zu löschen oder zu modifizieren, bei denen der Clustername mit beginnt `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"
    }
  ]
}
```

Beispiel 4: Einem Benutzer die Autorisierung und den Widerruf des Zugriffs auf Snapshots erlauben

Die folgende Richtlinie erlaubt einem Benutzer, etwa Benutzer A, Folgendes zu tun:

- Autorisieren des Zugriffs zu allen von einem Cluster mit der Bezeichnung erstellten Snapshots `shared`.
- Widerrufen des Snapshot-Zugriffs für alle vom Cluster `shared` erstellten Snapshots, bei denen der Snapshot-Name mit `revokable` beginnt.

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

Wenn Benutzer A Benutzer B den Zugriff auf einen Snapshot gestattet hat, muss Benutzer B über eine Richtlinie wie die folgende verfügen, damit Benutzer B einen Cluster aus dem Snapshot wiederherstellen kann. Die folgende Richtlinie gestattet Benutzer B die Beschreibung und Wiederherstellung von Snapshots sowie die Erstellung von Clusters. Die Namen dieser Cluster müssen mit beginnen `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"
    }
  ]
}
```

Beispiel 5: Einem Benutzer gestatten, einen Cluster-Snapshot zu kopieren und einen Cluster von einem Snapshot wiederherzustellen

Die folgende Richtlinie erlaubt einem Benutzer, alle von einem Cluster mit der Bezeichnung `big-cluster-1` erstellten Snapshots zu kopieren und alle Snapshots wiederherzustellen, deren Name mit `snapshot-for-restore` beginnt.

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

Beispiel 6: Benutzer Zugriff auf Amazon Redshift und gängige Aktionen und Ressourcen für verwandte AWS -Services gewähren

Die folgende Beispielrichtlinie ermöglicht den Zugriff auf alle Aktionen und Ressourcen für Amazon Redshift, Amazon Simple Notification Service (Amazon SNS) und Amazon. CloudWatch Sie erlaubt darüber hinaus bestimmte Aktionen für alle verwandten Amazon-EC2-Ressourcen im Konto.

> **Note**
>
> Berechtigungen auf Ressourcenebene werden für die in dieser Beispielrichtlinie angegebenen Amazon-EC2-Aktionen nicht unterstützt.

```
{
  "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": [
        "*"
      ]
    }
  ]
}
```

Beispiel 7: Benutzer erlauben, mit der Amazon-Redshift-Konsole Ressourcen zu markieren

Mit der folgenden Beispielrichtlinie kann ein Benutzer Ressourcen mit der Amazon-Redshift-Konsole über die AWS Resource Groups markieren. Diese Richtlinie kann einer Benutzerrolle zugewiesen werden, die die neue oder ursprüngliche Amazon-Redshift-Konsole aufruft. Weitere Informationen über das Markieren mit Tags finden Sie unter Markieren von Ressourcen in Amazon Redshift.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Tagging permissions",
            "Effect": "Allow",
            "Action": [
                "redshift:DeleteTags",
                "redshift:CreateTags",
                "redshift:DescribeTags",
                "tag:UntagResources",
                "tag:TagResources"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Beispielrichtlinie für die Verwendung GetClusterCredentials

Die folgende Richtlinie verwendet diese Beispielparameterwerte:

- Region: `us-west-2`
- AWS Konto: `123456789012`
- Cluster name: `examplecluster`

Die folgende Richtlinie aktiviert die Aktionen `GetCredentials`, `CreateClusterUser` und `JoinGroup`. Die Richtlinie verwendet Bedingungsschlüssel, um die `CreateClusterUser` Aktionen `GetClusterCredentials` und nur dann zuzulassen, wenn die AWS Benutzer-ID übereinstimmt`"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"`. IAM-Zugriff ist nur für die `"testdb"`-Datenbank erforderlich. Die Richtlinie erlaubt Benutzern auch, einer Gruppe namens `"common_group"` beizutreten.

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

Nativer Identitätsanbieter(IdP)-Verbund für Amazon Redshift

Die Verwaltung von Identitäten und Berechtigungen für Amazon Redshift wird durch den nativen Identitätsanbieter-Verbund erleichtert, da dieser Ihren bestehenden Identitätsanbieter nutzt und damit die Authentifizierung und Verwaltung von Berechtigungen vereinfacht. Zu diesem Zweck besteht die Möglichkeit, Identitätsmetadaten von Ihrem Identitätsanbieter an Redshift freizugeben. Für die erste Iteration dieser Funktion wird der Identitätsanbieter Microsoft Azure Active Directory (Azure AD) unterstützt.

Um Amazon Redshift so zu konfigurieren, dass es Identitäten von dem externen Identitätsanbieter authentifizieren kann, registrieren Sie den Identitätsanbieter bei Amazon Redshift. Auf diese Weise ist Redshift in der Lage, Benutzer und Rollen zu authentifizieren, die von dem Identitätsanbieter definiert wurden. Da Identitätsinformationen gemeinsam genutzt werden, ist es somit nicht notwendig, dass Sie sowohl bei Ihrem externen Identitätsanbieter als auch in Amazon Redshift ein differenziertes Identitätsmanagement durchführen.

Informationen zur Verwendung von Sitzungsrollen, die von Identitätsanbieter-Gruppen übertragen werden, finden Sie unter PG_GET_SESSION_ROLES im Datenbankentwicklerhandbuch zu Amazon Redshift.

Einrichten des Identitätsanbieters in Amazon Redshift

In diesem Abschnitt werden die Schritte zur Konfiguration des Identitätsanbieters sowie von Amazon Redshift beschrieben, um die Kommunikation für den nativen Identitätsanbieter-Verbund herzustellen. Sie benötigen ein aktives Konto bei Ihrem Identitätsanbieter. Vor der Konfiguration von Amazon Redshift registrieren Sie Redshift als Anwendung bei Ihrem Identitätsanbieter und erteilen dabei Administratoreinwilligung.

Führen Sie die folgenden Schritte in Amazon Redshift aus:

1. Führen Sie eine SQL-Anweisung zum Registrieren des Identitätsanbieters, einschließlich Beschreibungen der Metadaten der Azure-Anwendung, aus. Um den Identitätsanbieter in Amazon Redshift zu erstellen, führen Sie den folgenden Befehl aus, nachdem Sie die Werte für die Parameter issuer (Aussteller), client_id (Client-ID), client_secret (Client-Schlüssel) und audience (Zielgruppe) ersetzt haben. Diese Parameter sind für Microsoft Azure AD spezifisch. Ersetzen Sie den Namen des Identitätsanbieters durch einen Namen Ihrer Wahl und ersetzen Sie den Namespace durch einen eindeutigen Namen für einen Namespace, der Benutzer und Rollen aus Ihrem Identitätsanbieter-Verzeichnis enthalten soll.

   ```
   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"]
   }'
   ```

   Der Typ `azure` zeigt an, dass der Anbieter speziell die Kommunikation mit Microsoft Azure AD ermöglicht. Azure ist derzeit der einzige unterstützte externe Identitätsanbieter.

   - issuer (Aussteller) – Die Aussteller-ID, der beim Empfang eines Tokens vertraut werden soll. Die eindeutige Kennung für die tenant_id (Mandanten-ID) wird an den Aussteller angehängt.
   - client_id (Client–ID) – Die eindeutige, öffentliche Kennung der bei dem Identitätsanbieter registrierten Anwendung. Diese kann als Anwendungs-ID bezeichnet werden.

- client_secret (Client–Schlüssel) – Eine geheime Kennung oder ein Passwort, das nur dem Identitätsanbieter und der registrierten Anwendung bekannt ist.
- audience (Zielgruppe) – Die Anwendungs-ID, die der Anwendung in Azure zugewiesen ist.

Anstatt ein gemeinsames Clientgeheimnis zu verwenden, können Sie beim Erstellen des Identitätsanbieters Parameter festlegen, um ein Zertifikat, einen privaten Schlüssel und ein Passwort für den privaten Schlüssel anzugeben.

```
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"}';
```

Das Passwort des privaten Schlüssels client_pk_password ist optional.

2. Optional: Führen Sie SQL-Befehle in Amazon Redshift aus, um Benutzer und Rollen vorab zu erstellen. Auf diese Weise ist es leichter möglich, Berechtigungen im Voraus zu erteilen. Der Rollenname in Amazon Redshift lautet wie folgt:: **<** GroupName auf Azure AD**><**Namespace**>**. Wenn Sie beispielsweise eine Gruppe in Microsoft Azure AD mit dem Namen `rsgroup` und einen Namespace namens `aad` erstellen, lautet der Rollenname `aad:rsgroup`. Der Benutzername und die Rollennamen in Amazon Redshift werden anhand dieser Benutzernamen und Gruppenmitgliedschaften im Namespace des Identitätsanbieters zugeordnet.

   Die Zuordnung für Rollen und Benutzer umfasst die Überprüfung ihres `external_id`-Werts, um sicherzustellen, dass er auf dem neuesten Stand ist. Die externe ID entspricht der Kennung der Gruppe oder des Benutzers im Identitätsanbieter. Beispielsweise wird die externe ID einer Rolle der entsprechenden Azure-AD-Gruppen-ID zugeordnet. In ähnlicher Weise wird die externe ID jedes Benutzers seiner ID im Identitätsanbieter zugeordnet.

   ```
   create role "aad:rsgroup";
   ```

3. Gewähren Sie Ihren Anforderungen entsprechend relevante Berechtigungen für die Rollen. Zum Beispiel:

```
GRANT SELECT on all tables in schema public to role "aad:rsgroup";
```

4. Sie können auch einem bestimmten Benutzer Berechtigungen erteilen.

```
GRANT SELECT on table foo to aad:alice@example.com
```

Beachten Sie, dass die Rollenmitgliedschaft eines externen Verbundbenutzers nur in der Sitzung dieses Benutzers verfügbar ist. Dies hat Auswirkungen auf die Erstellung von Datenbankobjekten. Wenn ein externer Verbundbenutzer beispielsweise eine Ansicht oder gespeicherte Prozedur erstellt, kann derselbe Benutzer die Berechtigung für diese Objekte nicht an andere Benutzer und Rollen delegieren.

Erläuterung zu Namespaces

Ein Namespace ordnet einen Benutzer oder eine Rolle einem bestimmten Identitätsanbieter zu. Das Präfix für in AWS IAM erstellte Benutzer lautet beispielsweise. `iam:` Dieses Präfix verhindert Kollisionen von Benutzernamen und ermöglicht die Unterstützung mehrerer Identitätsspeicher. Wenn sich ein Benutzer alice@example.com von der mit dem Namespace aad registrierten Identitätsquelle aus anmeldet, wird der Benutzer `aad:alice@example.com` in Redshift erstellt, sofern dieser noch nicht vorhanden ist. Beachten Sie, dass ein Namespace für Benutzer und Rollen eine andere Funktion als ein Namespace für Cluster in Amazon Redshift hat. Bei letzterem handelt es sich um eine eindeutige Kennung, die einem Cluster zugeordnet ist.

So funktioniert die Anmeldung bei Verwendung des nativen Identitätsanbieter(IdP)-Verbunds

Um die vorläufige Einrichtung des Identitätsanbieters sowie von Amazon Redshift abzuschließen, führen Sie einige Schritte aus: Zuerst registrieren Sie Amazon Redshift als Drittanwendung bei Ihrem Identitätsanbieter und fordern die erforderlichen API-Berechtigungen an. Dann erstellen Sie Benutzer und Gruppen im Identitätsanbieter. Zuletzt registrieren Sie den Identitätsanbieter bei Amazon Redshift unter Verwendung von SQL-Anweisungen, die für den Identitätsanbieter eindeutige Authentifizierungsparameter festlegen. Im Rahmen der Registrierung des Identitätsanbieters bei Redshift weisen Sie einen Namespace zu, um sicherzustellen, dass Benutzer und Rollen korrekt gruppiert werden.

Wenn der Identitätsanbieter bei Amazon Redshift registriert ist, ist die Kommunikation zwischen Redshift und dem Identitätsanbieter eingerichtet. Ein Client kann nun Token übergeben und sich bei

Redshift als Identitätsanbieter-Entität authentifizieren. Amazon Redshift verwendet die Informationen zur IdP-Gruppenmitgliedschaft, um Redshift-Rollen zuzuordnen. Wenn der Benutzer zuvor noch nicht in Redshift vorhanden ist, wird er erstellt. Es werden Rollen erstellt, die Identitätsanbietergruppen zugeordnet werden, wenn sie noch nicht vorhanden sind. Der Amazon-Redshift-Administrator erteilt die Berechtigung für die Rollen, und Benutzer können Abfragen und andere Datenbankaufgaben ausführen.

Die folgenden Schritte beschreiben die Funktionsweise des nativen Identitätsanbieter-Verbunds bei Anmeldung eines Benutzers:

1. Wenn sich ein Benutzer unter Verwendung der nativen IdP-Option vom Client aus anmeldet, wird das Identitätsanbieter-Token vom Client an den Treiber gesendet.
2. Der Benutzer wird authentifiziert. Falls der Benutzer noch nicht in Amazon Redshift vorhanden ist, wird ein neuer Benutzer erstellt. Redshift ordnet die Identitätsanbietergruppen des Benutzers Redshift-Rollen zu.
3. Berechtigungen werden basierend auf den Redshift-Rollen des Benutzers zugewiesen. Diese werden Benutzern und Rollen von einem Administrator gewährt.
4. Der Benutzer kann Redshift abfragen.

Verwenden von Desktop-Client-Tools zum Herstellen einer Verbindung zu Amazon Redshift

Anweisungen zur Verwendung des nativen Identitätsanbieter-Verbunds, um eine Verbindung zu Amazon Redshift mit Power BI herzustellen, finden Sie in dem Blogbeitrag Integrate Amazon Redshift native IdP federation with Microsoft Azure Active Directory (AD) and Power BI. Es beschreibt eine step-by-step Implementierung des nativen IdP-Setups von Amazon Redshift mit Azure AD. Die Schritte zum Einrichten der Client-Verbindung für Power BI Desktop oder den Power-BI-Service werden erläutert. Die Schritte umfassen die Anwendungsregistrierung, das Konfigurieren von Berechtigungen und die Konfiguration von Anmeldeinformationen.

Sehen Sie sich das folgende Video an, um zu erfahren, wie Sie den nativen IDP-Verbund von Amazon Redshift in Azure AD integrieren können, indem Sie Power BI Desktop und JDBC Client-SQL Workbench/J verwenden:

Anweisungen zur Verwendung des nativen Identitätsanbieter-Verbunds, um eine Verbindung zu Amazon Redshift mit einem SQL-Client, insbesondere DBeaver oder SQL Workbench/J, herzustellen,

finden Sie im Blogbeitrag Integrate Amazon Redshift native IdP federation with Microsoft Azure AD using a SQL client.

Connect Redshift mit IAM Identity Center, um Benutzern eine Single-Sign-On-Erfahrung zu bieten

Sie können den Benutzer- und Gruppenzugriff auf Amazon-Redshift-Data-Warehouses über die Verbreitung vertrauenswürdiger Identitäten verwalten. Dies funktioniert über eine Verbindung zwischen Redshift und AWS IAM Identity Center, die Ihren Benutzern ein Single-Sign-On-Erlebnis bietet. Auf diese Weise können Sie Benutzer und Gruppen aus Ihrem Verzeichnis integrieren und diesen direkt Berechtigungen zuweisen. Anschließend unterstützt diese Verbindung die Integration zusätzlicher Tools und Services. Um einen end-to-end Fall zu veranschaulichen, können Sie ein Amazon QuickSight Dashboard oder den Amazon Redshift Query Editor v2 verwenden, um auf Redshift zuzugreifen. Der Zugriff basiert in diesem Fall auf IAM-Identity-Center-Gruppen. Redshift kann die Identität und die Gruppenmitgliedschaften eines Benutzers feststellen. IAM Identity Center ermöglicht es auch, Identitäten über einen externen Identitätsanbieter (IdP) wie Okta oder zu verwalten. PingOne

Nachdem der Einrichtung der Verbindung zwischen Redshift und IAM Identity Center durch Ihren Administrator kann dieser einen differenzierten Zugriff auf der Grundlage von Identitätsanbietergruppen konfigurieren, um den Benutzerzugriff auf Daten zu autorisieren.

Die Vorteile der Redshift-Integration mit AWS IAM Identity Center

Die Verwendung von IAM Identity Center mit Redshift kann Ihrer Organisation die folgenden Vorteile bieten:

- Dashboard-Autoren Amazon QuickSight können eine Verbindung zu Redshift-Datenquellen herstellen, ohne Passwörter erneut eingeben zu müssen oder dass ein Administrator IAM-Rollen mit komplexen Berechtigungen einrichten muss.
- Das IAM Identity Center stellt Ihren Benutzern einen zentralen Ort in AWS bereit. Sie können Benutzer und Gruppen direkt in IAM Identity Center erstellen oder bestehende Benutzer und Gruppen verbinden, die Sie in einem standardbasierten Identitätsanbieter wie Okta oder Microsoft Entra PingOne ID (Azure AD) verwalten. IAM Identity Center leitet die Authentifizierung für Benutzer und Gruppen an die von Ihnen ausgewählte Informationsquelle weiter und verwaltet ein Verzeichnis mit Benutzern und Gruppen, auf das Redshift zugreifen kann. Weitere Informationen finden Sie unter Identitätsquelle ändern und Unterstützte Identitätsanbieter im AWS -IAM-Identity-Center-Benutzerhandbuch.

- Sie können eine einzelne IAM-Identity-Center-Instance mit mehreren Redshift-Clustern und -Arbeitsgruppen über eine einfache Funktion für automatische Erkennung und Verbindung teilen. So können Cluster schnell hinzugefügt werden, ohne dass die IAM-Identity-Center-Verbindung für jeden einzelnen Cluster zusätzlich konfiguriert werden muss. Außerdem stellt dies sicher, dass die Ansicht für Benutzer, Benutzerattribute und Gruppen über alle Cluster und Arbeitsgruppen hinweg konsistent ist. Beachten Sie, dass sich die IAM-Identity-Center-Instance Ihrer Organisation in derselben Region befinden muss wie die Redshift-Datashares, zu denen Sie eine Verbindung herstellen.
- Da die Benutzeridentitäten bekannt sind und zusammen mit dem Datenzugriff protokolliert werden, können Sie Compliance-Vorschriften einfacher erfüllen, indem Sie den Benutzerzugriff in AWS CloudTrail prüfen.

Einrichten der IAM-Identity-Center-Integration mit Amazon Redshift

Der Administrator Ihres Amazon-Redshift-Clusters oder Ihr Amazon-Redshift-Serverless-Administrator muss verschiedene Schritte ausführen, um Redshift für IAM Identity Center zu konfigurieren. Auf diese Weise kann Redshift das IAM Identity Center automatisch erkennen und Verbindung zu ihm herstellen, um Anmelde- und Benutzerverzeichnisservices zu nutzen. Anschließend kann Ihr Redshift-Administrator während der Erstellung eines Clusters oder einer Arbeitsgruppe das neue Data Warehouse so einrichten, dass es IAM Identity Center zur Verwaltung des Datenbankzugriffs verwendet.

Wenn Sie Redshift als von IAM Identity Center verwaltete Anwendung konfigurieren, können Sie Benutzer- und Gruppenberechtigungen über IAM Identity Center oder einen externen Identitätsanbieter steuern, der mit dem System integriert ist. Wenn sich Ihre Datenbankbenutzer bei einer Redshift-Datenbank anmelden, z. B. Analysten oder Datenwissenschaftler, werden ihre Gruppen in IAM Identity Center überprüft und ob sie mit den Rollennamen in Redshift übereinstimmen. So kann eine Gruppe, die den Namen für eine Redshift-Datenbankrolle definiert, auf Tabellen zugreifen, beispielsweise für Vertriebsanalysen. In den folgenden Abschnitten wird gezeigt, wie dies eingerichtet wird.

Voraussetzungen

Dies sind die Voraussetzungen für die Integration von IAM Identity Center mit Amazon Redshift:

- Kontokonfiguration — Sie müssen IAM Identity Center im Verwaltungskonto Ihrer AWS Organisation konfigurieren, wenn Sie kontoübergreifende Anwendungsfälle planen oder wenn Sie Redshift-Cluster in verschiedenen Konten mit derselben IAM Identity Center-Instanz verwenden.

Dies umfasst auch die Konfiguration Ihrer Identitätsquelle. Weitere Informationen finden Sie unter Erste Schritte, Mitarbeiteridentitäten und Unterstützte Identitätsanbieter im AWS -IAM-Identity-Center-Benutzerhandbuch. Sie müssen Benutzer oder Gruppen in IAM Identity Center erstellt haben oder Benutzer und Gruppen aus Ihrer Identitätsquelle synchronisiert haben, bevor Sie diese zu Daten in Redshift zuweisen können.

> **Note**
>
> Sie haben die Möglichkeit, eine Kontoinstanz von IAM Identity Center zu verwenden, vorausgesetzt, Redshift und IAM Identity Center befinden sich in demselben Konto. Sie können diese Instance mitttels eines Widgets erstellen, wenn Sie einen Redshift-Cluster oder eine Redshift-Arbeitsgruppe erstellen und konfigurieren.

- Konfigurieren eines vertrauenswürdigen Token-Ausstellers – In einigen Fällen müssen Sie möglicherweise einen vertrauenswürdigen Token-Aussteller verwenden. Dies ist eine Entität, die vertrauenswürdige Token ausstellen und verifizieren kann. Bevor der Redshift-Administrator, der die IAM-Identity-Center-Integration konfiguriert, den vertrauenswürdigen Token-Aussteller auswählen und zum Abschluss der Konfiguration die erforderlichen Attribute hinzufügen kann, müssen einige Schritte zur Vorbereitung ausgeführt werden. Dies kann bedeuten, einen externen Identitätsanbieter als vertrauenswürdigen Token-Aussteller zu konfigurieren und dessen Attribute in der IAM-Identity-Center-Konsole hinzuzufügen. Informationen zu diesen Schritten finden Sie unter Einrichten eines vertrauenswürdigen Token-Ausstellers.

  > **Note**
  >
  > Die Einrichtung eines vertrauenswürdigen Token-Ausstellers ist nicht für alle externen Verbindungen erforderlich. Für die Verbindung mit Ihrer Redshift-Datenbank mit dem Amazon Redshift Query Editor v2 ist keine Konfiguration des vertrauenswürdigen Token-Ausstellers erforderlich. Dies kann jedoch für Anwendungen von Drittanbietern wie Dashboards oder benutzerdefinierte Anwendungen gelten, die sich bei Ihrem Identitätsanbieter authentifizieren.

- Konfigurieren einer oder mehrerer IAM-Rollen – In den folgenden Abschnitten werden Berechtigungen genannt, die konfiguriert werden müssen. Sie müssen Berechtigungen gemäß bewährten IAM-Methoden hinzufügen. Die spezifischen Berechtigungen werden in den folgenden Verfahren beschrieben.

Weitere Informationen finden Sie unter Erste Schritte mit IAM Identity Center.

Konfigurieren Ihres Identitätsanbieters für IAM Identity Center

Der erste Schritt bei der Benutzer- und Gruppenidentitätsverwaltung besteht in der Herstellung einer Verbindung mit IAM Identity Center und der Konfiguration des Identitätsanbieters. Sie können IAM Identity Center als Identitätsanbieter verwenden oder eine Verbindung zum Identitätsspeicher eines Drittanbieters herstellen, z. B. Okta. Weitere Informationen zum Einrichten der Verbindung zum Identitätsanbieter und zu dessen Konfiguration finden Sie unter Verbinden mit einem externen Identitätsanbieter im IAM-Identity-Center-Benutzerhandbuch. Fügen Sie am Ende dieses Vorgangs zu Testzwecken eine kleine Sammlung von Benutzern und Gruppen zu IAM Identity Center hinzu.

Administrative Berechtigungen

Erforderliche Berechtigungen für das RedShift/IAM Identity Center-Anwendungslebenszyklusmanagement

Sie müssen eine IAM-Identität erstellen, die ein Redshift-Administrator verwendet, um Redshift für die Verwendung mit IAM Identity Center zu konfigurieren. In den meisten Fällen würden Sie eine IAM-Rolle mit Berechtigungen erstellen und sie nach Bedarf anderen Identitäten zuweisen. Sie muss über die aufgelisteten Berechtigungen verfügen, um die folgenden Aktionen ausführen zu können.

Die Redshift/IAM Identity Center-Anwendung erstellen

- `sso:PutApplicationAssignmentConfiguration` – Für die Security.
- `sso:CreateApplication` – Zur Erstellung einer IAM-Identity-Center-Anwendung verwendet.
- `sso:PutApplicationAuthenticationMethod` – Gewährt Redshift-Authentifizierungszugriff.
- `sso:PutApplicationGrant` – Zur Änderung der Informationen zu vertrauenswürdigen Token-Ausstellern verwendet.
- `sso:PutApplicationAccessScope` – Zum Einrichten der Redshift-IAM-Identity-Center-Anwendung. Dies gilt auch für AWS Lake Formation und für Amazon S3 Access Grants.
- `redshift:CreateRedshiftIdcApplication` – Zur Erstellung der Redshift-IDC-Anwendung verwendet.

Beschreibung der Redshift/IAM Identity Center-Anwendung

- `sso:GetApplicationGrant` – Zum Auflisten der Informationen zu vertrauenswürdigen Token-Ausstellern verwendet.

- `sso:ListApplicationAccessScopes`— Für die Einrichtung der Redshift IAM Identity Center-Anwendung zur Auflistung nachgelagerter Integrationen wie for AWS Lake Formation und S3 Access Grants.
- `redshift:DescribeRedshiftIdcApplications`— Wird verwendet, um bestehende IAM Identity Center-Anwendungen zu beschreiben.

Änderung der Redshift/IAM Identity Center-Anwendung

- `redshift:ModifyRedshiftIdcApplication` – Zur Änderung einer bestehenden Redshift-Anwendung verwendet.
- `sso:UpdateApplication` – Zur Aktualisierung einer IAM-Identity-Center-Anwendung verwendet.
- `sso:GetApplicationGrant`— Ruft die Informationen zum Emittenten des Trust-Tokens ab.
- `sso:ListApplicationAccessScopes` – Zum Einrichten der Redshift-IAM-Identity-Center-Anwendung.
- `sso:DeleteApplicationGrant` – Löscht die Informationen zum vertrauenswürdigen Token-Aussteller.
- `sso:PutApplicationGrant` – Zur Änderung der Informationen zu vertrauenswürdigen Token-Ausstellern verwendet.
- `sso:PutApplicationAccessScope` – Zum Einrichten der Redshift-IAM-Identity-Center-Anwendung. Dies gilt auch für AWS Lake Formation und für Amazon S3 Access Grants.
- `sso:DeleteApplicationAccessScope`— Zum Löschen des Redshift IAM Identity Center-Anwendungs-Setups. Dies gilt auch für AWS Lake Formation und für Amazon S3 Access Grants.

Löschen der RedShift/IAM Identity Center-Anwendung

- `sso:DeleteApplication` – Zum Löschen einer IAM-Identity-Center-Anwendung verwendet.
- `redshift:DeleteRedshiftIdcApplication` – Ermöglicht das Löschen einer bestehenden Redshift-IDC-Anwendung.

Erforderliche Berechtigungen für das RedShift/Query Editor v2-Anwendungslebenszyklusmanagement

Sie müssen eine IAM-Identität erstellen, die ein Redshift-Administrator verwendet, um Redshift für die Verwendung mit IAM Identity Center zu konfigurieren. In den meisten Fällen würden Sie eine IAM-

Rolle mit Berechtigungen erstellen und sie nach Bedarf anderen Identitäten zuweisen. Sie muss über die aufgelisteten Berechtigungen verfügen, um die folgenden Aktionen ausführen zu können.

Die Query-Editor-V2-Anwendung wird erstellt

- `redshift:CreateQev2IdcApplication`— Wird verwendet, um die QEV2-Anwendung zu erstellen.
- `sso:CreateApplication`— Ermöglicht die Erstellung einer IAM Identity Center-Anwendung.
- `sso:PutApplicationAuthenticationMethod` – Gewährt Redshift-Authentifizierungszugriff.
- `sso:PutApplicationGrant` – Zur Änderung der Informationen zu vertrauenswürdigen Token-Ausstellern verwendet.
- `sso:PutApplicationAccessScope` – Zum Einrichten der Redshift-IAM-Identity-Center-Anwendung. Dies umfasst auch den Query Editor v2.
- `sso:PutApplicationAssignmentConfiguration` – Für die Security.

Beschreiben Sie die Anwendung Query Editor v2

- `redshift:DescribeQev2IdcApplications`— Wird zur Beschreibung der IAM Identity Center QEV2-Anwendung verwendet.

Ändern Sie die Query Editor v2-Anwendung

- `redshift:ModifyQev2IdcApplication`— Wird verwendet, um die IAM Identity Center QEV2-Anwendung zu ändern.
- `sso:UpdateApplication`— Wird verwendet, um die IAM Identity Center QEV2-Anwendung zu ändern.

Löschen Sie die Query Editor v2-Anwendung

- `redshift:DeleteQev2IdcApplication`— Wird verwendet, um die QEV2-Anwendung zu löschen.
- `sso:DeleteApplication`— Wird verwendet, um die QEV2-Anwendung zu löschen.

> **Note**
>
> Im Amazon Redshift SDK sind die folgenden APIs nicht verfügbar:

- CreateQev2 IdcApplication
- DescribeQev2 IdcApplications
- ModifyQev2 IdcApplication
- DeleteQev2 IdcApplication

Diese Aktionen sind spezifisch für die Durchführung der IAM Identity Center-Integration mit Redshift QEV2 in der Konsole. AWS Weitere Informationen finden Sie unter Von Amazon Redshift definierte Aktionen.

Für den Datenbankadministrator sind Berechtigungen erforderlich, um neue Ressourcen in der Konsole zu verbinden

Diese Berechtigungen sind erforderlich, um neue bereitgestellte Cluster oder Amazon-Redshift-Serverless-Arbeitsgruppen während der Erstellung zu verbinden. Wenn Sie diese Berechtigungen besitzen, werden in der Konsole Optionen für die Verbindung mit der von IAM Identity Center verwalteten Anwendung für Redshift angezeigt.

- `redshift:DescribeRedshiftIdcApplications`
- `sso:ListApplicationAccessScopes`
- `sso:GetApplicationAccessScope`
- `sso:GetApplicationGrant`

Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Redshift als AWS verwaltete Anwendung mit IAM Identity Center einrichten

Bevor IAM Identity Center Identitäten für einen von Amazon Redshift bereitgestellten Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe verwalten kann, muss der Redshift-Administrator die folgenden Schritte ausführen, um Redshift zu einer von IAM Identity Center verwalteten Anwendung zu machen:

1. Wählen Sie im Konsolenmenü von Amazon Redshift oder Amazon Redshift Serverless die Option IAM-Identity-Center-Integration und dann Mit IAM Identity Center verbinden aus.

Anschließend werden Sie durch verschiedene Optionen geleitet, um die Eigenschaften für die IAM-Identity-Center-Integration auszuwählen.

2. Wählen Sie einen Anzeigenamen und einen eindeutigen Namen für die von Redshift IDC verwaltete Anwendung aus.
3. Geben Sie den Namespace für Ihre Organisation an. Dies ist in der Regel eine abgekürzte Version des Namens Ihrer Organisation. Er wird Ihren von IDC verwalteten Benutzern und Rollen in der Redshift-Datenbank als Präfix vorangestellt.
4. Wählen Sie die IAM-Rolle aus, die verwendet werden soll. Diese IAM-Rolle sollte von anderen Rollen getrennt sein, die für Redshift verwendet werden. Wir empfehlen, sie nicht für andere Zwecke zu verwenden. Die folgenden spezifischen Richtlinienberechtigungen sind erforderlich:

   - `sso:DescribeApplication` – Zur Erstellung eines Identitätsanbieters (IdP) im Katalog erforderlich.
   - `sso:DescribeInstance` – Zur manuellen Erstellung von IdP-Verbundrollen oder -Benutzern verwendet.
5. Konfigurieren Sie Client-Verbindungen und vertrauenswürdige Token-Aussteller.
   Die Konfiguration vertrauenswürdiger Token-Aussteller ermöglicht die Verbreitung vertrauenswürdiger Identitäten, indem eine Beziehung mit einem externen Identitätsanbieter eingerichtet wird. Die Verbreitung von Identitäten ermöglicht Benutzern beispielsweise, sich bei einer Anwendung anzumelden und auf bestimmte Daten in einer anderen Anwendung zuzugreifen. So können Benutzer Daten von unterschiedlichen Standorten einfacher sammeln. In diesem Schritt legen Sie in der Konsole Attribute für jeden vertrauenswürdigen Token-Aussteller fest. Zu den Attributen gehören der Name und der Zielgruppenanspruch (oder Aud-Claim), die Sie möglicherweise aus den Konfigurationsattributen des Tools oder Service abrufen müssen. Möglicherweise müssen Sie auch den Namen der Anwendung aus dem JSON Web Token (JWT) des Drittanbieter-Tools bereitstellen.

   > **Note**
   >
   > Der `aud claim`, der von den einzelnen Drittanbieter-Tools oder Services abgerufen werden muss, ist vom Token-Typ abhängig. Dabei kann es sich um ein von einem Identitätsanbieter ausgestelltes Zugriffstoken oder um einen anderen Typ handeln, z. B. ein ID-Token. Jeder Anbieter kann sich hier unterscheiden. Wenn Sie die Verbreitung vertrauenswürdiger Identitäten und die Integration mit Redshift implementieren, müssen

Sie den richtigen aud-Wert für den Token-Typ bereitstellen, den das Drittanbieter-Tool an AWS sendet. Lesen Sie die Empfehlungen Ihres Tools oder Serviceanbieters.

Ausführliche Informationen zur Verbreitung vertrauenswürdiger Identitäten finden Sie unter So funktioniert die Weitergabe vertrauenswürdiger Identitäten. Weitere Informationen finden Sie auch in der Beta-Dokumentation für IAM Identity Center, die dieser Dokumentation angefügt ist.

Nachdem der Redshift-Administrator die Schritte abgeschlossen und die Konfiguration gespeichert hat, werden die IAM-Identity-Center-Eigenschaften in der Redshift-Konsole angezeigt. Sie können auch die Systemansicht SVV_IDENTITY_PROVIDERS abfragen, um die Eigenschaften der Anwendung zu überprüfen. Zu diesen gehören auch der Anwendungsname und der Namespace. Sie verwenden den Namespace als Präfix für Redshift-Datenbankobjekte, die der Anwendung zugeordnet sind. Die Ausführung dieser Aufgaben macht Redshift zu einer Anwendung, die mit IAM Identity Center kompatibel ist. Die Eigenschaften in der Konsole umfassen auch den Integrationsstatus. Wenn die Integration abgeschlossen ist, wird Aktiviert angezeigt. Nach diesem Vorgang kann die IAM-Identity-Center-Integration für jeden neuen Cluster aktiviert werden.

Nach der Konfiguration können Sie Benutzer und Gruppen aus IAM Identity Center in Redshift integrieren, indem Sie die Registerkarten Benutzer oder Gruppen und dann Zuweisen auswählen.

Aktivieren der IAM-Identity-Center-Integration für einen neuen Amazon-Redshift-Cluster oder eine Amazon-Redshift-Serverless-Arbeitsgruppe

Ihr Datenbankadministrator richtet die Konfiguration neuer Redshift-Ressourcen auf IAM Identity Center aus, um Anmeldung und Datenzugriff zu vereinfachen. Dies erfolgt im Rahmen der Schritte zur Erstellung eines bereitgestellten Clusters oder einer Serverless-Arbeitsgruppe. Alle Benutzer, die zur Erstellung von Redshift-Ressourcen berechtigt sind, können diese IAM-Identity-Center-Integrationsaufgaben ausführen. Wenn Sie einen bereitgestellten Cluster erstellen, wählen Sie zunächst in der Amazon-Redshift-Konsole die Option Cluster erstellen aus. Die folgenden Schritte zeigen, wie Sie die IAM-Identity-Center-Verwaltung für eine Datenbank aktivieren. (Es werden nicht alle Schritte zum Erstellen eines Clusters beschrieben.)

1. Wählen Sie <your cluster name>im Abschnitt für die IAM Identity Center-Integration in den Schritten zum Erstellen eines Clusters die Option Aktivieren für aus.
2. Es gibt einen Schritt im Prozess, in dem Sie die Integration aktivieren. Hierzu wählen Sie in der Konsole IAM-Identity-Center-Integration aktivieren aus.

3. Erstellen Sie für den neuen Cluster oder die neue Arbeitsgruppe in Redshift Datenbankrollen mittels SQL-Befehlen aus. Dies ist der Befehl:

   ```
   CREATE ROLE <idcnamespace:rolename>;
   ```

   Der Namespace und der Rollenname sind:

   - IAM-Identity-Center-Namespace-Präfix – Dies ist der Namespace, den Sie beim Einrichten der Verbindung zwischen IAM Identity Center und Redshift definiert haben.
   - Rollenname – Diese Redshift-Datenbankrolle muss mit dem Gruppennamen in IAM Identity Center übereinstimmen.

   Redshift stellt eine Verbindung mit IAM Identity Center her und ruft die Informationen ab, die für die Erstellung und Zuordnung der Datenbankrolle zur IAM-Identity-Center-Gruppe erforderlich sind.

Beachten Sie, dass bei der Erstellung eines neuen Data Warehouse die für die IDC-Integration angegebene IAM-Rolle automatisch dem bereitgestellten Cluster oder der Amazon-Redshift-Serverless-Arbeitsgruppe zugewiesen wird. Nachdem Sie die erforderlichen Cluster-Metadaten eingegeben und die Ressource erstellt haben, können Sie den Status der IAM-Identity-Center-Integration in den Eigenschaften überprüfen. Wenn Ihre Gruppennamen in IAM Identity Center Leerzeichen enthalten, müssen Sie bei der Erstellung der entsprechenden Rolle in SQL Anführungszeichen verwenden.

Nachdem Sie die Redshift-Datenbank aktiviert und Rollen erstellt haben, können Sie mit dem Amazon Redshift Query Editor v2 oder Amazon QuickSight eine Verbindung zur Datenbank herstellen. Die Details werden in den folgenden Abschnitten beschrieben.

Einrichten der Standard-**`RedshiftIdcApplication`** über die API

Die Einrichtung wird von Ihrem Identitätsadministrator ausgeführt. Sie können über die API eine `RedshiftIdcApplication` erstellen, die die Redshift-Anwendung in IAM Identity Center darstellt.

1. Zunächst können Sie Benutzer erstellen und diese zu Gruppen in IAM Identity Center hinzufügen. Sie tun dies in der AWS Konsole für IAM Identity Center (IDC).
2. Rufen Sie `create-redshift-idc-application` auf, um eine IDC-Anwendung zu erstellen und sie mit der Redshift-Nutzung kompatibel zu machen. Sie erstellen die Anwendung, indem

Sie die erforderlichen Werte eingeben. Der Anzeigename ist der Name, der im IDC-Dashboard angezeigt werden soll. Der ARN der IAM-Rolle ist ein ARN, der Berechtigungen für IAM Identity Center besitzt und von Redshift übernommen werden kann.

```
aws redshift create-redshift-idc-application
--idc-instance-arn 'arn:aws:sso:::instance/ssoins-1234a01a1b12345d'
--identity-namespace 'MyIdcIdentityNamespace'
--idc-display-name 'TEST-NEW-APPLICATION'
--iam-role-arn 'arn:aws:redshift:us-east-1:012345678901:role/TestRedshiftRole'
--redshift-idc-application-name 'myredshiftidcapplication'
```

Das folgende Beispiel zeigt eine `RedshiftIdcApplication`-Beispielantwort, die vom Aufruf von `create-redshift-idc-application` zurückgegeben wurde.

```
"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": "AWSIDC",
                "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. Sie können `create-application-assignment` verwenden, um der verwalteten Anwendung in IAM Identity Center bestimmte Gruppen oder einzelne Benutzer zuzuweisen. Auf diese Weise können Sie Gruppen angeben, die über IAM Identity Center verwaltet werden sollen. Wenn der Datenbankadministrator Datenbankrollen in Redshift erstellt, werden die Gruppennamen in IAM Identity Center den Rollennamen in Redshift zugeordnet. Die Rollen steuern die Berechtigungen in der Datenbank. Weitere Informationen finden Sie unter Zuweisen von Benutzerzugriff zu Anwendungen in der IAM-Identity-Center-Konsole.

4. Nachdem Sie die Anwendung aktiviert haben, rufen Sie `create-cluster` auf und fügen den ARN der von Redshift verwalteten Anwendung aus IAM Identity Center hinzu. Hierdurch wird der Cluster mit der verwalteten Anwendung in IAM Identity Center verknüpft.

Zuordnen einer IAM-Identity-Center-Anwendung zu einem vorhandenen Cluster oder einer vorhandenen Arbeitsgruppe

Wenn Sie Cluster oder Arbeitsgruppen besitzen, die Sie für die IAM-Identity-Center-Integration aktivieren möchten, können Sie dies mittels eines SQL-Befehls ausführen. Führen Sie den folgenden Befehl aus, um die Integration zu aktivieren. Die Abfrage muss von einem Datenbankadministrator ausgeführt werden und die Verbindung zwischen Redshift und IAM Identity Center muss bereits eingerichtet sein. Wenn Sie diese ENABLE festgelegt haben, kann IAM Identity Center die Identitätsverwaltung für den Cluster oder die Arbeitsgruppe bereitstellen.

```
ALTER IDENTITY PROVIDER
<idp_name> | NAMESPACE <namespace> | IAM_ROLE default | 'arn:aws:iam::<AWS account-
id-1>:role/<role-name>' | [DISABLE | ENABLE]
```

Sie können einen vorhandenen Identitätsanbieter entfernen. Das folgende Beispiel zeigt, wie CASCADE Benutzer und Rollen löscht, die dem Identitätsanbieter angefügt sind.

```
DROP IDENTITY PROVIDER
<provider_name> [ CASCADE ]
```

Einrichten von Benutzerberechtigungen

Ein Administrator konfiguriert Berechtigungen für verschiedene Ressourcen basierend auf den Identitätsattributen und Gruppenmitgliedschaften der Benutzer innerhalb des Identitätsanbieters oder direkt in IAM Identity Center. Beispielsweise kann der Administrator des Identitätsanbieters einen Datenbankingenieur zu einer Gruppe hinzufügen, die dessen Rolle entspricht. Dieser Gruppenname ist einem Redshift-Datenbankrollennamen zugeordnet. Die Rolle ermöglicht den Zugriff auf bestimmte Tabellen oder Ansichten in Redshift oder schränkt den Zugriff auf diese ein.

Administrator-Personas für die Verbindung von Anwendungen

Die folgenden Personas sind für die Verbindung von Analyseanwendungen mit der von IAM Identity Center verwalteten Anwendung für Redshift wichtig:

- Anwendungsadministrator – Erstellt eine Anwendung und konfiguriert die Services, mit denen der Austausch von Identitätstoken möglich ist. Dieser Administrator gibt auch an, welche Benutzer oder Gruppen Zugriff auf die Anwendung haben.
- Datenadministrator – Konfiguriert den detaillierten Zugriff auf Daten. Benutzer und Gruppen in IAM Identity Center können bestimmten Berechtigungen zugeordnet werden.

Verbindung zu Amazon Redshift mit IAM Identity Center herstellen über Amazon QuickSight

Im Folgenden wird gezeigt, wie Amazon QuickSight zur Authentifizierung bei Redshift verwendet wird, wenn eine Verbindung mit dem IAM Identity Center besteht und der Zugriff über dieses verwaltet wird: Autorisieren von Verbindungen von Amazon QuickSight zu Amazon Redshift Redshift-Clustern. Diese Schritte gelten auch für Amazon Redshift Serverless.

Verbindung zu Amazon Redshift mit IAM Identity Center über Amazon Redshift Query Editor v2

Nach Abschluss der Schritte für die Einrichtung einer IAM-Identity-Center-Verbindung mit Redshift können Benutzer über ihre IAM-Identity-Center-basierte Identität mit Namespace-Präfix auf die Datenbank und die entsprechenden Objekte in der Datenbank zugreifen. Weitere Informationen zum Herstellen einer Verbindung zu Redshift-Datenbanken mit Query Editor v2 finden Sie unter Arbeiten mit Query Editor v2.

Daten abfragen über AWS Lake Formation

Das AWS Lake Formation macht es einfacher, Ihren Data Lake zentral zu verwalten und zu sichern und den Datenzugriff zu ermöglichen. Durch die Konfiguration der Identitätsverbreitung zu Lake Formation über IAM Identity Center und Redshift kann ein Administrator einen differenzierten Zugriff auf Data Lakes in Amazon S3 gewähren, basierend auf den Identitätsanbieter (IdP)-Gruppen der Organisation. Diese Gruppen werden über IAM Identity Center verwaltet. In diesem Abschnitt wird die Konfiguration einiger Anwendungsfälle gezeigt, d. h. Abfragen eines Data Lake und Abfragen einer Datenfreigabe. Diese zeigen, wie IAM Identity Center mit Redshift zur Herstellung von Verbindungen mit von Lake Formation verwalteten Ressourcen genutzt werden kann.

Verwenden einer IAM-Identity-Center- und Redshift-Verbindung zur Abfrage eines Data Lake

Diese Schritte zeigen einen Anwendungsfall, in dem Sie IAM Identity Center mit Redshift verwenden, um einen Data Lake abzufragen, der von Lake Formation verwaltet wird.

Voraussetzungen

Dieses Verfahren setzt einige Schritte voraus:

1. IAM Identity Center muss für die Unterstützung der Authentifizierungs- und Identitätsverwaltung mit Redshift eingerichtet sein. Sie können IAM Identity Center über die Konsole aktivieren und eine Identitätsanbieter (IdP)-Quelle auswählen. Anschließend können Sie einige IdP-Benutzer mit IAM Identity Center synchronsieren. Sie müssen außerdem eine Verbindung zwischen IAM Identity Center und Redshift einrichten. Führen Sie hierzu die zuvor in diesem Dokument beschriebenen Schritte aus.
2. Erstellen Sie einen neuen Amazon-Redshift-Cluster und aktivieren Sie die Identitätsverwaltung über IAM Identity Center in den Konfigurationsschritten.
3. Erstellen Sie eine verwaltete IAM-Identity-Center-Anwendung für Lake Formation und konfigurieren Sie diese. Dies erfolgt nach der Einrichtung der Verbindung zwischen IAM Identity Center und Redshift. Dies sind die Schritte:
   a. Verwenden Sie in der AWS CLI den Befehl `modify-redshift-idc-application`, um die Integration des Lake-Formation-Service mit der von IAM Identity Center verwalteten Anwendung für Redshift zu aktivieren. Dieser Aufruf enthält den Parameter `service-integrations`, der auf einen Zeichenfolgenwert für die Konfiguration festgelegt ist, der die Autorisierung für Lake Formation ermöglicht.
   b. Konfigurieren Sie Lake Formation mit dem Befehl `create-lake-formation-identity-center-configuration`. Hierdurch wird eine IAM-Identity-Center-Anwendung für Lake Formation erstellt, die im IAM-Identity-Center-Portal angezeigt wird. Der Administrator muss das `--cli-input-json` Argument festlegen, dessen Wert der Pfad zu einer JSON-Datei ist, die das Standardformat für alle AWS CLI-API-Aufrufe verwendet. Sie müssen Werte für Folgendes einfügen:
      - `CatalogId` – Lake-Formation-Katalog-ID.
      - `InstanceArn` – ARN-Wert der IAM-Identity-Center-Instance.

Nachdem der Administrator die erforderliche Konfiguration abgeschlossen hat, kann der Datenbankadministrator ein externes Schema für die Abfrage des Data Lake erstellen.

1. Der Administrator erstellt das externe Schema – Der Redshift-Datenbankadministrator stellt eine Verbindung zur Datenbank her und erstellt mithilfe der folgenden SQL-Anweisung ein externes Schema:

```
CREATE EXTERNAL SCHEMA if not exists my_external_schema from DATA CATALOG database
 'my_lf_integrated_db' catalog_id '12345678901234';
```

Beachten Sie, dass die Angabe einer IAM-Rolle in diesem Fall nicht erforderlich ist, da der Zugriff über IAM Identity Center verwaltet wird.

2. Der Administrator gewährt Berechtigungen – Der Administrator gewährt die Nutzung für eine IAM-Identity-Center-Gruppe, die Berechtigungen für Redshift-Ressourcen gewährt. Hierzu führen Sie eine SQL-Anweisung wie die folgende aus:

   ```
   GRANT USAGE ON SCHEMA "my_external_schema" to "IDCCO:sales";
   ```

   Anschließend erteilt der Administrator Lake Formation Formation-Berechtigungen für Objekte, basierend auf den Anforderungen der Organisation, mithilfe der AWS CLI:

   ```
   aws lakeformation grant-permissions ...
   ```

3. Benutzer führen Abfragen aus – An diesem Punkt kann sich beispielsweise ein IAM-Identity-Center-Benutzer, der Mitglied der Vertriebsgruppe ist, über den Query Editor v2 bei der Redshift-Datenbank anmelden. Anschließend können sie eine Abfrage ausführen, die auf eine Tabelle im externen Schema zugreift, wie im folgenden Beispiel gezeigt:

   ```
   SELECT * from my_external_schema.table1;
   ```

Verwenden einer IAM-Identity-Center- und Redshift-Verbindung zur Verbindung mit einem Datashare

Sie können über ein anderes Redshift-Data-Warehouse auf einen Datashare zugreifen, wenn der Zugriff über IAM Identity Center verwaltet wird. Hierzu führen Sie eine Abfrage aus, um eine externe Datenbank einzurichten. Bevor Sie diese Schritte ausführen, wird davon ausgegangen, dass Sie eine Verbindung zwischen Redshift und IAM Identity Center eingerichtet haben und dass Sie die AWS Lake Formation Anwendung erstellt haben, wie im vorherigen Verfahren beschrieben.

1. Erstellen der externen Datenbank – Der Administrator erstellt eine externe Datenbank für die Datenfreigabe und referenziert sie über ihren ARN. Dies ist ein Beispiel für die Vorgehensweise:

   ```
   CREATE DATABASE "redshift_external_db" FROM ARN 'arn:aws:glue:us-
   east-1:123456789012:database/redshift_external_db-iad' WITH NO DATA CATALOG SCHEMA;
   ```

In diesem Anwendungsfall, in dem Sie IAM Identity Center mit Redshift für die Identitätsverwaltung verwenden, ist die IAM-Rolle nicht enthalten.

2. Der Administrator richtet Berechtigungen ein – Nach der Erstellung einer Datenbank gewährt der Administrator einer IAM-Identity-Center-Gruppe die Nutzung. Hierdurch werden Berechtigungen für Redshift-Ressourcen gewährt:

```
GRANT USAGE ON DATABASE "my_external_db" to "IDCCO:sales";
```

Der Administrator erteilt Lake Formation mithilfe der AWS CLI auch Berechtigungen für Objekte:

```
aws lakeformation grant-permissions ...
```

3. Benutzer führen Abfragen aus – Ein Benutzer in der Vertriebsgruppe kann auf der Grundlage der zugewiesenen Berechtigungen eine Tabelle in der Datenbank abfragen:

```
select * from redshift_external_db.public.employees;
```

Weitere Informationen zur Gewährung von Berechtigungen für einen Data Lake und Datenfreigaben finden Sie unter Gewähren von Berechtigungen für Benutzer und Gruppen. Weitere Informationen zur Gewährung der Nutzung für ein Schema oder eine Datenbank finden Sie unter Gewährung.

Integration Ihrer Anwendung oder Ihres Tools mit OAuth über einen vertrauenswürdigen Token-Aussteller

Tool-Anbieter können Funktionen für die Verbindung zu Redshift über die IAM-Identity-Center-Verbindung hinzufügen.

Plug-In für die Verwendung von Redshift mit IAM Identity Center

Dieses Plug-In, das für die Authentifizierung mit IAM Identity Center verwendet wird, stellt zusätzliche Verbindungseigenschaften bereit, um die Authentifizierung zu unterstützen:

Name des Plug-Ins	Beschreibung	Wert
`IdpTokenAuthPlugin`	Ein Authentifizierungs-Plug-In, das ein IAM-Identity-Center (IDC)-Token oder	`com.amazon.redshift.plugin.IdpTokenAuthPlugin`

Name des Plug-Ins	Beschreibung	Wert
	ein OIDC-JWT von allen mit IDC verbundenen Web-Identitätsanbietern akzeptiert.	

Der entsprechende Plugin-Name für ODBC und Python lautet IdpTokenAuthPlugin. ODBC und Python verwenden nicht den vollständig qualifizierten Klassennamen für Plug-Ins. Nur JDBC verwendet diesen. Geben Sie in Ihrem Tool den Namenswert mittels der Eigenschaft `plugin_name` ein. In Python-basierten Tools wird diese Eigenschaft als `credentials_provider` bezeichnet.

Das Plug-In besitzt die folgenden Verbindungsoptionen:

- IDC_Region — Die AWS Region, in der sich die IAM Identity Center (IDC) -Instanz befindet.
- Identity_Namespace — Der Identitäts-Namespace, der bei der Authentifizierung mit dem verwendet werden soll. IdpTokenAuthPlugin Er hilft Redshift, zu bestimmen, welche IAM-Identity-Center-Instance verwendet werden soll.

Sie geben diese Werte in den Verbindungseigenschaften des Tools ein, das Sie entwickeln und für die Verbindung verwenden. Weitere Informationen zu JDBC-Optionen finden Sie unter Optionen für die JDBC-Treiberversion 2.1. Weitere Informationen zu ODBC-Optionen finden Sie unter Konfiguration der ODBC-Treiberoptionen.

Einschränkungen

Es gelten einige Einschränkungen:

- Die JDBC-, ODBC- und Python-basierte Tool-Authentifizierung über Redshift wird nicht unterstützt, wenn es mit IAM Identity Center verbunden ist. Hierzu müssen Sie den Treiber Ihres Tools anpassen. Er unterstützt nur Verbindungen von und mit dem Abfrage-Editor v2. Amazon QuickSight
- Die Sicherheits- und Datenschutzeinstellungen Ihres Internetbrowsers, insbesondere diejenigen, die sichere Cookie-Einstellungen steuern, wie z. B. die Total Cookie Protection-Funktion von Firefox, können dazu führen, dass Verbindungsversuche vom Abfrage-Editor v2 zu Ihrer Redshift-Datenbank blockiert werden. Um das Problem zu beheben, können Sie die URL der Konsolenseite des Query-Editors v2 zur Ausnahmeliste des Browsers für den Tracking-Schutz hinzufügen. Klicken Sie dazu in Firefox auf das Schild in der Adressleiste des Browsers und schalten Sie

den Schalter um, um den Tracking-Schutz für den Abfrage-Editor v2 auszuschalten. Wenn Sie in Chrome den Inkognito-Modus verwenden, klicken Sie auf das Augensymbol in der Adressleiste, um Drittanbieter-Cookies für den Abfrage-Editor v2 zuzulassen.

Verwenden serviceverknüpfter Rollen für Amazon Redshift

Amazon Redshift verwendet mit dem AWS Identity and Access Management (IAM)-Service verknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein spezieller Typ von IAM-Rolle, der direkt mit Amazon Redshift verknüpft ist. Serviceverknüpfte Rollen sind von Amazon Redshift vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen von AWS-Services im Namen Ihres Amazon-Redshift-Clusters benötigt.

Eine serviceverknüpfte Rolle macht die Einrichtung von Amazon Redshift einfacher, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Die Rolle ist mit Amazon-Redshift-Anwendungsfällen verknüpft und verfügt über vordefinierte Berechtigungen. Nur Amazon Redshift kann diese Rolle übernehmen und nur die serviceverknüpfte Rolle kann die vordefinierte Berechtigungsrichtlinie nutzen. Amazon Redshift erstellt eine serviceverknüpfte Rolle in Ihrem Konto, wenn Sie zum ersten Mal einen Cluster erstellen. Sie können die serviceverknüpfte Rolle erst löschen, nachdem Sie alle Amazon-Redshift-Cluster in Ihrem Konto gelöscht haben. Dies schützt Ihre Amazon Redshift-Ressourcen, da Sie nicht versehentlich die Berechtigungen für den Zugriff auf die Ressourcen entfernen können.

Amazon Redshift unterstützt die Verwendung serviceverknüpfter Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWSRegionen und Endpunkte.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Berechtigungen für serviceverknüpfte Rollen für Amazon Redshift

Amazon Redshift verwendet die serviceverknüpfte Rolle namens AWSServiceRoleForRedshift – Ermöglicht Amazon Redshift, -AWSServices in Ihrem Namen aufzurufen. Diese verwaltete Richtlinie ist mit der folgenden serviceverknüpften Rolle verbunden: `AmazonRedshiftServiceLinkedRolePolicy`. Aktualisierungen dieser Richtlinie finden Sie unter Von AWS verwaltete (vordefinierte) Richtlinien für Amazon Redshift.

Die AWSServiceRoleForRedshift serviceverknüpfte Rolle vertraut nur darauf**redshift.amazonaws.com**, die Rolle zu übernehmen.

Die Berechtigungsrichtlinie AWSServiceRoleForRedshift für serviceverknüpfte Rollen ermöglicht es Amazon Redshift, Folgendes für alle zugehörigen Ressourcen durchzuführen:

- `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`

Berechtigungen für Netzwerkressourcen

Die folgenden Berechtigungen ermöglichen Aktionen in Amazon EC2 zum Erstellen und Verwalten von Sicherheitsgruppenregeln. Diese Sicherheitsgruppen und Regeln sind speziell dem Amazon-

Redshift-Ressourcen-Tag `aws:RequestTag/Redshift` zugeordnet. Dies beschränkt den Geltungsbereich der Berechtigungen auf bestimmte Amazon-Redshift-Ressourcen.

- `ec2:CreateSecurityGroup`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`
- `ec2:ModifySecurityGroupRules`
- `ec2:DeleteSecurityGroup`

Aktionen für die Prüfungsprotokollierung

Aktionen mit dem Präfix `logs` hängen mit der Audit-Protokollierung und verwandten Funktionen zusammen, insbesondere der Erstellung und Verwaltung von Protokollgruppen und Protokollstreams.

- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogStreams`
- `logs:GetLogEvents`

Der folgende JSON-Code zeigt Aktionen und Ressourcenumfang für Amazon Redshift für die Audit-Protokollierung.

```
[
    {
        "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:*"
        ]
    }
]
```

Weitere Informationen zur Verwendung von serviceverknüpften Rollen und deren Zweck in AWS finden Sie unter Verwenden serviceverknüpfter Rollen. Weitere Informationen zu bestimmten Aktionen und anderen IAM-Ressourcen für Amazon Redshift finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Redshift.

Aktionen zur Verwaltung von Administratoranmeldeinformationen mit AWS Secrets Manager

Aktionen mit dem Präfix `secretsmanager` sind für die Verwendung von Amazon Redshift zur Verwaltung von Administratoranmeldeinformationen relevant. Mit diesen Aktionen kann Amazon Redshift Secrets, die Administratoranmeldeinformationen enthalten, über AWS Secrets Manager erstellen und verwalten.

Der folgende JSON-Code zeigt die Aktionen und den Ressourcenumfang für Amazon Redshift an, um Administratoranmeldeinformationen mit AWS Secrets Manager zu verwalten.

```
[
    {
        "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": "*"
    }
]
```

So erlauben Sie einer IAM-Entität das Erstellen von AWSServiceRoleForRedshift serviceverknüpften Rollen

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

So erlauben Sie einer IAM-Entität das Löschen von AWSServiceRoleForRedshift serviceverknüpften Rollen

Die folgende Berechtigungsanweisung zu den Berechtigungen für diese IAM-Entität hinzufügen:

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

Alternativ können Sie eine von AWS verwaltete Richtlinie verwenden, um vollständigen Zugriff auf Amazon Redshift zu gewähren.

Erstellen einer serviceverknüpften Rolle für Amazon Redshift

Sie müssen eine AWSServiceRoleForRedshift serviceverknüpfte Rolle nicht manuell erstellen. Amazon Redshift erstellt die serviceverknüpfte Rolle für Sie. Wenn die AWSServiceRoleForRedshift serviceverknüpfte Rolle aus Ihrem Konto gelöscht wurde, erstellt Amazon Redshift die Rolle, wenn Sie einen neuen Amazon-Redshift-Cluster starten.

> **Important**
>
> Wenn Sie den Amazon-Redshift-Service vor dem 18. September 2017 verwendet haben, als dieser serviceverknüpfte Rollen unterstützt, hat Amazon Redshift die AWSServiceRoleForRedshift Rolle in Ihrem Konto erstellt. Weitere Informationen finden Sie unter In meinem IAM-Konto wird eine neue Rolle angezeigt.

Bearbeiten einer serviceverknüpften Rolle für Amazon Redshift

Amazon Redshift erlaubt es Ihnen nicht, die AWSServiceRoleForRedshift serviceverknüpfte Rolle zu bearbeiten. Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten auf die Rolle verweisen könnten. Sie können jedoch die Beschreibung der Rolle mit der IAM-Konsole, der AWS Command Line Interface (AWS CLI) oder der IAM API bearbeiten. Weitere Informationen finden Sie unter Ändern einer Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon Redshift

Wenn Sie eine Funktion oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

Bevor Sie die serviceverknüpfte Rolle aus einem Konto löschen können, müssen Sie alle entsprechenden Cluster Ihres Kontos deaktivieren und aus Ihrem Konto löschen. Weitere Informationen finden Sie unter Schließen und Löschen von Clustern.

Sie können die IAM-Konsole, die AWS CLI oder die IAM-API verwenden, um eine serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Verwenden der IAM-Authentifizierung zur Erstellung von Anmeldeinformationen für Datenbankbenutzern

Sie können temporäre Datenbank-Anmeldeinformationen auf der Grundlage von Berechtigungen erstellen, die durch eine AWS Identity and Access Management (IAM)-Berechtigungsrichtlinie gewährt wurden, um den Zugriff Ihrer Benutzer auf die Amazon-Redshift-Datenbank zu verwalten.

Normalerweise melden sich Benutzer von Amazon-Redshift-Datenbanken mit einem Datenbankbenutzernamen und -passwort bei der Datenbank an. Sie müssen jedoch keine Benutzernamen und Passwörter in Ihrer Amazon-Redshift-Datenbank verwalten. Sie können Ihr System so konfigurieren, dass es Benutzern erlaubt, Benutzeranmeldeinformationen zu erstellen und sich auf Basis ihrer IAM-Anmeldeinformationen an der Datenbank anzumelden.

Weitere Informationen finden Sie unter Identitätsanbieter und Verbund im IAM-Benutzerhandbuch.

Themen

- Übersicht
- Erstellen temporärer IAM-Anmeldeinformationen
- Optionen für die Bereitstellung von IAM-Anmeldeinformationen

Übersicht

Amazon Redshift bietet den GetClusterCredentialsAPI-Vorgang zur Generierung temporärer Datenbank-Benutzeranmeldedaten. Sie können Ihren SQL-Client mit Amazon-Redshift-JDBC- oder -ODBC-Treibern konfigurieren, die den Aufruf des `GetClusterCredentials`-Vorgangs verwalten. Dies erreichen sie durch Abrufen der Benutzeranmeldeinformationen für die Datenbank und Herstellen einer Verbindung zwischen dem SQL-Client und der Amazon-Redshift-Datenbank. Sie können auch Ihre Datenbankanwendung dazu verwenden, programmgesteuert die Operation `GetClusterCredentials` aufzurufen, die Benutzeranmeldeinformationen für die Datenbank abzurufen und eine Verbindung mit der Datenbank herzustellen.

Wenn Sie Benutzeridentitäten bereits außerhalb verwalten AWS, können Sie einen Identity Provider (IdP) verwenden, der der Security Assertion Markup Language (SAML) 2.0 entspricht, um den Zugriff auf Amazon Redshift Redshift-Ressourcen zu verwalten. Sie konfigurieren einen Identitätsanbieter (IdP), um verbundenen Benutzern den Zugriff auf eine IAM-Rolle zu gewähren. Mit dieser IAM-Rolle können Sie temporäre Datenbank-Anmeldeinformationen erstellen und sich bei Amazon-Redshift-Datenbanken anmelden.

Ihr SQL-Client muss zum Aufruf der Operation `GetClusterCredentials` für Sie berechtigt sein. Sie verwalten diese Berechtigungen, indem Sie eine IAM-Rolle erstellen und eine IAM-Berechtigungsrichtlinie zuweisen, die den Zugriff auf die Operation `GetClusterCredentials` und zugehörige Aktionen gewährt bzw. einschränkt. Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Die Richtlinie gewährt auch Zugriff auf bestimmte Ressourcen, z. B. Cluster, Datenbanken, Datenbankbenutzernamen und Benutzergruppennamen von Amazon Redshift, bzw. schränkt diesen ein.

> **Note**
>
> Wir raten zur Verwendung der Amazon-Redshift-JDBC- oder -ODBC-Treiber zur Verwaltung des Aufrufs des `GetClusterCredentials`-Vorgangs und der Anmeldung bei der Datenbank. Der Einfachheit halber wird in diesem Themenabschnitt davon ausgegangen, dass Sie einen SQL-Client mit JDBC- oder ODBC-Treiber verwenden.
> Spezifische Details und Beispiele zur Verwendung der `GetClusterCredentials` Operation oder des parallel `get-cluster-credentials` CLI-Befehls finden Sie unter GetClusterCredentialsund get-cluster-credentials.

Um die Authentifizierung und Autorisierung zentral zu verwalten, unterstützt Amazon Redshift die Datenbankauthentifizierung mit IAM und ermöglicht so eine Benutzerauthentifizierung über Unternehmensverbund. Statt einen Benutzer zu erstellen, können Sie vorhandene Identitäten von AWS Directory Service, aus Ihrem Unternehmens-Benutzerverzeichnis oder von einem Web-Identitätsanbieter verwenden. Diese werden als Verbundbenutzer bezeichnet. AWS weist einem Verbundbenutzer eine Rolle zu, wenn der Zugriff über einen IdP angefordert wird.

Um einem Benutzer oder einer Clientanwendung in Ihrer Organisation Verbundzugriff zum Aufrufen von Amazon-Redshift-API-Vorgängen bereitzustellen, können Sie auch den JDBC- oder ODBC-Treiber mit SAML-2.0-Unterstützung verwenden, um die Authentifizierung vom Identitätsanbieter Ihrer Organisation anzufordern. In diesem Fall haben die Benutzer Ihrer Organisation keinen direkten Zugriff auf Amazon Redshift.

Erstellen temporärer IAM-Anmeldeinformationen

In diesem Abschnitt finden Sie Anleitungen zur Konfiguration Ihres Systems für die Erstellung temporärer IAM-basierter Benutzeranmeldeinformationen für die Datenbank und für die Anmeldung bei der Datenbank mit den neuen Anmeldeinformationen.

Allgemein betrachtet, umfasst dieser Prozess Folgendes:

1. Schritt 1: Erstellen einer IAM-Rolle für den IAM-Zugriff mit Single Sign-On

   (Optional) Sie können Benutzer für den Zugriff auf eine Amazon-Redshift-Datenbank authentifizieren, indem Sie IAM-Authentifizierung und einen Identitäts-Drittanbieter integrieren.
2. Schritt 2: Konfigurieren von SAML-Zusicherungen für den Identitätsanbieter

   (Optional) Damit Sie die IAM-Authentifizierung mit einem Identitätsanbieter nutzen können, müssen Sie in der Identitätsanbieteranwendung eine Anspruchsregel definieren, die Benutzer oder Gruppen innerhalb Ihrer Organisation der IAM-Rolle zuordnet. Optional können Sie Attributelemente einschließen, um `GetClusterCredentials`-Parameter festzulegen.
3. Schritt 3: Erstellen Sie eine IAM-Rolle mit Aufrufrechten GetClusterCredentials

   Ihre SQL-Clientanwendung übernimmt beim Aufruf der Operation `GetClusterCredentials` den Benutzer. Falls Sie eine IAM-Rolle für den Zugriff mithilfe eines Identitätsanbieters erstellt haben, können Sie dieser Rolle die nötige Berechtigung hinzufügen.
4. Schritt 4: Erstellen eines Datenbankbenutzers und von Datenbankgruppen

   (Optional) Standardmäßig erstellen `GetClusterCredentials`-Rückgabewerte einen neuen Benutzer, wenn der Benutzername nicht vorhanden ist. Sie können auch Benutzergruppen bestimmen, denen Benutzer bei der Anmeldung zugewiesen werden. Standardmäßig treten Datenbankbenutzer der Gruppe „PUBLIC“ bei.
5. Schritt 5: Konfigurieren einer JDBC- oder ODBC-Verbindung zur Verwendung von IAM-Anmeldeinformationen

Zum Verbinden mit Ihrer Amazon-Redshift-Datenbank konfigurieren Sie Ihren SQL-Client zur Verwendung eines Amazon-Redshift-JDBC- oder -ODBC-Treibers.

Schritt 1: Erstellen einer IAM-Rolle für den IAM-Zugriff mit Single Sign-On

Sie können diesen Schritt überspringen, wenn Sie keinen Identitätsanbieter für Zugriff mit einmaliger Anmeldung verwenden.

Wenn Sie bereits Benutzeridentitäten außerhalb von verwalten AWS, können Sie Benutzer für den Zugriff auf eine Amazon Redshift Redshift-Datenbank authentifizieren, indem Sie die IAM-Authentifizierung und einen SAML-2.0-Identitätsanbieter (IdP) eines Drittanbieters integrieren.

Weitere Informationen finden Sie unter Identitätsanbieter und Verbund im IAM-Benutzerhandbuch.

Bevor Sie die Amazon Redshift IdP-Authentifizierung verwenden können, müssen Sie einen AWS SAML-Identitätsanbieter erstellen. Sie erstellen einen IdP in der IAM-Konsole, um AWS über den IdP und seine Konfiguration zu informieren. Dadurch wird Vertrauen zwischen Ihrem AWS Konto und dem IdP hergestellt. Informationen zur Erstellen einer Rolle finden Sie unter Erstellen einer Rolle für SAML-2.0-Verbund (Konsole) im IAM-Benutzerhandbuch.

Schritt 2: Konfigurieren von SAML-Zusicherungen für den Identitätsanbieter

Nach der Erstellung der IAM-Rolle müssen Sie in Ihrer IdP-Anwendung eine Antragsregel definieren, die Benutzer oder Gruppen innerhalb Ihrer Organisation der IAM-Rolle zuordnet. Weitere Informationen finden Sie unter Konfigurieren von SAML-Zusicherungen für die Authentifizierungsantwort im IAM-Benutzerhandbuch.

Wenn Sie die optionalen `GetClusterCredentials`-Parameter `DbUser`, `AutoCreate`, und `DbGroups` verwenden, haben Sie zwei Optionen. Sie können die Werte für die Parameter mit Ihrer JDBC- oder ODBC-Verbindung festlegen, oder Sie können die Werte durch Hinzufügen von SAML-Attributelementen zu Ihrem IdP festlegen. Weitere Hinweise zu den Parametern `DbUser`, `AutoCreate` und `DbGroups` finden Sie unter Schritt 5: Konfigurieren einer JDBC- oder ODBC-Verbindung zur Verwendung von IAM-Anmeldeinformationen.

> **Note**
>
> Wenn Sie eine IAM-Richtlinienvariable verwenden, `${redshift:DbUser}`, wie in Ressourcenrichtlinien für GetClusterCredentials beschrieben, wird der Wert für `DbUser` durch

den Wert ersetzt, der vom Abfragekontext der API-Operation abgerufen wird. Die Amazon-Redshift-Treiber verwenden den von der Verbindungs-URL bereitgestellten Wert für die `DbUser`-Variable, nicht den als SAML-Attribut bereitgestellten Wert.
Wir empfehlen, für die Sicherstellung dieser Konfiguration eine Bedingung in einer IAM-Richtlinie zu verwenden, um den `DbUser`-Wert mit `RoleSessionName` zu validieren. Beispiele, wie Sie eine Bedingung in einer IAM-Richtlinie einrichten, finden Sie in Beispielrichtlinie für die Verwendung GetClusterCredentials.

Um Ihren IdP so zu konfigurieren, dass die Parameter `DbUser`, `AutoCreate` und `DbGroups` festgelegt werden, schließen Sie die folgenden `Attribute`-Elemente ein:

- Ein `Attribute` Element, bei dem das `Name` Attribut auf "https://redshift.amazon.com/SAML/Attributes/DbUser" gesetzt ist

  Setzen Sie das `AttributeValue`-Element auf den Namen eines Benutzers, der sich mit der Amazon-Redshift-Datenbank verbinden wird.

  Der Wert des `AttributeValue`-Elements muss aus Kleinbuchstaben bestehen, muss mit einem Buchstaben beginnen, darf nur alphanumerische Zeichen, Unterstriche („_“), Pluszeichen („+“), Punkte („.“), At-Zeichen („@“) oder Bindestriche („-“) enthalten und muss weniger als 128 Zeichen lang sein. Üblicherweise ist der Benutzername eine Benutzer-ID (z. B. bobsmith) oder eine E-Mail-Adresse (z. B. bobsmith@beispiel.com): Der Wert darf kein Leerzeichen enthalten (wie etwa der Anzeigename eines Benutzers, z. B. Bob Smith).

  ```
  <Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbUser">
      <AttributeValue>user-name</AttributeValue>
  </Attribute>
  ```

- Ein Attributelement, bei dem das Name-Attribut auf "https://redshift.amazon.com/SAML/Attributes/AutoCreate" gesetzt ist

  Setzen Sie das AttributeValue Element auf true, um einen neuen Datenbankbenutzer zu erstellen, falls noch keiner existiert. Setzen Sie den Wert AttributeValue auf False, um anzugeben, dass der Datenbankbenutzer in der Amazon Redshift Redshift-Datenbank vorhanden sein muss.

  ```
  <Attribute Name="https://redshift.amazon.com/SAML/Attributes/AutoCreate">
      <AttributeValue>true</AttributeValue>
  </Attribute>
  ```

- Ein `Attribute` Element, bei dem das `Name` Attribut auf "https://redshift.amazon.com/SAML/Attributes/DbGroups" gesetzt ist

  Dieses Element enthält ein oder mehrere `AttributeValue`-Elemente. Legen Sie jedes `AttributeValue`-Element auf den Namen einer Datenbankgruppe fest, der der `DbUser` für die Dauer der Sitzung beitritt, wenn er sich mit der Amazon-Redshift-Datenbank verbindet.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbGroups">
    <AttributeValue>group1</AttributeValue>
    <AttributeValue>group2</AttributeValue>
    <AttributeValue>group3</AttributeValue>
</Attribute>
```

Schritt 3: Erstellen Sie eine IAM-Rolle mit Aufrufrechten GetClusterCredentials

Ihr SQL-Client benötigt eine Autorisierung, um die Operation `GetClusterCredentials` in Ihrem Namen aufrufen zu können. Diese Autorisierung stellen Sie zur Verfügung, indem Sie einen Benutzer oder eine Rolle erstellen und eine Richtlinie anfügen, die die notwendigen Berechtigungen gewährt.

Um eine IAM-Rolle mit Anrufberechtigungen zu erstellen GetClusterCredentials

1. Erstellen Sie einen Benutzer oder eine Rolle mithilfe des IAM-Service. Sie können auch einen vorhandenen Benutzer bzw. eine vorhandene Rolle verwenden. Falls Sie beispielsweise eine IAM-Rolle für den Zugriff mithilfe eines Identitätsanbieters erstellt haben, können Sie dieser Rolle die nötigen IAM-Richtlinien anfügen.
2. Fügen Sie eine Berechtigungsrichtlinie mit der Berechtigung zum Aufruf der Operation `redshift:GetClusterCredentials` an. Je nachdem, welche optionalen Parameter Sie angeben, können Sie auch zusätzliche Aktionen und Ressourcen in der Richtlinie zulassen oder einschränken:

   - Damit Ihr SQL-Client Cluster-ID, AWS Region und Port abrufen kann, schließen Sie die Erlaubnis ein, den `redshift:DescribeClusters` Vorgang mit der Redshift-Clusterressource aufzurufen.
   - Wenn Sie die Option `AutoCreate` verwenden, schließen Sie die Berechtigung zum Aufruf von `redshift:CreateClusterUser` mit der `dbuser`-Ressource ein. Der folgende Amazon-Ressourcenname (ARN) gibt den Amazon-Redshift- an `dbuser`. Ersetzen Sie *`regionaccount-id`*, und *`cluster-name`*durch die Werte für Ihre AWS Region, Ihr

Konto und Ihren Cluster. Geben Sie für *dbuser-name* den Benutzernamen an, der für die Anmeldung bei der Clusterdatenbank verwendet werden soll.

```
arn:aws:redshift:region:account-id:dbuser:cluster-name/dbuser-name
```

- (Optional) Fügen Sie einen ARN hinzu, der die Amazon-Redshift-dbname-Ressource im folgenden Format angibt. Ersetzen Sie *regionaccount-id*, und *cluster-name*durch die Werte für Ihre AWS Region, Ihr Konto und Ihren Cluster. Geben Sie für *database-name* den Namen einer Datenbank an, bei der sich der Benutzer anmelden soll.

  ```
  arn:aws:redshift:region:account-id:dbname:cluster-name/database-name
  ```

- Wenn Sie die Option `DbGroups` verwenden, schließen Sie die Berechtigung zum Aufrufen des `redshift:JoinGroup`-Vorgangs mit der Amazon-Redshift-Ressource `dbgroup` im folgenden Format ein. Ersetzen Sie *regionaccount-id*, und *cluster-name*durch die Werte für Ihre AWS Region, Ihr Konto und Ihren Cluster. Geben Sie für *dbgroup-name* den Namen einer Benutzergruppe an, der der Benutzer bei der Anmeldung zugewiesen wird.

  ```
  arn:aws:redshift:region:account-id:dbgroup:cluster-name/dbgroup-name
  ```

Weitere Informationen und Beispiele finden Sie unter Ressourcenrichtlinien für GetClusterCredentials.

Das folgende Beispiel zeigt eine Richtlinie, die zulässt, dass die IAM-Rolle die Operation `GetClusterCredentials` aufruft. Indem Sie die Amazon-Redshift-Ressource `dbuser` angeben, gewähren Sie der Rolle Zugriff auf den Datenbankbenutzernamen `temp_creds_user` auf dem Cluster `examplecluster`.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
temp_creds_user"
  }
}
```

Sie können einen Platzhalter (*) verwenden, um Cluster-Namen, Benutzernamen und Datenbankgruppennamen ganz oder teilweise zu ersetzen. Im folgenden Beispiel wird jedem Benutzernamen Zugriff gewährt, der mit `temp_` beginnt, sich in einem beliebigen Cluster befindet und zum angegebenen Konto gehört.

> **Important**
>
> Die Anweisung im folgenden Beispiel gibt ein Platzhalterzeichen (*) als Teil des Werts für die Ressource an, sodass durch die Richtlinie alle Ressourcen zugelassen werden, die mit dem angegebenen Zeichen beginnen. Durch die Verwendung eines Platzhalterzeichens in Ihren IAM-Richtlinien werden großzügige Berechtigungen erteilt. Deshalb wird empfohlen, eine möglichst restriktive Richtlinie für Ihre Geschäftsanwendung zu nutzen.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:*/temp_*"
  }
}
```

Das folgende Beispiel zeigt eine Richtlinie, die der IAM-Rolle den Aufruf der Operation `GetClusterCredentials` ermöglicht. Dabei besteht die Möglichkeit, automatisch einen neuen Benutzer zu erstellen und Gruppen anzugeben, denen der Benutzer bei der Anmeldung zugewiesen wird. Die Klausel `"Resource": "*"` gewährt der Rolle Zugriff auf jede beliebige Ressource, einschließlich Clustern, Datenbankbenutzern und Benutzergruppen.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
              "redshift:GetClusterCredentials",
              "redshift:CreateClusterUser",
  "redshift:JoinGroup"
            ],
    "Resource": "*"
  }
```

```
}
```

Weitere Informationen dazu finden Sie unter Amazon Redshift – ARN-Syntax.

Schritt 4: Erstellen eines Datenbankbenutzers und von Datenbankgruppen

Optional können Sie einen Datenbankbenutzer erstellen, mit dem Sie sich bei der Cluster-Datenbank anmelden. Wenn Sie temporäre Benutzeranmeldedaten für einen bestehenden Benutzer erstellen, können Sie das Passwort des Benutzers deaktivieren, um den Benutzer dazu zu zwingen, sich mit dem temporären Passwort anzumelden. Alternativ können Sie die Option „AutoCreate“ der Operation `GetClusterCredentials` dazu verwenden, automatisch einen neuen Datenbankbenutzer zu erstellen.

Sie können Datenbankbenutzergruppen mit den Berechtigungen erstellen, die der IAM-Datenbankbenutzer erhalten soll, wenn er den Gruppen bei der Anmeldung zugewiesen wird. Wenn Sie die Operation `GetClusterCredentials` aufrufen, können Sie eine Liste von Benutzergruppennamen angeben, denen ein neuer Benutzer bei der Anmeldung zugewiesen wird. Diese Gruppenmitgliedschaften sind nur für Sitzungen gültig, die mit Anmeldeinformationen generiert wurden, für die diese Anfrage gilt.

Erstellen Sie einen Datenbankbenutzer und Datenbankgruppen wie folgt:

1. Melden Sie sich bei Ihrer Amazon-Redshift-Datenbank an und erstellen Sie einen Datenbankbenutzer mithilfe von CREATE USER (BENUTZER ERSTELLEN) oder bearbeiten Sie einen vorhandenen Benutzer mithilfe von ALTER USER (BENUTZER ÄNDERN).
2. Optional aktivieren Sie die Option „PASSWORD DISABLE“, um zu verhindern, dass der Benutzer ein Passwort verwendet. Wenn das Passwort eines Benutzers deaktiviert ist, kann sich der Benutzer nur anhand der temporären Anmeldeinformationen anmelden. Wenn das Passwort nicht deaktiviert ist, kann sich der Benutzer entweder mithilfe des Passworts oder mithilfe der temporären Anmeldeinformationen anmelden. Sie können das Passwort eines Superusers nicht deaktivieren.

   Benutzer benötigen programmgesteuerten Zugriff, wenn sie mit AWS außerhalb des AWS Management Console interagieren möchten. Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt von der Art des Benutzers ab, der zugreift. AWS

   Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwenden im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldedaten im Benutzerhandbuch. AWS CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Im folgenden Beispiel wird ein Benutzer mit deaktiviertem Passwort erstellt.

```
create user temp_creds_user password disable;
```

Im folgenden Beispiel wird das Passwort eines bestehenden Benutzers deaktiviert.

```
alter user temp_creds_user password disable;
```

3. Erstellen Sie Datenbankbenutzergruppen mithilfe des Befehls CREATE GROUP.
4. Mit dem Befehl GRANT definieren Sie Zugriffsrechte für die Gruppen.

Schritt 5: Konfigurieren einer JDBC- oder ODBC-Verbindung zur Verwendung von IAM-Anmeldeinformationen

Sie können Ihren SQL-Client mit einem Amazon-Redshift-JDBC- oder -ODBC-Treiber konfigurieren. Dieser Treiber verwaltet das Erstellen von Anmeldeinformationen für Datenbankbenutzer und das Herstellen einer Verbindung zwischen Ihrem SQL-Client und Ihrer Amazon-Redshift-Datenbank.

Wenn Sie einen Identitätsanbieter zur Authentifizierung erstellen, geben Sie den Namen eines Anmeldeinformationsanbieter-Plug-ins ein. Die Amazon-Redshift-JDBC- und -ODBC-Treiber enthalten Plug-Ins für die folgenden SAML-basierten Identitätsanbieter:

- Active Directory Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure AD

  Die Schritte zum Einrichten von Microsoft Azure AD als Identitätsanbieter finden Sie unter Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit Microsoft Azure AD.

Konfigurieren Sie eine JDBC-Verbindung zur Verwendung von IAM-Anmeldeinformationen wie folgt:

1. Laden Sie den neuesten Amazon-Redshift-JDBC-Treiber von der Seite Konfigurieren einer Verbindung für JDBC-Treiberversion 2.1 für Amazon Redshift herunter.
2. Erstellen Sie mit den Optionen für IAM-Anmeldeinformationen eine JDBC-URL in einem der folgenden Formate. Um die IAM-Authentifizierung zu verwenden, fügen Sie der Amazon-Redshift-JDBC-URL nach `jdbc:redshift:` das Element `iam:` hinzu, wie im folgenden Beispiel gezeigt.

   ```
   jdbc:redshift:iam://
   ```

Fügen Sie `cluster-name`, `region` und `account-id` hinzu. Der JDBC-Treiber verwendet Ihre IAM-Kontoinformationen und den Clusternamen, um die Cluster-ID und Region abzurufen. AWS Dazu muss Ihr Benutzer oder Ihre Rolle zum Aufruf der Operation `redshift:DescribeClusters` mit dem angegebenen Cluster berechtigt sein. Wenn Ihr Benutzer oder Ihre Rolle nicht berechtigt ist, den `redshift:DescribeClusters` Vorgang aufzurufen, geben Sie die Cluster-ID, AWS Region und Port an, wie im folgenden Beispiel gezeigt. Der Portnummer ist optional.

```
jdbc:redshift:iam://examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com:5439/dev
```

3. Fügen Sie JDBC-Optionen hinzu, um IAM-Anmeldeinformationen bereitzustellen. Sie verwenden verschiedene Kombinationen von JDBC-Optionen, um IAM-Anmeldeinformationen bereitzustellen. Details hierzu finden Sie unter JDBC- und ODBC-Optionen zur Erstellung von Benutzeranmeldeinformationen für die Datenbank.

   Die folgende URL gibt die AccessKey ID und SecretAccessKey für einen Benutzer an.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?
   AccessKeyID=AKIAIOSFODNN7EXAMPLE&SecretAccessKey=wJalrXUtnFEMI/K7MDENG/
   bPxRfiCYEXAMPLEKEY
   ```

   Im folgenden Beispiel wird ein benanntes Profil angegeben, das die IAM-Anmeldeinformationen enthält.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?Profile=user2
   ```

4. Fügen Sie JDBC-Optionen hinzu, die der JDBC-Treiber zum Aufrufen der API-Operation `GetClusterCredentials` verwendet. Schließen Sie diese Optionen nicht ein, wenn Sie die API-Operation `GetClusterCredentials` programmgesteuert aufrufen.

   Das folgende Beispiel enthält die JDBC-`GetClusterCredentials`-Optionen.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?
   plugin_name=com.amazon.redshift.plugin.AzureCredentialsProvider&UID=user&PWD=password&idp_t
   ```

Konfigurieren Sie eine ODBC-Verbindung zur Verwendung von IAM-Anmeldeinformationen wie folgt:

Im folgenden Verfahren finden Sie Schritte nur zum Konfigurieren der IAM-Authentifizierung. Anweisungen zur Verwendung der Standardauthentifizierung mit einem Datenbankbenutzernamen und -passwort finden Sie unter Konfigurierung einer ODBC-Verbindung.

1. Installieren und konfigurieren Sie den neuesten Amazon-Redshift-OBDC-Treiber für Ihr Betriebssystem. Weitere Informationen finden Sie auf der Seite Konfigurierung einer ODBC-Verbindung.

   > **Important**
   >
   > Der Amazon-Redshift-ODBC-Treiber muss Version 1.3.6.1000 oder neuer sein.

2. Befolgen Sie die betriebssystemspezifischen Anweisungen zur Konfiguration der Verbindungseinstellungen.

   Weitere Informationen finden Sie unter einem der folgenden Themen:

   - Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows
   - Verwenden Sie einen ODBC-Treibermanager, um den Treiber unter Linux und macOS X zu konfigurieren

3. Greifen Sie unter Microsoft-Windows-Betriebssystemen auf das Fenster „Amazon Redshift ODBC Driver DSN Setup“ (DSN-Einrichtung des Amazon-Redshift-ODBC-Treibers) zu.

   a. Geben Sie unter Connection Settings (Verbindungseinstellungen) die folgenden Informationen ein:

      - Datenquellenname
      - Server (optional)
      - Port (optional)
      - Datenbank

      Verfügt der Benutzer bzw. die Rolle über die Berechtigung zum Aufrufen der Operation `redshift:DescribeClusters`, sind nur Datenquellenname und Datenbank erforderlich. Amazon Redshift verwendet ClusterIdand Region, um den Server und den Port durch Aufrufen des `DescribeCluster` Vorgangs abzurufen.

Verfügt der Benutzer bzw. die Rolle nicht über die Berechtigung zum Aufruf der Operation `redshift:DescribeClusters`, müssen Sie Server und Port angeben.

b. Wählen Sie unter Authentifizierung einen Wert für Authentifizierungstypaus.

Geben Sie für jeden Authentifizierungstyp Werte wie folgt ein:

AWS -Profil

Geben Sie die folgenden Informationen ein:

- ClusterID
- Region
- Profilname

  Geben Sie den Namen eines Profils in eine AWS Konfigurationsdatei ein, die Werte für die ODBC-Verbindungsoptionen enthält. Weitere Informationen finden Sie unter Verwendung eines Konfigurationsprofils.

(Optional) Geben Sie Details zu den Optionen an, die der ODBC-Treiber zum Aufrufen der API-Operation `GetClusterCredentials` verwendet:

- DbUser
- Benutzer AutoCreate
- DbGroups

  Weitere Informationen finden Sie unter JDBC- und ODBC-Optionen zur Erstellung von Benutzeranmeldeinformationen für die Datenbank.

IAM-Anmeldeinformationen

Geben Sie die folgenden Informationen ein:

- ClusterID
- Region
- AccessKeyID und SecretAccessKey

  Die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel der IAM-Rolle bzw. des Benutzers, die bzw. der für die IAM-Datenbankauthentifizierung konfiguriert wurde.

- SessionToken

SessionTokenist für eine IAM-Rolle mit temporären Anmeldeinformationen erforderlich. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen.

Geben Sie Details zu den Optionen an, die der ODBC-Treiber zum Aufrufen der API-Operation `GetClusterCredentials` verwendet:

- DbUser(erforderlich)
- Benutzer AutoCreate (optional)
- DbGroups(fakultativ)

  Weitere Informationen finden Sie unter JDBC- und ODBC-Optionen zur Erstellung von Benutzeranmeldeinformationen für die Datenbank.

Identitätsanbieter: AD FS

Lassen Sie zur Verwendung der Windows-integrierten Authentifizierung mit AD FS die Felder User und Passwort frei.

Geben Sie IdP-Details an:

- IdP Host

  Der Name des Identitätsanbieterhosts des Unternehmens. Der Name darf keine Schrägstriche („/“) enthalten.
- IdP Port (optional)

  Der vom Identitätsanbieter verwendete Port. Der Standardwert ist 443.
- Preferred Role

  Ein Amazon-Ressourcenname (ARN) für die IAM-Rolle von den Mehrwerte-`AttributeValue`-Elementen für das `Role`-Attribut in der SAML-Zusicherung. Wenden Sie sich für den korrekten Wert für die bevorzugte Rolle an den IdP-Administrator. Weitere Informationen finden Sie unter Konfigurieren von SAML-Zusicherungen für den Identitätsanbieter.

(Optional) Geben Sie Details zu den Optionen an, die der ODBC-Treiber zum Aufrufen der API-Operation `GetClusterCredentials` verwendet:

- DbUser
- Nutzer AutoCreate

- DbGroups

Weitere Informationen finden Sie unter JDBC- und ODBC-Optionen zur Erstellung von Benutzeranmeldeinformationen für die Datenbank.

Identitätsanbieter: PingFederate

Geben Sie für User (Benutzer) und Password (Passwort) den Benutzernamen und das Passwort für Ihren Identitätsanbieter (IdP) ein.

Geben Sie IdP-Details an:

- IdP Host

  Der Name des Identitätsanbieterhosts des Unternehmens. Der Name darf keine Schrägstriche („/“) enthalten.

- IdP Port (optional)

  Der vom Identitätsanbieter verwendete Port. Der Standardwert ist 443.

- Preferred Role

  Ein Amazon-Ressourcenname (ARN) für die IAM-Rolle von den Mehrwerte-`AttributeValue`-Elementen für das `Role`-Attribut in der SAML-Zusicherung. Wenden Sie sich für den korrekten Wert für die bevorzugte Rolle an den IdP-Administrator. Weitere Informationen finden Sie unter Konfigurieren von SAML-Zusicherungen für den Identitätsanbieter.

(Optional) Geben Sie Details zu den Optionen an, die der ODBC-Treiber zum Aufrufen der API-Operation `GetClusterCredentials` verwendet:

- DbUser
- Nutzer AutoCreate
- DbGroups

Weitere Informationen finden Sie unter JDBC- und ODBC-Optionen zur Erstellung von Benutzeranmeldeinformationen für die Datenbank.

Identitätsanbieter: Okta

Geben Sie für User (Benutzer) und Password (Passwort) den Benutzernamen und das Passwort für Ihren Identitätsanbieter (IdP) ein.

Geben Sie IdP-Details an:

- IdP Host

  Der Name des Identitätsanbieterhosts des Unternehmens. Der Name darf keine Schrägstriche („/“) enthalten.

- IdP Port

  Dieser Wert wird von Okta nicht verwendet.

- Preferred Role

  Ein Amazon-Ressourcenname (ARN) für die IAM-Rolle von den `AttributeValue`-Elementen für das `Role`-Attribut in der SAML-Zusicherung. Wenden Sie sich für den korrekten Wert für die bevorzugte Rolle an den IdP-Administrator. Weitere Informationen finden Sie unter Konfigurieren von SAML-Zusicherungen für den Identitätsanbieter.

- Okta App ID

  Eine ID für eine Okta-Anwendung. Der Wert für die Anwendungs-ID folgt im Anwendungseinbettungslink von Okta auf „amazon_aws“. Der Identitätsanbieteradministrator kann Ihnen diesen Wert zur Verfügung stellen.

(Optional) Geben Sie Details zu den Optionen an, die der ODBC-Treiber zum Aufrufen der API-Operation `GetClusterCredentials` verwendet:

- DbUser
- Nutzer AutoCreate
- DbGroups

Weitere Informationen finden Sie unter JDBC- und ODBC-Optionen zur Erstellung von Benutzeranmeldeinformationen für die Datenbank.

Identitätsanbieter: Azure AD

Geben Sie für User (Benutzer) und Password (Passwort) den Benutzernamen und das Passwort für Ihren Identitätsanbieter (IdP) ein.

Geben Sie für Cluster ID (Cluster-ID) und Region die Cluster-ID und AWS -Region Ihres Amazon-Redshift-Clusters ein.

Geben Sie bei Database (Datenbank) die Datenbank ein, die Sie für Ihren Amazon-Redshift-Cluster erstellt haben.

Geben Sie IdP-Details an:

- IdP Tenant (dP-Mandant

  Der für Azure AD verwendete Mandant.
- Azure Client Secret (Azure-Clientgeheimnis

  Das Client-Secret der Amazon-Redshift-Unternehmensanwendung in Azure.
- Azure Client ID (Azure-Client-ID

  Die Client-ID (Anwendungs-ID) der Amazon-Redshift-Unternehmensanwendung in Azure.

(Optional) Geben Sie Details zu den Optionen an, die der ODBC-Treiber zum Aufrufen der API-Operation `GetClusterCredentials` verwendet:

- DbUser
- Nutzer AutoCreate
- DbGroups

Weitere Informationen finden Sie unter JDBC- und ODBC-Optionen zur Erstellung von Benutzeranmeldeinformationen für die Datenbank.

Optionen für die Bereitstellung von IAM-Anmeldeinformationen

Wählen Sie eine der folgenden Optionen aus, um IAM-Anmeldeinformationen für eine JDBC- oder ODBC-Verbindung bereitzustellen.

- AWS profile

  Als Alternative zur Bereitstellung von Anmeldeinformationswerten in der Form von JDBC- bzw. ODBC-Einstellungen können Sie die Werte in einem benannten Profil platzieren. Weitere Informationen finden Sie unter Verwendung eines Konfigurationsprofils.

- IAM-Anmeldeinformationen

  Geben Sie Werte für AccessKey ID und optional SessionToken in Form von JDBC- oder ODBC-Einstellungen an. SecretAccessKey SessionToken ist nur für eine IAM-Rolle mit temporären Anmeldeinformationen erforderlich. Weitere Informationen finden Sie unter JDBC- und ODBC-Optionen für die Bereitstellung von IAM-Anmeldeinformationen.

- Identitätsanbieterverbund

  Wenn Sie den Identitätsanbieterverbund verwenden, um Benutzern von einem Identitätsanbieter die Authentifizierung bei Amazon Redshift zu ermöglichen, geben Sie den Namen eines Anmeldeinformationsanbieter-Plug-Ins an. Weitere Informationen finden Sie unter Verwenden eines Anmeldeinformationsanbieter-Plug-ins.

  Die Amazon-Redshift-JDBC- und -ODBC-Treiber beinhalten Plug-Ins für die folgenden SAML-basierten Identitätsverbund-Anmeldeinformationsanbieter:

  - Microsoft Active Identity Federation Services (AD FS)
  - PingOne
  - Okta
  - Microsoft Azure Active Directory (Azure AD)

  Sie können den Namen des jeweiligen Plug-Ins und zugehörige Werte in der Form von JDBC- bzw. ODBC-Einstellungen oder durch Verwendung eines Profils bereitstellen. Weitere Informationen erhalten Sie unter Konfigurationsoptionen der JDBC-Treiberversion 2.1 und Konfigurieren von ODBC-Treiberoptionen.

Weitere Informationen finden Sie unter Konfigurieren einer JDBC- oder ODBC-Verbindung zur Verwendung von IAM-Anmeldeinformationen.

Verwendung eines Konfigurationsprofils

Sie können die Optionen und `GetClusterCredentials` Optionen für die IAM-Anmeldeinformationen als Einstellungen in benannten Profilen in Ihrer AWS Konfigurationsdatei angeben. Stellen Sie den Profilnamen über die Option „Profile JDBC“ bereit. Die Konfiguration ist

in einer Datei namens `config` oder `credentials` im Ordner `.aws` in Ihrem Stammverzeichnis gespeichert.

Für ein Plug-In für einen SAML-basierten Anmeldeinformationsanbieter, das in einem Amazon-Redshift-JDBC- oder -ODBC-Treiber enthalten ist, können Sie die zuvor in beschriebenen Einstellungen verwenden Verwenden eines Anmeldeinformationsanbieter-Plug-ins. Wenn `plugin_name` nicht verwendet wird, werden die anderen Optionen ignoriert.

Das folgende Beispiel zeigt die Datei ~/.aws/credentials mit zwei Profilen.

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

[user2]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
session_token=AQoDYXdzEPT//////////
wEXAMPLEtc764bNrC9SAPBSM22wDOk4x4HIZ8j4FZTwdQWLWsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTflfKD8YUuwthAx7
qkPpKPi/kMcGd
QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5VSXDvp75YU
9HFvlRd8Tx6q6fE8YQcHNVXAkiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fPOLn9FX9KSYvKTr4rvx3iSIlTJabIQwj2ICCR/oLxBA==
```

Geben Sie zur Verwendung der Anmeldedaten für das Beispiel `user2` in der JDBC-URL `Profile=user2` an.

Weitere Informationen zur Verwendung von Profilen finden Sie unter Einstellungen für die Konfiguration und die Anmeldeinformationsdatei im AWS Command Line Interface Benutzerhandbuch.

Weitere Informationen zur Verwendung von Profilen für JDBC-Treiber finden Sie in Angeben von Profilen.

Weitere Informationen zur Verwendung von Profilen für ODBC-Treiber finden Sie in Konfigurieren der Authentifizierung.

JDBC- und ODBC-Optionen für die Bereitstellung von IAM-Anmeldeinformationen

In der folgenden Tabelle sind die JDBC- und ODBC-Optionen für die Bereitstellung von IAM-Anmeldeinformationen aufgeführt.

Option	Beschreibung
`Iam`	Ausschließlich zur Verwendung in ODBC-Verbindungszeichenfolgen gedacht. Legen Sie „1“ fest, um die IAM-Authentifizierung zu verwenden.

`AccessKeyID`
 	
`SecretAccessKey`
 	
`SessionToken`
	Die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel für die IAM-Rolle oder den Benutzer, der für die IAM-Datenbankauthentifizierung konfiguriert ist. `SessionToken` ist nur für eine IAM-Rolle mit temporären Anmeldeinformationen erforderlich. SessionToken wird nicht für einen Benutzer verwendet. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen.

`plugin_name`	Der vollqualifizierte Name einer Klasse, die einen Anmeldeinformationsanbieter implementiert. Der Amazon-Redshift-JDBC-Treiber beinhaltet Plug-Ins für SAML-basierte Anmeldeinformationsanbieter. Wenn Sie `plugin_name` angeben, können Sie auch andere verwandte Optionen angeben. Weitere Informationen finden Sie unter Verwenden eines Anmeldeinformationsanbieter-Plug-ins.
`Profile`	Der Name eines Profils in einer AWS Anmelde- oder Konfigurationsdatei, die Werte für die JDBC-Verbindungsoptionen enthält. Weitere Informationen finden Sie unter Verwendung eines Konfigurationsprofils.

Verwenden eines Anmeldeinformationsanbieter-Plug-ins

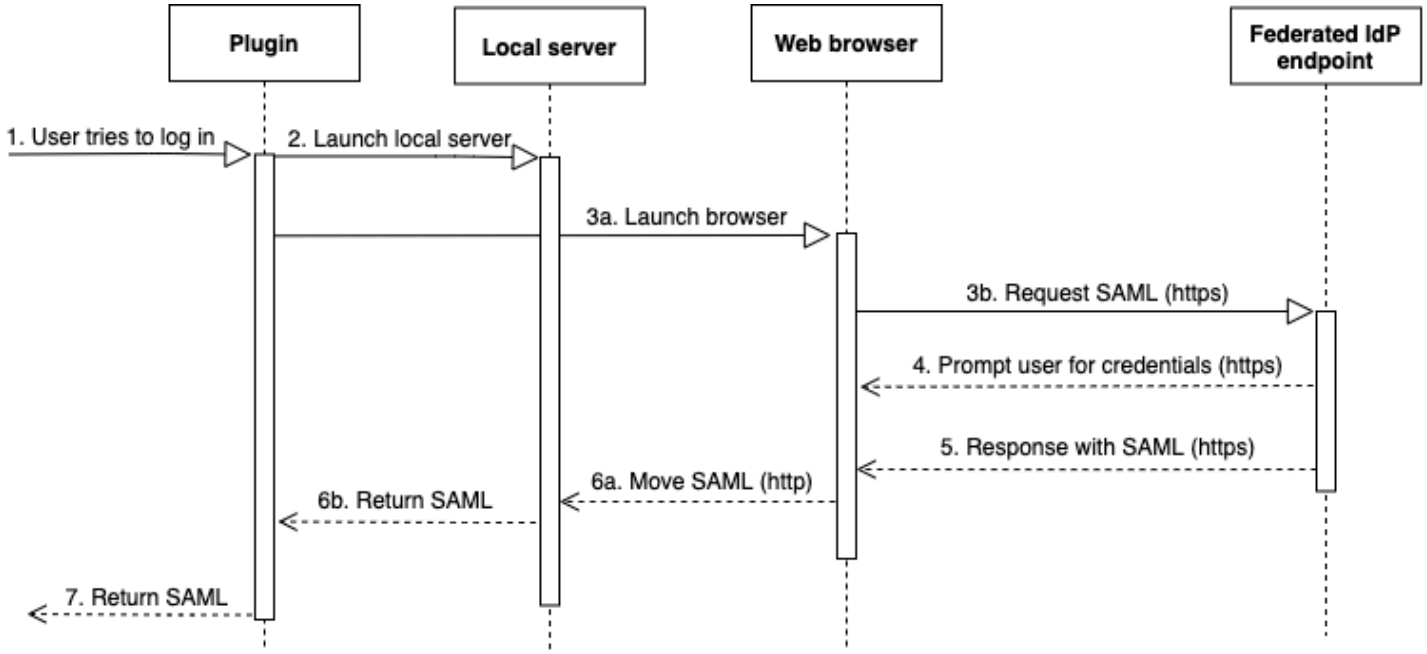
Amazon Redshift verwendet Plug-Ins für Anmeldeinformationsanbieter zur Single-Sign-On-Authentifizierung.

Zur Unterstützung der Single-Sign-On-Authentifizierung stellt Amazon Redshift das Azure-AD-Plug-In für Microsoft Azure Active Directory bereit. Informationen zur Konfiguration dieses Plug-ins finden Sie unter Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit Microsoft Azure AD.

Einrichten der Multi-Factor Authentication
Einrichten der Multi-Factor Authentication

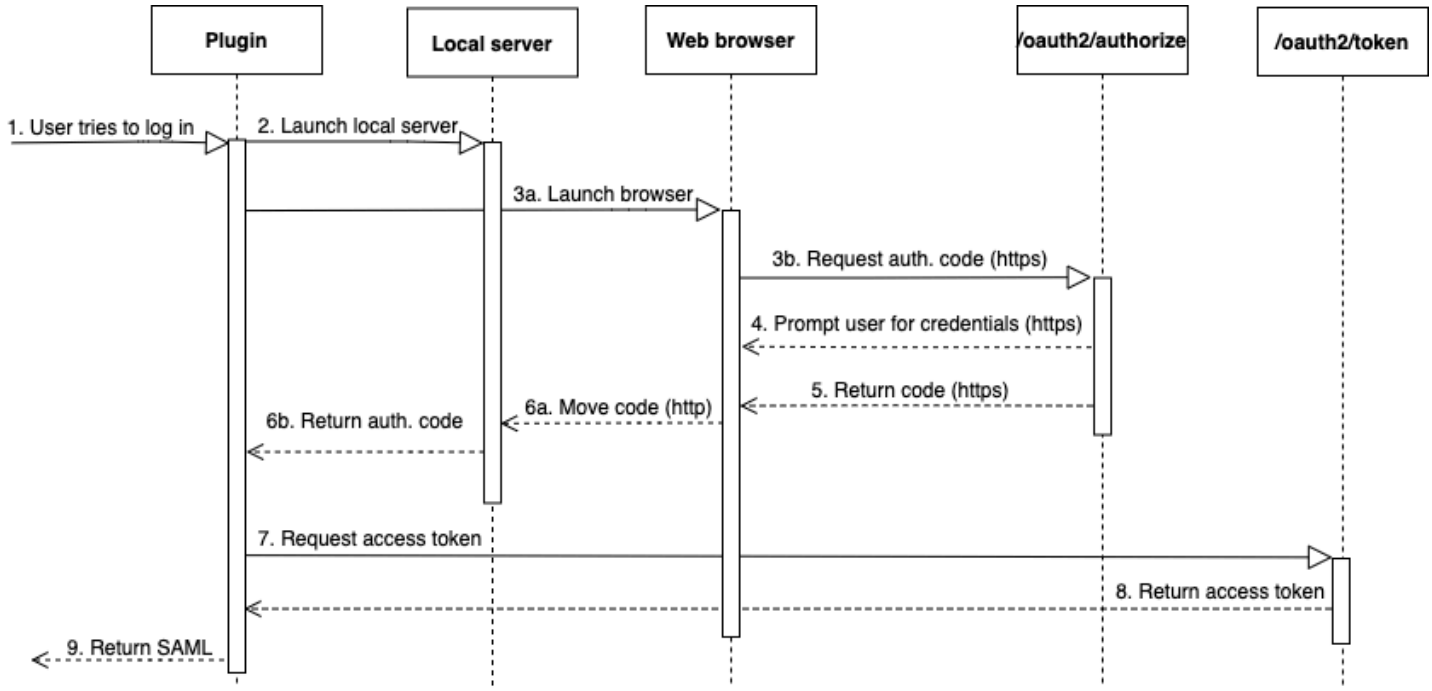
Zur Unterstützung von Multi-Faktor-Authentifizierung (MFA) stellt Amazon Redshift browserbasierte Plug-Ins bereit. Verwenden Sie das Browser-SAML-Plug-In für Okta und das Browser-Plug-In Azure AD für Microsoft Azure Active Directory. PingOne

Mit dem Browser SAML-Plugin verläuft die SAML-Authentifizierung wie folgt:



1. Ein Benutzer versucht sich anzumelden.
2. Das Plug-in startet einen lokalen Server, um eingehende Verbindungen auf dem localhost zu hören.
3. Das Plug-in startet einen Webbrowser, um eine SAML-Antwort über HTTPS von der angegebenen Single-Sign-On-URL des Verbundidentitätsanbieter-Endpunkts anzufordern.
4. Der Webbrowser folgt dem Link und fordert den Benutzer auf, Anmeldeinformationen einzugeben.
5. Nachdem der Benutzer sich authentifiziert und seine Zustimmung erteilt hat, gibt der Endpunkt des Verbundidentitätsanbieters eine SAML-Antwort über HTTPS an den von angegebenen URI zurück `redirect_uri`.
6. Der Webbrowser verschiebt die Antwortnachricht mit der SAML-Antwort auf die angegebene `redirect_uri`.
7. Der lokale Server akzeptiert die eingehende Verbindung und das Plug-In ruft die SAML-Antwort ab und gibt sie an Amazon Redshift weiter.

Mit dem Browser-Azure AD-Plug-in läuft die SAML-Authentifizierung folgendermaßen ab:



1. Ein Benutzer versucht sich anzumelden.
2. Das Plug-in startet einen lokalen Server, um eingehende Verbindungen auf dem localhost zu hören.
3. Das Plugin startet einen Webbrowser, um einen Autorisierungscode vom Azure AD `oauth2/authorize`-Endpunkt anzufordern.
4. Der Webbrowser folgt dem generierten Link über HTTPS und fordert den Benutzer auf, Anmeldeinformationen einzugeben. Der Link wird mithilfe von Konfigurationseigenschaften wie Mandant und client_id generiert.
5. Nachdem der Benutzer sich authentifiziert und seine Zustimmung erteilt hat, gibt der Azure AD `oauth2/authorize`-Endpunkt eine Antwort zurück und sendet sie über HTTPS mit dem Autorisierungscode an den angegebenen `redirect_uri`.
6. Der Webbrowser verschiebt die Antwortnachricht mit der SAML-Antwort auf die angegebene `redirect_uri`.
7. Der lokale Server akzeptiert die eingehende Verbindung, und das Plug-in ruft den Autorisierungscode ab und sendet eine POST-Anforderung an den Azure AD `oauth2/token`-Endpunkt.
8. Der Azure AD `oauth2/token`-Endpunkt gibt eine Antwort mit einem Zugriffs-Token an den angegebenen `redirect_uri` zurück.

9. Das Plug-In ruft die SAML-Antwort ab und übergibt sie an Amazon Redshift.

Lesen Sie die folgenden Abschnitte:

- Active Directory Federation Services (AD FS)

  Weitere Informationen finden Sie unter Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit AD FS.
- PingOne (Ping)

  Ping wird nur mit dem vordefinierten PingOne IdP-Adapter unterstützt, der die Forms-Authentifizierung verwendet.

  Weitere Informationen finden Sie unter Einrichten der Single-Sign-On-Authentifizierung über JDBC oder ODBC mit Ping Identity.
- Okta

  Okta wird nur für die von Okta bereitgestellte Anwendung unterstützt, die mit dem verwendet wird AWS Management Console.

  Weitere Informationen finden Sie unter Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit Okta.
- Microsoft Azure Active Directory

  Weitere Informationen finden Sie unter Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit Microsoft Azure AD.

Konfigurieren von Plug-in-Optionen
Konfigurieren von Plug-in-Optionen

Geben Sie zur Verwendung eines SAML-basierten Anmeldeinformationsanbieter-Plug-ins die folgenden Optionen mithilfe von JDBC- oder ODBC-Optionen oder in Form eines benannten Profils an. Wenn `plugin_name` nicht angegeben ist, werden die anderen Optionen ignoriert.

Option	Beschreibung
`plugin_name`	Bei JDBC der Klassenname, der einen Anmeldeinformationsanbieter implementiert. Geben Sie eines der folgenden Elemente an:

Option	Beschreibung

	• Für Active Directory Federation Services
	`com.amazon.redshift.plugin.AdfsCredentialsProvider`
	• Für Okta
	`com.amazon.redshift.plugin.OktaCredentialsProvider`
	• Für PingFederate
	`com.amazon.redshift.plugin.PingCredentialsProvider`
	• Für Microsoft Azure Active Directory
	`com.amazon.redshift.plugin.AzureCredentialsProvider`
	• Für SAML MFA
	`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`
	• Für Microsoft Azure Active Directory Single Sign-On mit MFA
	`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`
	
	Geben Sie bei ODBC eines der folgenden Elemente an:
	• Für Active Directory Federation Services (AD FS): `adfs`
	• Für Okta: `okta`
	• Für PingFederate: `ping`
	• Für Microsoft Azure Active Directory: `azure`
	• Für SAML MFA: `browser saml`
	• Für Microsoft Azure Active Directory Single Sign-On mit MFA: `browser azure ad`

Option	Beschreibung
`idp_host`	Der Name des Identitätsanbieterhosts des Unternehmens. Der Name darf keine Schrägstriche („/“) enthalten. Bei einem Okta-Identitätsanbieter sollte der Wert für `idp_host` mit `.okta.com` enden.
`idp_port`	Der vom Identitätsanbieter verwendete Port. Der Standardwert ist 443. Für Okta wird dieser Port ignoriert.
`preferred_role`	Ein Rollen-ARN (Amazon-Ressourcenname) der `AttributeValue` -Elemente für das `Role`-Attribut in der SAML-Zusicherung. Wenden Sie sich für den korrekten Wert für die bevorzugte Rolle an den IdP-Administrator. Weitere Informationen finden Sie unter Konfigurieren von SAML-Zusicherungen für den Identitätsanbieter.
`user`	Ein Unternehmensbenutzername, ggf. einschließlich der Domäne. Beispielsweise erfordert Active Directory den Domänennamen im Format Domäne\Benutzername.
password	Das Passwort des Unternehmensbenutzers. Wir empfehlen, diese Option nicht zu verwenden. Verwenden Sie stattdessen den SQL-Client, um ein Passwort bereitzustellen.
`app_id`	Eine ID für eine Okta-Anwendung. Wird nur mit Okta verwendet. Der Wert für `app_id` folgt im Anwendungseinbettungslink von Okta auf `amazon_aws` . Wenden Sie sich für diesen Wert an den Identitätsanbieteradministrator . Es folgt ein Beispiel für einen Anwendungseinbettungslink: `https://example.okta.com/home/amazon_aws/0oa2hylwrpM8UGehd1t7/272`
`idp_tenant`	Ein Mandant, der für Azure AD verwendet wird. Wird nur mit Azure verwendet.
`client_id`	Eine Client-ID für die Amazon-Redshift-Unternehmensanwendung in Azure AD. Wird nur mit Azure verwendet.

Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit Microsoft Azure AD

Sie können Microsoft Azure AD als Identitätsanbieter verwenden, um auf Ihren Amazon-Redshift-Cluster zuzugreifen. Im Anschluss finden Sie eine Prozedur, die beschreibt, wie Sie eine Vertrauensstellung für diesen Zweck einrichten. Weitere Informationen zur Konfiguration AWS als

Service Provider für den IdP finden Sie unter Configuring Your SAML 2.0 IdP with Relying Party Trust and Adding Claims im IAM-Benutzerhandbuch.

> **Note**
>
> Um Azure AD mit JDBC verwenden zu können, muss der Amazon-Redshift-JDBC-Treiber Version 1.2.37.1061 oder höher sein. Um Azure AD mit ODBC verwenden zu können, muss der Amazon-Redshift-ODBC-Treiber Version 1.4.10.1000 oder höher sein.

Sehen Sie sich das folgende Video an, um zu erfahren, wie Sie Amazon-Redshift-Zugriff mit Microsoft-Azure-AD-Single-Sign-On verbinden: Federating Amazon Redshift access with Microsoft Azure AD single sign-on.

So richten Sie Azure AD und Ihr AWS Konto so ein, dass sie sich gegenseitig vertrauen

1. Erstellen oder verwenden Sie einen vorhandenen Amazon-Redshift-Cluster, mit dem sich Ihre Azure-AD-Benutzer verbinden können. Um die Verbindung zu konfigurieren, werden bestimmte Eigenschaften dieses Clusters benötigt, z. B. die Clusterkennung. Weitere Informationen finden Sie unter Erstellen eines Clusters.
2. Richten Sie ein Azure Active Directory, Gruppen und Benutzer ein, die AWS im Microsoft Azure-Portal verwendet werden.
3. Fügen Sie Amazon Redshift als Unternehmensanwendung auf dem Microsoft Azure-Portal hinzu, um es für Single Sign-On an der AWS Konsole und die Verbundanmeldung bei Amazon Redshift zu verwenden. Wählen Sie Enterprise application (Unternehmensanwendung).
4. Wählen Sie +New Application (+Neue Anwendung). Die Seite „Add an application (Anwendung hinzufügen)“ wird angezeigt.
5. Suchen Sie im Suchfeld nach **AWS**.
6. Wählen Sie Amazon Web Services (AWS) und dann Add (Hinzufügen) aus. Dadurch wird die Anwendung erstellt. AWS
7. Wählen Sie unter Manage (Verwalten) die Option Single Sign-onaus.
8. Wählen Sie SAML. Die Seite „Amazon Web Services (AWS) | SAML-based Sign-on“ wird angezeigt.
9. Wählen Sie Yes (Ja) um zur Seite „Setup Single-Sign-On with SAML (Single-Sign-On mit SAML einrichten)“ fortzufahren. Auf dieser Seite wird die Liste vorkonfigurierter Attribute angezeigt, die sich auf Single Sign-On beziehen.

10. Wählen Sie für Basic SAML Configuration (Grundlegende SAML-Konfiguration) das Bearbeitungssymbol und dann Save (Speichern).
11. Wenn Sie für mehrere Anwendungen konfigurieren, geben Sie einen ID-Wert ein. Geben Sie z. B. ei ***https://signin.aws.amazon.com/saml#2***. Beachten Sie, dass ab der zweiten Anwendung dieses Format mit einem # -Zeichen verwendet werden muss, um einen eindeutigen SPN-Wert anzugeben.
12. Wählen Sie im Abschnitt User Attributes and Claims (Benutzerattribute und Anträge) das Bearbeitungssymbol aus.

    Standardmäßig sind der Unique User Identifier (UID), die Rolle und die SessionDuration Ansprüche vorkonfiguriert. RoleSessionName
13. Wählen Sie + Add new claim (+ Neuen Antrag hinzufügen), um einen Antrag für Datenbankbenutzer hinzuzufügen.

    Geben Sie unter Name **`DbUser`** ein.

    Geben Sie für Namespace **`https://redshift.amazon.com/SAML/Attributes`** ein.

    Wählen Sie unter Source (Quelle) die Option Attribute (Attribut) aus.

    Wählen Sie für Source attribute (Quellattribut) user.userprincipalname aus. Wählen Sie dann Save (Speichern) aus.
14. Wählen Sie + Neuen Anspruch hinzufügen, um einen Anspruch hinzuzufügen. AutoCreate

    Geben Sie unter Name **`AutoCreate`** ein.

    Geben Sie für Namespace **`https://redshift.amazon.com/SAML/Attributes`** ein.

    Wählen Sie unter Source (Quelle) die Option Attribute (Attribut) aus.

    Wählen Sie für Source attribute (Quellattribut) „true“. Wählen Sie dann Save (Speichern) aus.

    Hier ist *`123456789012`* Ihr AWS -Konto, *`AzureSSO`* ist eine von Ihnen erstellte IAM-Rolle und *`AzureADProvider`* ist der IAM-Anbieter.

Name des Antrags	Wert
Eindeutige Benutzer-ID (Namens-ID)	user.userprincipalname

Name des Antrags	Wert
https://aws.amazon.com/SAML/Attributes/SessionDuration	„900“
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam::*123456789012* :role/*AzureSSO*,arn:aws:iam::*123456789012* :saml-provider/*AzureADProvider*
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.userprincipalname
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. Fügen Sie unter App Registration (App-Registrierung) > ***your-application-name*** > Authentication (Authentifizierung) die Option Mobile And Desktop Application (Mobile und Desktop-Anwendung) hinzu. Geben Sie die URL als „http://localhost/redshift/“ an.
16. Wählen Sie im Abschnitt SAML Signing Certificate (SAML-Signaturzertifikat) die Option Download (Herunterladen) aus, um die XML-Datei für die Verbundmetadaten herunterzuladen und zu speichern, die beim Erstellen eines IAM-SAML-Identitätsanbieters verwendet werden soll. Diese Datei wird verwendet, um die Single-Sign-On-Verbundidentität zu erstellen.
17. Erstellen Sie auf der IAM-Konsole einen IAM SAML-Identitätsanbieter. Das Metadatendokument, das Sie bereitstellen, ist die XML-Datei für Verbundmetadaten, die Sie beim Einrichten der Azure Enterprise-Anwendung gespeichert haben. Ausführliche Schritte finden Sie unter Erstellen und Verwalten eines IAM-Identitätsanbieters (Konsole) im IAM-Benutzerhandbuch.
18. Erstellen Sie auf der IAM-Konsole eine IAM-Rolle für SAML 2.0-Verbund. Detaillierte Schritte finden Sie unter Erstellen einer Rolle für SAML im IAM-Benutzerhandbuch.
19. Erstellen Sie eine IAM-Richtlinie, die Sie an die IAM-Rolle anhängen können, die Sie für den SAML 2.0-Verbund auf der IAM-Konsole erstellt haben. Ausführliche Schritte finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Ändern Sie die folgende Richtlinie (im JSON-Format) für Ihre Umgebung:

- Ersetzen Sie die AWS Region Ihres Clusters durch*us-west-1*.
- Ersetzen Sie Ihr AWS Konto durch *123456789012*.
- Ersetzen Sie *cluster-identifier* durch Ihre Cluster-ID (oder * für alle Cluster).
- Ersetzen Sie Ihre Datenbank (oder * alle Datenbanken) durch *dev*.
- Ersetzen Sie den eindeutigen Bezeichner Ihrer IAM-Rolle durch *AROAJ2UCCR6DPCEXAMPLE*.
- Geben Sie anstelle von Ihre Mandanten- oder Unternehmens-E-Mail-Domäne ein *example.com*.
- Geben Sie anstelle von die Datenbankgruppe ein, der Sie den Benutzer zuweisen möchten *my_dbgroup*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "redshift:GetClusterCredentials",
            "Resource": [
                "arn:aws:redshift:us-west-1:123456789012:dbname:cluster-
identifier/dev",
                "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-identifier/
${redshift:DbUser}",
                "arn:aws:redshift:us-west-1:123456789012:cluster:cluster-
identifier"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:userid": "AROAJ2UCCR6DPCEXAMPLE:
${redshift:DbUser}@example.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "redshift:CreateClusterUser",
            "Resource": "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-
identifier/${redshift:DbUser}"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "redshift:JoinGroup",
            "Resource": "arn:aws:redshift:us-west-1:123456789012:dbgroup:cluster-
identifier/my_dbgroup"
        },
        {
            "Effect": "Allow",
            "Action": [
                "redshift:DescribeClusters",
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

Diese Richtlinie gewährt Berechtigungen wie folgt:

- Der erste Abschnitt erteilt der API-Operation `GetClusterCredentials` die Berechtigung, temporäre Anmeldeinformationen für den angegebenen Cluster abzurufen. In diesem Beispiel ist die Ressource *`cluster-identifier`* mit Datenbank *`dev`* im Konto *`123456789012`* und in AWS -Region *`us-west-1`*. Die Klausel `${redshift:DbUser}` ermöglicht es nur Benutzern, die dem in Azure AD angegebenen `DbUser`-Wert entsprechen, eine Verbindung herzustellen.
- Die Bedingungsklausel erzwingt, dass nur bestimmte Benutzer temporäre Anmeldeinformationen erhalten. Dies sind Benutzer unter der Rolle, die durch die eindeutige ID der Rolle *`AROAJ2UCCR6DPCEXAMPLE`* im IAM-Konto angegeben wird, das durch eine E-Mail-Adresse in der E-Mail-Domäne Ihres Unternehmens identifiziert wird. Weitere Informationen zu eindeutigen IDs finden Sie unter Eindeutige IDs im IAM-Benutzerhandbuch.

  Ihr Setup mit Ihrem IdP (in diesem Fall Azure AD) bestimmt, wie die Bedingungsklausel geschrieben wird. Wenn die E-Mail Ihres Mitarbeiters `johndoe@example.com` lautet, stellen Sie `${redshift:DbUser}` zuerst auf das Superfeld ein, das dem Benutzernamen `johndoe` des Mitarbeiters entspricht. Stellen Sie dann das AWS -SAML-Feld `RoleSessionName` auf das Superfeld ein, das mit der Mitarbeiter-E-Mail-Adresse `johndoe@example.com` übereinstimmt, damit diese Bedingung funktioniert. Berücksichtigen Sie bei diesem Ansatz Folgendes:

  - Wenn Sie `${redshift:DbUser}` als E-Mail des Mitarbeiters festlegen, entfernen Sie das `@example.com` im JSON-Beispiel,um dem `RoleSessionName` zu entsprechen.
  - Wenn Sie die `RoleSessionId` auf nur den Benutzernamen des Mitarbeiters eingestellt haben, entfernen Sie die `@example.com` im Beispiel, um dem `RoleSessionName` zu entsprechen.
  - Im JSON-Beispiel sind `${redshift:DbUser}` und `RoleSessionName` beide auf die E-Mail des Mitarbeiters festgelegt. In diesem JSON-Beispiel wird der Amazon-Redshift-Datenbankbenutzername mit `@example.com` verwendet, um den Benutzer für den Zugriff auf den Cluster anzumelden.
- Der zweite Abschnitt erteilt die Berechtigung zum Erstellen eines `dbuser`-Namens im angegebenen Cluster. In diesem Beispiel beschränkt JSON die Erstellung auf `${redshift:DbUser}`.
- Der dritte Abschnitt erteilt die Berechtigung zur Angabe, welcher `dbgroup` ein Benutzer beitreten kann. In diesem JSON-Beispiel kann ein Benutzer der Gruppe `my_dbgroup` im angegebenen Cluster beitreten.
- Der vierte Abschnitt berechtigt Aktionen, die der Benutzer für alle Ressourcen ausführen kann. In diesem JSON-Beispiel können Benutzer anrufen, `redshift:DescribeClusters` um Clusterinformationen wie den Cluster-Endpunkt, die AWS Region und den Port abzurufen. Auch ermöglicht es Benutzern, `iam:ListRoles` aufzurufen, um zu überprüfen, welche Rollen ein Benutzer übernehmen kann.

So richten Sie JDBC für die Authentifizierung bei Microsoft Azure AD ein:

- Konfigurieren Sie Ihren Datenbankclient für die Verbindung mit Ihrem Cluster über JDBC mithilfe von Azure AD Single Sign-On.

  Sie können jeden Client verwenden, der mithilfe eines JDBC-Treibers eine Verbindung mit Azure AD Single Sign-On herstellt oder eine Sprache wie Java verwendet, um über ein Skript eine Verbindung herzustellen. Informationen zur Installation und Konfiguration finden Sie unter Konfigurieren einer Verbindung für JDBC-Treiberversion 2.1 für Amazon Redshift.

  Sie können beispielsweise SQLWorkbench/J als Client verwenden. Wenn Sie SQLWorkbench/J konfigurieren, verwendet die URL Ihrer Datenbank das folgende Format.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

Wenn Sie SQLWorkbench/J als Client verwenden, führen Sie die folgenden Schritte aus:

a. Starten Sie SQL Workbench/J. Fügen Sie auf der Seite Select Connection Profile (Verbindungsprofil auswählen) eine Profile Group (Profilgruppe) namens **`AzureAuth`** hinzu.

b. Geben Sie für Connection Profile (Verbindungsprofil) **`Azure`** ein.

c. Wählen Sie Manage Drivers (Treiber verwalten) und dann Amazon Redshift aus. Wählen Sie das Symbol Open Folder (Ordner öffnen) neben Library (Bibliothek) und dann die entsprechende JDBC-JAR-Datei aus.

d. Fügen Sie auf der Seite Select Connection Profile (Verbindungsprofil auswählen) dem Verbindungsprofil Informationen wie folgt hinzu:

   - Geben Sie für User (Benutzer) Ihren Microsoft Azure-Benutzernamen ein. Dies ist der Benutzername des Microsoft Azure-Kontos, das Sie für die einmalige Anmeldung (Single-Sign-On) verwenden und das über die Berechtigung für den Cluster verfügt, für den Sie sich authentifizieren möchten.
   - Geben Sie für Password (Passwort) Ihr Microsoft Azure-Passwort ein.
   - Wählen Sie für Driver (Treiber) die Option Amazon Redshift (com.amazon.redshift.jdbc.Driver) aus.
   - Geben Sie für URL **`jdbc:redshift:iam://`*`your-cluster-identifier`*`:`*`your-cluster-region`*`/`*`your-database-name`* ein.

e. Wählen Sie Extended Properties (Erweiterte Eigenschaften), um den Verbindungseigenschaften wie folgt zusätzliche Informationen hinzuzufügen:

   Fügen Sie für die Single-Sign-On-Konfiguration von Azure AD zusätzliche Informationen wie folgt hinzu:

   - Geben Sie für plugin_name **`com.amazon.redshift.plugin.AzureCredentialsProvider`** ein. Dieser Wert gibt an, dass der Treiber Azure AD Single Sign-On als Authentifizierungsmethode verwenden soll.
   - Geben Sie für idp_tenant ***`your-idp-tenant`*** ein. Wird nur für Microsoft Azure AD verwendet. Dies ist der Mandantenname Ihres Unternehmens, der auf Ihrem Azure AD konfiguriert ist. Dieser Wert kann entweder der Mandantenname oder die eindeutige ID des Mandanten mit Bindestrichen sein.

- Geben Sie für client_secret ***your-azure-redshift-application-client-secret*** ein. Wird nur für Microsoft Azure AD verwendet. Dies ist Ihr Client-Secret der Amazon-Redshift-Anwendung, das Sie beim Einrichten der Azure-Single-Sign-On-Konfiguration erstellt haben. Dies gilt nur für das com.amazon.redshift.plugin. AzureCredentialsProvider Plugin.
- Geben Sie für client_id ***your-azure-redshift-application-client-id*** ein. Wird nur für Microsoft Azure AD verwendet. Dies ist die Client-ID (mit Bindestrichen) der Amazon-Redshift-Anwendung, die Sie beim Einrichten der Azure-Single-Sign-On-Konfiguration erstellt haben.

Fügen Sie für Single Sign-On von Azure AD mit MFA-Konfiguration den Verbindungseigenschaften wie folgt zusätzliche Informationen hinzu:

- Geben Sie für plugin_name **com.amazon.redshift.plugin.BrowserAzureCredentialsProvider** ein. Dies signalisiert dem Treiber, dass Single Sign-On für Azure AD mit MFA als Authentifizierungsmethode verwendet werden soll.
- Geben Sie für idp_tenant ***your-idp-tenant*** ein. Wird nur für Microsoft Azure AD verwendet. Dies ist der Mandantenname Ihres Unternehmens, der auf Ihrem Azure AD konfiguriert ist. Dieser Wert kann entweder der Mandantenname oder die eindeutige ID des Mandanten mit Bindestrichen sein.
- Geben Sie für client_id ***your-azure-redshift-application-client-id*** ein. Diese Option wird nur für Microsoft Azure AD verwendet. Dies ist die Client-ID (mit Bindestrichen) der Amazon-Redshift-Anwendung, die Sie beim Einrichten von Single Sign-On für Azure AD mit MFA-Konfiguration erstellt haben.
- Geben Sie bei listen_port „***your-listen-port***“ ein. Dies ist der Port, den der lokale Server überwacht. Der Standardwert ist 7890.
- Geben Sie für idp_response_timeout ***the-number-of-seconds*** ein. Dies ist die Anzahl der Sekunden, für die vor dem Timeout gewartet werden muss, wenn der IdP-Server eine Antwort zurücksendet. Die Mindestanzahl von Sekunden muss 10 sein. Wenn es länger dauert, eine Verbindung mit dem Server herzustellen, als durch diesen Schwellenwert angegeben, wird die Verbindung abgebrochen.

So richten Sie ODBC für die Authentifizierung bei Microsoft Azure AD ein:

- Konfigurieren Sie Ihren Datenbankclient für die Verbindung mit Ihrem Cluster über ODBC mithilfe von Azure AD Single Sign-On.

  Amazon Redshift stellt ODBC-Treiber für Linux-, Windows- und macOS-Betriebssysteme bereit. Stellen Sie vor der Installation eines ODBC-Treibers fest, ob Ihr SQL-Client-Tool 32-Bit oder 64-Bit ist. Installieren Sie den ODBC-Treiber, der den Anforderungen Ihres SQL-Clienttools entspricht.

  Installieren und konfigurieren Sie außerdem den neuesten Amazon-Redshift-ODBC-Treiber für Ihr Betriebssystem wie folgt:

  - Informationen für Windows finden Sie unter Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows.
  - Informationen zu macOS finden Sie unter Installieren des Amazon-Redshift-ODBC-Treibers unter macOS X.
  - Weitere Informationen für Linux finden Sie unter Installieren des Amazon-Redshift-ODBC-Treibers unter Linux.

  Geben Sie unter Windows auf der Seite Amazon Redshift ODBC Driver DSN Setup (DSN-Setup für Amazon Redshift ODBC-Treiber) unter Connection Settings (Verbindungseinstellungen) die folgenden Informationen ein:

  - Geben Sie für Data Source Name (Datenquellenname) ***your-DSN*** ein. Dies gibt den Datenquellennamen an, der als ODBC-Profilname verwendet wird.
  - Wählen Sie für die Single-Sign-On-Konfiguration von Azure AD unter Auth type (Authentifizierungstyp) **`Identity Provider: Azure AD`** aus. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung mit Azure Single Sign-On verwendet.
  - Wählen Sie für die Single-Sign-On-Konfiguration von Azure AD mit MFA-Konfiguration unter Auth type (Authentifizierungstyp) **`Identity Provider: Browser Azure AD`** aus. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung mit Azure Single Sign-On mit MFA verwendet.
  - Geben Sie für Cluster ID (Cluster-ID) ***your-cluster-identifier*** ein.
  - Geben Sie für Region ***your-cluster-region*** ein.

- Geben Sie für Database (Datenbank) ***your-database-name*** ein.
- Geben Sie für User (Benutzer) ***your-azure-username*** ein. Dies ist der Benutzername des Microsoft Azure-Kontos, das Sie für die einmalige Anmeldung (Single-Sign-On) verwenden und das über die Berechtigung für den Cluster verfügt, für den Sie sich authentifizieren möchten. Verwenden Sie dies nur, wenn Auth Type (Authentifizierungstyp) Identity Provider: Azure AD (Identitätsanbieter: Azure AD) ist.
- Geben Sie unter Password (Passwort) ***your-azure-password*** ein. Verwenden Sie dies nur, wenn Auth Type (Authentifizierungstyp) Identity Provider: Azure AD (Identitätsanbieter: Azure AD) ist.
- Geben Sie für IdP Tenant (IdP-Mandant) ***your-idp-tenant*** ein. Dies ist der Mandantenname Ihres Unternehmens, der auf Ihrem IdP (Azure) konfiguriert ist. Dieser Wert kann entweder der Mandantenname oder die eindeutige ID des Mandanten mit Bindestrichen sein.
- Geben Sie für Azure Client Secret (Azure-Clientgeheimnis) ***your-azure-redshift-application-client-secret*** ein. Dies ist das Client-Secret der Amazon-Redshift-Anwendung, das Sie beim Einrichten der Azure-Single-Sign-On-Konfiguration erstellt haben.
- Geben Sie für Azure Client ID (Azure-Client-ID) ***your-azure-redshift-application-client-id*** ein. Dies ist die Client-ID (mit Bindestrichen) der Amazon-Redshift-Anwendung, die Sie beim Einrichten der Azure-Single-Sign-On-Konfiguration erstellt haben.
- Geben Sie als Listen Port „***your-listen-port***“ ein. Dies ist der standardmäßige Listening-Port, den der lokale Server überwacht. Der Standardwert ist 7890. Dies gilt nur für das Browser Azure AD-Plug-in.
- Geben Sie für Response Timeout (Antwortzeitüberschreitung) ***the-number-of-seconds*** ein. Dies ist die Anzahl der Sekunden, für die vor dem Timeout gewartet werden muss, wenn der IdP-Server eine Antwort zurücksendet. Die Mindestanzahl von Sekunden muss 10 sein. Wenn es länger dauert, eine Verbindung mit dem Server herzustellen, als durch diesen Schwellenwert angegeben, wird die Verbindung abgebrochen. Dies gilt nur für das Browser-Azure-AD-Plug-In.

Bearbeiten Sie die `odbc.ini`-Datei unter Mac OS und Linux wie folgt:

> **Note**
>
> Bei allen Eingaben wird zwischen Groß- und Kleinschreibung unterschieden.

- Geben Sie für clusterid ***your-cluster-identifier*** ein. Dies ist der Name des erstellten Amazon-Redshift-Clusters.
- Geben Sie für Region ***your-cluster-region*** ein. Dies ist die AWS Region des erstellten Amazon Redshift Redshift-Clusters.
- Geben Sie für die database ***your-database-name*** ein. Dies ist der Name der Datenbank, auf die Sie im Amazon-Redshift-Cluster zugreifen möchten.
- Geben Sie für locale **en-us** ein. Dies ist die Sprache, in der Fehlermeldungen angezeigt werden.
- Geben Sie für iam **1** ein. Dieser Wert signalisiert dem Treiber, dass mit IAM-Anmeldeinformationen authentifiziert werden soll.
- Geben Sie für die Single-Sign-On-Konfiguration von Azure AD im Feld plugin_name **AzureAD** ein. Dies signalisiert dem Treiber, Azure Single Sign-On als Authentifizierungsmethode zu verwenden.
- Geben Sie für Single Sign-On von Azure AD mit MFA-Konfiguration im Feld plugin_name **BrowserAzureAD** ein. Dies signalisiert dem Treiber, dass Azure Single Sign-On mit MFA als Authentifizierungsmethode verwendet werden soll.
- Geben Sie für uid ***your-azure-username*** ein. Dies ist der Benutzername des Microsoft Azure-Kontos, das Sie für die einmalige Anmeldung (Single-Sign-On) verwenden und das über die Berechtigung für den Cluster verfügt, für den Sie sich authentifizieren möchten. Verwenden Sie dies nur, wenn der plugin_name AzureAd ist.
- Geben Sie für pwd ***your-azure-password*** ein. Verwenden Sie dies nur, wenn der plugin_name AzureAd ist.
- Geben Sie für idp_tenant ***your-idp-tenant*** ein. Dies ist der Mandantenname Ihres Unternehmens, der auf Ihrem IdP (Azure) konfiguriert ist. Dieser Wert kann entweder der Mandantenname oder die eindeutige ID des Mandanten mit Bindestrichen sein.
- Geben Sie für client_secret ***your-azure-redshift-application-client-secret*** ein. Dies ist das Client-Secret der Amazon-Redshift-Anwendung, das Sie beim Einrichten der Azure-Single-Sign-On-Konfiguration erstellt haben.
- Geben Sie für client_id ***your-azure-redshift-application-client-id*** ein. Dies ist die Client-ID (mit Bindestrichen) der Amazon-Redshift-Anwendung, die Sie beim Einrichten der Azure-Single-Sign-On-Konfiguration erstellt haben.
- Geben Sie bei listen_port „***your-listen-port***“ ein. Dies ist der Port, den der lokale Server überwacht. Der Standardwert ist 7890. Dies gilt für das Browser Azure AD-Plug-in.

- Geben Sie für idp_response_timeout ***the-number-of-seconds*** ein. Dies ist der angegebene Zeitraum in Sekunden, für den auf die Antwort von Azure gewartet werden soll. Diese Option gilt für das Browser-Azure-AD-Plug-In.

Bearbeiten Sie unter macOS und Linux auch die Profileinstellungen, um folgende Exporte hinzuzufügen:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

So beheben Sie Probleme mit dem Browser-Azure AD-Plug-in

1. Zur Verwendung des Browser-Azure AD-Plug-ins müssen Sie die in der Anforderung angegebene Antwort-URL so festlegen, dass sie mit der für Ihre Anwendung konfigurierten Antwort-URL übereinstimmt.

   Navigieren Sie im Microsoft Azure-Portal zur Seite Set up Single Sign-On with SAML (Single Sign-On mit SAML einrichten). Überprüfen Sie dann, ob der Wert unter Reply URL (Antwort-URL) auf „http://localhost/redshift/“ festgelegt ist.
2. Wenn Sie einen IdP-Mandantenfehler erhalten, überprüfen Sie, ob der Name unter IdP Tenant (IdP-Mandant mit dem Domänennamen übereinstimmt, den Sie ursprünglich zum Einrichten von Active Directory in Microsoft Azure verwendet haben.

   Navigieren Sie unter Windows zum Bereich Connection Settings (Verbindungseinstellungen) der Seite Amazon Redshift ODBC DSN Setup (DSN-Einrichtung von Amazon-Redshift-ODBC). Überprüfen Sie dann, ob der für den IdP (Azure) konfigurierte Mandantenname Ihres Unternehmens mit dem Domänennamen übereinstimmt, den Sie ursprünglich zum Einrichten von Active Directory in Microsoft Azure verwendet haben.

   Suchen Sie unter macOS und Linux die Datei odbc.ini. Überprüfen Sie dann, ob der für den IdP (Azure) konfigurierte Mandantenname Ihres Unternehmens mit dem Domänennamen übereinstimmt, den Sie ursprünglich zum Einrichten von Active Directory in Microsoft Azure verwendet haben.

3. Wenn Sie einen Fehler erhalten, dass die in der Anforderung angegebene Antwort-URL nicht mit den für Ihre Anwendung konfigurierten Antwort-URLs übereinstimmt, überprüfen Sie, ob die Redirect URIs (Umleitungs-URIs) mit der Antwort-URL übereinstimmen.

   Navigieren Sie im Microsoft Azure-Portal zur Seite App registration (App-Registrierung) Ihrer Anwendung. Überprüfen Sie dann, ob die Umleitungs-URIs mit der Antwort-URL übereinstimmen.
4. Wenn Sie einen unerwarteten Fehler wegen fehlender Autorisierung erhalten, überprüfen Sie, ob Sie die Konfiguration der Mobil- und Desktopanwendungen abgeschlossen haben.

   Navigieren Sie im Microsoft Azure-Portal zur Seite App registration (App-Registrierung) Ihrer Anwendung. Navigieren Sie dann zu Authentication (Authentifizierung) und überprüfen Sie, ob Sie die Mobil- und Desktopanwendungen für die Verwendung von „http://localhost/redshift/“ als Umleitungs-URIs konfiguriert haben.

Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit AD FS

Sie können AD FS als Identitätsanbieter (IdP) verwenden, um auf Ihren Amazon-Redshift-Cluster zuzugreifen. Im Anschluss finden Sie eine Prozedur, die beschreibt, wie Sie eine Vertrauensstellung für diesen Zweck einrichten. Weitere Informationen zur Konfiguration AWS als Service Provider für AD FS finden Sie unter Configuring Your SAML 2.0 IdP with Relying Party Trust und Adding Claims im IAM-Benutzerhandbuch.

So richten Sie AD FS und Ihr AWS Konto so ein, dass sie sich gegenseitig vertrauen

1. Erstellen oder verwenden Sie einen vorhandenen Amazon-Redshift-Cluster, mit dem sich Ihre AD-FS-Benutzer verbinden können. Um die Verbindung zu konfigurieren, werden bestimmte Eigenschaften dieses Clusters benötigt, z. B. die Clusterkennung. Weitere Informationen finden Sie unter Erstellen eines Clusters.
2. Richten Sie AD FS ein, um den Amazon-Redshift-Zugriff auf die Microsoft Management Console zu steuern:

   1. Wählen Sie ADFS 2.0 und dann Add relying Party Trust (Vertrauensstellung von vertrauender Partei hinzufügen). Wählen Sie auf der Seite Add Relying Party Trust Wizard (Assistent zum Hinzufügen vertrauender Parteien) die Option Start.
   2. Wählen Sie auf der Seite Select Data Source (Datenquelle auswählen) die Option Import data about the relying party published online or on a local network (Online oder im lokalen Netzwerk veröffentlichte Daten über die vertrauende Partei importieren).

3. Geben Sie für Federation metadata address (host name or URL) (Verbundmetadatenadresse (Hostname oder URL)) **`https://signin.aws.amazon.com/saml-metadata.xml`** ein. Bei der XML-Metadatendatei handelt es sich um ein standardmäßiges SAML-Metadatendokument, das AWS als vertrauende Partei bezeichnet wird.
4. Geben Sie auf der Seite Specify Display Name (Anzeigename angeben) einen Wert für Display name (Anzeigename) ein.
5. Wählen Sie auf der Seite Choose Issuance Authorization Rules (Ausgabeautorisierungsregeln auswählen)eine Ausgabeautorisierungsregel aus, um allen Benutzern den Zugriff auf diese vertrauende Partei zu erlauben oder zu verweigern.
6. Überprüfen Sie auf der Seite Ready to Add trust (Bereit zum Hinzufügen von Vertrauensstellungen) Ihre Einstellungen.
7. Wählen Sie auf der Seite Finish (Fertig stellen) die Option Open the Edit Claim Rules dialog for this relying party trust when the wizard closes (Nach Abschluss des Assistenten das Dialogfeld „Antragsregeln bearbeiten“ für diese Vertrauensstellung der vertrauenden Seite öffnen).
8. Wählen Sie im Kontextmenü (Rechtsklick) Relying Party Trusts (Vertrauensstellungen von vertrauenden Parteien).
9. Öffnen Sie für Ihre vertrauende Partei das Kontextmenü (Rechtsklick), und wählen Sie Edit Claim Rules (Antragsregeln bearbeiten). Wählen Sie auf der Seite Edit Claim Rules (Antragsregeln bearbeiten) die Option Add Rule (Regel hinzufügen).
10. Wählen Sie als Vorlage für eine Forderungsregel die Option Eingehenden Anspruch transformieren aus, und gehen Sie dann auf der NameId Seite Regel bearbeiten — wie folgt vor:
    - Geben Sie als Namen der Anspruchsregel Folgendes ein NameId.
    - Wählen Sie unter Incoming claim name (Name des eingehenden Antrags) die Option Windows Account Name (Windows-Kontoname).
    - Wählen Sie unter Outgoing claim name (Name des ausgehenden Antrags) die Option Name ID.
    - Wählen Sie unter Outgoing name ID format (Format der ausgehenden Namens-ID) die Option Persistent identifier (Persistente ID).
    - Wählen Sie Pass through all claim values (Alle Antragswerte durchleiten).
11. Wählen Sie auf der Seite Edit Claim Rules (Antragsregeln bearbeiten) die Option Add Rule (Regel hinzufügen). Wählen Sie auf der Seite Select Rule Template (Regelvorlage auswählen)

für Claim rule template (Antragsregelvorlage) die Option Send LDAP Attributes as Claims (LDAP-Attribute als Anträge senden).

12. Führen Sie auf der Seite Configure Rule (Regel konfigurieren) die folgenden Schritte aus:
    - Geben Sie unter Claim rule name (Name der Antragsregel) RoleSessionName ein.
    - Wählen Sie unter Attribute store (Attributspeicher) Active Directory.
    - Wählen Sie für LDAP Attribute (LDAP-Attribut) Email Addresses (E-Mail-Adressen).
    - Wählen Sie bei Outgoing Claim Type (Art des ausgehenden Anspruchs) https://aws.amazon.com/SAML/Attributes/RoleSessionName aus.
13. Wählen Sie auf der Seite Edit Claim Rules (Antragsregeln bearbeiten) die Option Add Rule (Regel hinzufügen). Wählen Sie auf der Seite Select Rule Template (Regelvorlage auswählen) für Claim rule template (Antragsregelvorlage) die Option Send Claims Using a Custom Rule (Anträge mit benutzerdefinierter Regel senden).
14. Geben Sie auf der Seite Edit Rule – Get AD Groups (Regel bearbeiten – AD-Gruppen abrufen) für Claim rule name (Name der Antragsregel) Get AD Groups (AD-Gruppen abrufen) ein.
15. Geben Sie unter Custom rule (Benutzerdefinierte Regel) Folgendes ein.

```
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. Wählen Sie auf der Seite Edit Claim Rules (Antragsregeln bearbeiten) die Option Add Rule (Regel hinzufügen). Wählen Sie auf der Seite Select Rule Template (Regelvorlage auswählen) für Claim rule template (Antragsregelvorlage) die Option Send Claims Using a Custom Rule (Anträge mit benutzerdefinierter Regel senden).
17. Geben Sie auf der Seite Edit Rule - Roles (Regel bearbeiten — Rollen) für Claim rule name Namen der Antragsregel Roles (Rollen) ein.
18. Geben Sie unter Custom rule (Benutzerdefinierte Regel) Folgendes ein.

```
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-"));
```

Beachten Sie die ARNs des SAML-Anbieters und der zu übernehmenden Rolle. In diesem Beispiel ist `arn:aws:iam:123456789012:saml-provider/ADFS` der ARN des SAML-Providers und `arn:aws:iam:123456789012:role/ADFS-` der ARN der Rolle.

3. Stellen Sie sicher, dass Sie die `federationmetadata.xml`-Datei heruntergeladen haben. Überprüfen Sie, dass der Dokumentinhalt keine ungültigen Zeichen enthält. Dies ist die Metadatendatei, mit der Sie die Vertrauensstellung konfigurieren AWS.
4. Erstellen Sie auf der IAM-Konsole einen IAM SAML-Identitätsanbieter. Das Metadatendokument, das Sie bereitstellen, ist die XML-Datei mit Verbundmetadaten, die Sie beim Einrichten der Azure Enterprise-Anwendung gespeichert haben. Ausführliche Schritte finden Sie unter Erstellen und Verwalten eines IAM-Identitätsanbieters (Konsole) im IAM-Benutzerhandbuch.
5. Erstellen Sie auf der IAM-Konsole eine IAM-Rolle für SAML 2.0-Verbund. Detaillierte Schritte finden Sie unter Erstellen einer Rolle für SAML im IAM-Benutzerhandbuch.
6. Erstellen Sie eine IAM-Richtlinie, die Sie an die IAM-Rolle anhängen können, die Sie für den SAML 2.0-Verbund auf der IAM-Konsole erstellt haben. Ausführliche Schritte finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch. Ein Azure AD-Beispiel finden Sie unter Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit Microsoft Azure AD.

So richten Sie JDBC für die Authentifizierung bei AD FS ein:

- Konfigurieren Sie Ihren Datenbank-Client für die Verbindung mit Ihrem Cluster über JDBC mithilfe von AD FS Single Sign-On.

  Sie können jeden Client verwenden, der mithilfe eines JDBC-Treibers eine Verbindung mit AD FS Single Sign-On herstellt oder eine Sprache wie Java verwendet, um über ein Skript eine Verbindung herzustellen. Informationen zur Installation und Konfiguration finden Sie unter Konfigurieren einer Verbindung für JDBC-Treiberversion 2.1 für Amazon Redshift.

  Sie können beispielsweise SQLWorkbench/J als Client verwenden. Wenn Sie SQLWorkbench/J konfigurieren, verwendet die URL Ihrer Datenbank das folgende Format.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Wenn Sie SQLWorkbench/J als Client verwenden, führen Sie die folgenden Schritte aus:

a. Starten Sie SQL Workbench/J. Fügen Sie auf der Seite Select Connection Profile (Verbindungsprofil auswählen) eine Profile Group (Profilgruppe) hinzu, z. B. **`ADFS`**.

b. Geben Sie unter Connection Profile (Verbindungsprofil) Ihren Verbindungsprofilnamen ein, z. B. **`ADFS`**.

c. Wählen Sie Manage Drivers (Treiber verwalten) und dann Amazon Redshift aus. Wählen Sie das Symbol Open Folder (Ordner öffnen) neben Library (Bibliothek) und dann die entsprechende JDBC-JAR-Datei aus.

d. Fügen Sie auf der Seite Select Connection Profile (Verbindungsprofil auswählen) dem Verbindungsprofil Informationen wie folgt hinzu:

   - Geben Sie unter User (Benutzer) Ihren AD FS-Benutzernamen ein. Dies ist der Benutzername des -Kontos, das Sie für die einmalige Anmeldung (Single-Sign-On) verwenden, und das über die Berechtigung für den Cluster verfügt, für den Sie sich authentifizieren möchten.
   - Geben Sie unter Password (Passwort) Ihr AD FS-Passwort ein.
   - Wählen Sie für Driver (Treiber) die Option Amazon Redshift (com.amazon.redshift.jdbc.Driver) aus.
   - Geben Sie für URL **`jdbc:redshift:iam://`*`your-cluster-identifier`*`:`*`your-cluster-region`*`/`*`your-database-name`* ein.

e. Wählen Sie Extended Properties (Erweiterte Eigenschaften) aus. Geben Sie für plugin_name **`com.amazon.redshift.plugin.AdfsCredentialsProvider`** ein. Dieser Wert gibt an, dass der Treiber AD FS Single Sign-On als Authentifizierungsmethode verwenden soll.

So richten Sie ODBC für die Authentifizierung bei AD FS ein:

- Konfigurieren Sie Ihren Datenbank-Client für die Verbindung mit Ihrem Cluster über ODBC mithilfe von AD FS Single Sign-On.

  Amazon Redshift stellt ODBC-Treiber für Linux-, Windows- und macOS-Betriebssysteme bereit. Stellen Sie vor der Installation eines ODBC-Treibers fest, ob Ihr SQL-Client-Tool 32-Bit oder 64-Bit ist. Installieren Sie den ODBC-Treiber, der den Anforderungen Ihres SQL-Clienttools entspricht.

Installieren und konfigurieren Sie außerdem den neuesten Amazon-Redshift-ODBC-Treiber für Ihr Betriebssystem wie folgt:

- Informationen für Windows finden Sie unter Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows.
- Informationen zu macOS finden Sie unter Installieren des Amazon-Redshift-ODBC-Treibers unter macOS X.
- Weitere Informationen für Linux finden Sie unter Installieren des Amazon-Redshift-ODBC-Treibers unter Linux.

Geben Sie unter Windows auf der Seite Amazon Redshift ODBC Driver DSN Setup (DSN-Setup für Amazon Redshift ODBC-Treiber) unter Connection Settings (Verbindungseinstellungen) die folgenden Informationen ein:

- Geben Sie für Data Source Name (Datenquellenname) ***your-DSN*** ein. Dies gibt den Datenquellennamen an, der als ODBC-Profilname verwendet wird.
- Wählen Sie bei Auth type (Authentifizierungstyp) Identity Provider: SAML (Identitätsanbieter: SAML) aus. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung mit AD FS Single Sign-On verwendet.
- Geben Sie für Cluster ID (Cluster-ID) ***your-cluster-identifier*** ein.
- Geben Sie für Region ***your-cluster-region*** ein.
- Geben Sie für Database (Datenbank) ***your-database-name*** ein.
- Geben Sie für User (Benutzer) ***your-adfs-username*** ein. Dies ist der Benutzername des AD-FS-Kontos, das Sie für Single Sign-On verwenden und das über die Berechtigung für den Cluster verfügt, für den Sie sich authentifizieren möchten. Verwenden Sie dies nur, wenn Auth type (Authentifizierungstyp) Identity Provider: SAML (Identitätsanbieter: SAML) ist.
- Geben Sie unter Password (Passwort) ***your-adfs-password*** ein. Verwenden Sie dies nur, wenn Auth type (Authentifizierungstyp) Identity Provider: SAML (Identitätsanbieter: SAML) ist.

Bearbeiten Sie die `odbc.ini`-Datei unter Mac OS und Linux wie folgt:

> **Note**
>
> Bei allen Eingaben wird zwischen Groß- und Kleinschreibung unterschieden.

- Geben Sie für clusterid ***your-cluster-identifier*** ein. Dies ist der Name des erstellten Amazon-Redshift-Clusters.
- Geben Sie für Region ***your-cluster-region*** ein. Dies ist die AWS Region des erstellten Amazon Redshift Redshift-Clusters.
- Geben Sie für die database ***your-database-name*** ein. Dies ist der Name der Datenbank, auf die Sie im Amazon-Redshift-Cluster zugreifen möchten.
- Geben Sie für locale **`en-us`** ein. Dies ist die Sprache, in der Fehlermeldungen angezeigt werden.
- Geben Sie für iam **1** ein. Dieser Wert signalisiert dem Treiber, dass mit IAM-Anmeldeinformationen authentifiziert werden soll.
- Führen Sie für plugin_name einen der folgenden Schritte aus:
  - Geben Sie für Single Sign-On von AD FS mit MFA-Konfiguration **`BrowserSAML`** ein. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung bei AD FS verwendet.
  - Geben Sie für die Single-Sign-On-Konfiguration von AD FS **`ADFS`** ein. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung mit Azure AD Single Sign-On verwendet.
- Geben Sie für uid ***your-adfs-username*** ein. Dies ist der Benutzername des Microsoft-Azure-Kontos, das Sie für Single-Sign-On verwenden und das über die Berechtigung für den Cluster verfügt, für den Sie sich authentifizieren möchten. Verwenden Sie dies nur, wenn der plugin_name (Plug-In-Name) ADFS ist.
- Geben Sie für pwd ***your-adfs-password*** ein. Verwenden Sie dies nur, wenn der plugin_name (Plug-In-Name) ADFS ist.

Bearbeiten Sie unter macOS und Linux auch die Profileinstellungen, um folgende Exporte hinzuzufügen:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Einrichten der Single-Sign-On-Authentifizierung über JDBC oder ODBC mit Ping Identity

Sie können Ping Identity als Identitätsanbieter (IdP) verwenden, um auf Ihren Amazon-Redshift-Cluster zuzugreifen. Im Folgenden finden Sie ein Verfahren, das beschreibt, wie Sie zu diesem Zweck über das PingOne Portal eine Vertrauensbeziehung einrichten können. Weitere Informationen zur Konfiguration AWS als Service Provider für Ping Identity finden Sie unter Configuring Your SAML 2.0 IdP with Relying Party Trust and Adding Claims im IAM-Benutzerhandbuch.

So richten Sie Ping Identity und Ihr AWS Konto so ein, dass sie sich gegenseitig vertrauen

1. Erstellen oder verwenden Sie einen vorhandenen Amazon-Redshift-Cluster, mit dem Ihre Ping-Identity-Benutzer eine Verbindung herstellen können. Um die Verbindung zu konfigurieren, werden bestimmte Eigenschaften dieses Clusters benötigt, z. B. die Clusterkennung. Weitere Informationen finden Sie unter Erstellen eines Clusters.
2. Fügen Sie Amazon Redshift als neue SAML-Anwendung im PingOne Portal hinzu. Ausführliche Schritte finden Sie in der Ping Identity-Dokumentation.
    1. Wechseln Sie zu My Applications (Meine Anwendungen).
    2. Wählen Sie unter Add Application (Anwendung hinzufügen) die Option New SAML Application (Neue SAML-Anwendung).
    3. Geben Sie unter Application name (Anwendungsname) **`Amazon Redshift`** ein.
    4. Wählen Sie für Protocol Version (Protokollversion) SAML v2.0.
    5. Wählen Sie unter Category (Kategorie) ***`your-application-category`*** aus.
    6. Geben Sie für Assertion Consumer Service (ACS) ***`your-redshift-local-host-url`*** ein. Dies ist der lokale Host und Port, auf den die SAML-Zusicherung umgeleitet wird.
    7. Geben Sie für Entity ID (Entitäts-ID) `urn:amazon:webservices` ein.
    8. Wählen Sie für Signing (Signieren) die Option Sign Assertion (Zusicherung signieren).
    9. Erstellen Sie im Abschnitt SSO Attribute Mapping (SSO-Attributzuweisung) die Anträge wie in der folgenden Tabelle dargestellt.

Anwendungsattribut	Identity Bridge-Attribut des Literalwerts
https://aws.amazon.com/SAML/Attributes/Role	*`arn:aws:iam:: 123456789012:role/ Ping, arn:aws:iam:: 123456789012:saml-provider/ PingProvider`*

Anwendungsattribut	Identity Bridge-Attribut des Literalwerts
https://aws.amazon.com/SAML/Attributes/RoleSessionName	email
https://redshift.amazon.com/SAML/Attributes/AutoCreate	„true“
https://redshift.amazon.com/SAML/Attributes/ DbUser	email
https://redshift.amazon.com/SAML/Attributes/ DbGroups	Die Gruppen in den Attributen „DbGroups “ enthalten das Präfix @directory. Um es zu entfernen, geben Sie bei Identity bridge memberOf ein. Wählen Sie unter Funktion die Option ExtractByRegularExpression. Geben Sie bei Expression (Ausdruck) (.*) [\@](?:.*) ein.

3. Richten Sie unter Group Access (Gruppenzugriff) bei Bedarf den folgenden Gruppenzugriff ein:
   - 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. Überprüfen Sie Ihre Einrichtung und nehmen Sie Änderungen vor, wenn notwendig.
5. Verwenden Sie die Initiate Single Sign-On (SSO) URL als Anmelde-URL für das Browser-SAML-Plug-in.
6. Erstellen Sie auf der IAM-Konsole einen IAM SAML-Identitätsanbieter. Das Metadatendokument, das Sie bereitstellen, ist die XML-Datei für Verbundmetadaten, die Sie beim Einrichten von Ping Identity gespeichert haben. Ausführliche Schritte finden Sie unter Erstellen und Verwalten eines IAM-Identitätsanbieters (Konsole) im IAM-Benutzerhandbuch.
7. Erstellen Sie auf der IAM-Konsole eine IAM-Rolle für SAML 2.0-Verbund. Detaillierte Schritte finden Sie unter Erstellen einer Rolle für SAML im IAM-Benutzerhandbuch.
8. Erstellen Sie eine IAM-Richtlinie, die Sie an die IAM-Rolle anhängen können, die Sie für den SAML 2.0-Verbund auf der IAM-Konsole erstellt haben. Ausführliche Schritte finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch. Ein Azure AD-Beispiel finden

Sie unter Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit Microsoft Azure AD.

So richten Sie JDBC für die Authentifizierung bei Ping Identity ein:

- Konfigurieren Sie Ihren Datenbank-Client für die Verbindung mit Ihrem Cluster über JDBC mithilfe von Single Sign-On mit Ping Identity.

  Sie können jeden Client verwenden, der mithilfe eines JDBC-Treibers eine Verbindung mit Single Sign-On mit Ping Identity herstellt oder eine Sprache wie Java verwendet, um über ein Skript eine Verbindung herzustellen. Informationen zur Installation und Konfiguration finden Sie unter Konfigurieren einer Verbindung für JDBC-Treiberversion 2.1 für Amazon Redshift.

  Sie können beispielsweise SQLWorkbench/J als Client verwenden. Wenn Sie SQLWorkbench/J konfigurieren, verwendet die URL Ihrer Datenbank das folgende Format.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Wenn Sie SQLWorkbench/J als Client verwenden, führen Sie die folgenden Schritte aus:

  a. Starten Sie SQL Workbench/J. Fügen Sie auf der Seite Select Connection Profile (Verbindungsprofil auswählen) eine Profile Group (Profilgruppe) hinzu, z. B. **`Ping`**.

  b. Geben Sie unter Connection Profile (Verbindungsprofil) ***`your-connection-profile-name`*** ein, z. B. **`Ping`**.

  c. Wählen Sie Manage Drivers (Treiber verwalten) und dann Amazon Redshift aus. Wählen Sie das Symbol Open Folder (Ordner öffnen) neben Library (Bibliothek) und dann die entsprechende JDBC-JAR-Datei aus.

  d. Fügen Sie auf der Seite Select Connection Profile (Verbindungsprofil auswählen) dem Verbindungsprofil Informationen wie folgt hinzu:

     - Geben Sie unter Benutzer Ihren PingOne Benutzernamen ein. Dies ist der Benutzername des PingOne Kontos, das Sie für Single Sign-On verwenden und das über Berechtigungen für den Cluster verfügt, mit dem Sie sich authentifizieren möchten.
     - Geben Sie unter Passwort Ihr PingOne Passwort ein.
     - Wählen Sie für Driver (Treiber) die Option Amazon Redshift (com.amazon.redshift.jdbc.Driver) aus.

- Geben Sie für URL **jdbc:redshift:iam://*your-cluster-identifier*:*your-cluster-region*/*your-database-name*** ein.

e. Wählen Sie Extended Properties (Erweiterte Eigenschaften), und führen Sie einen der folgenden Schritte aus:

- Geben Sie für login_url ***your-ping-sso-login-url*** ein. Dieser Wert gibt die URL an, die Single Sign-On als Authentifizierungsmethode für die Anmeldung verwenden soll.
- Geben Sie bei Ping Identity für plugin_name **com.amazon.redshift.plugin.PingCredentialsProvider** ein. Dieser Wert gibt an, dass der Treiber Single Sign-On mit Ping Identity als Authentifizierungsmethode verwenden soll.
- Geben Sie für Ping Identity mit Single Sign-On im Feld plugin_name **com.amazon.redshift.plugin.BrowserSamlCredentialsProvider** ein. Dieser Wert gibt dem Treiber an, Ping Identity PingOne mit Single Sign-On als Authentifizierungsmethode zu verwenden.

So richten Sie ODBC für die Authentifizierung bei Ping Identity ein:

- Konfigurieren Sie Ihren Datenbankclient so, dass er mithilfe von Ping Identity PingOne Single Sign-On über ODBC eine Verbindung zu Ihrem Cluster herstellt.

  Amazon Redshift stellt ODBC-Treiber für Linux-, Windows- und macOS-Betriebssysteme bereit. Stellen Sie vor der Installation eines ODBC-Treibers fest, ob Ihr SQL-Client-Tool 32-Bit oder 64-Bit ist. Installieren Sie den ODBC-Treiber, der den Anforderungen Ihres SQL-Clienttools entspricht.

  Installieren und konfigurieren Sie außerdem den neuesten Amazon-Redshift-ODBC-Treiber für Ihr Betriebssystem wie folgt:

  - Informationen für Windows finden Sie unter Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows.
  - Informationen zu macOS finden Sie unter Installieren des Amazon-Redshift-ODBC-Treibers unter macOS X.
  - Weitere Informationen für Linux finden Sie unter Installieren des Amazon-Redshift-ODBC-Treibers unter Linux.

Geben Sie unter Windows auf der Seite Amazon Redshift ODBC Driver DSN Setup (DSN-Setup für Amazon Redshift ODBC-Treiber) unter Connection Settings (Verbindungseinstellungen) die folgenden Informationen ein:

- Geben Sie für Data Source Name (Datenquellenname) ***your-DSN*** ein. Dies gibt den Datenquellennamen an, der als ODBC-Profilname verwendet wird.
- Führen Sie für Auth type (Authentifizierungstyp) eine der folgenden Aktionen aus:
  - Wählen Sie für die Ping Identity-Konfiguration Identitätsanbieter: Ping Federate aus. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung mit Single Sign-On mit Ping Identity verwendet.
  - Wählen Sie für Ping Identity mit Single-Sign-On-Konfiguration Identity Provider: Browser SAML (Identitätsanbieter: Browser SAML) aus. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung mit Single Sign-On mit Ping Identity verwendet.
- Geben Sie für Cluster ID (Cluster-ID) ***your-cluster-identifier*** ein.
- Geben Sie für Region ***your-cluster-region*** ein.
- Geben Sie für Database (Datenbank) ***your-database-name*** ein.
- Geben Sie für User (Benutzer) ***your-ping-username*** ein. Dies ist der Benutzername für das PingOne Konto, das Sie für Single Sign-On verwenden und das über Berechtigungen für den Cluster verfügt, mit dem Sie sich authentifizieren möchten. Verwenden Sie dies nur für den Authentifizierungstyp Identity Provider:. PingFederate
- Geben Sie unter Password (Passwort) ***your-ping-password*** ein. Verwenden Sie dies nur für den Authentifizierungstyp Identity Provider:. PingFederate
- Geben Sie als Listen Port „***your-listen-port***“ ein. Dies ist der Port, den der lokale Server überwacht. Der Standardwert ist 7890. Dies gilt nur für das Browser SAML-Plug-in.
- Geben Sie für Response Timeout (Antwortzeitüberschreitung) ***the-number-of-seconds*** ein. Dies ist die Anzahl der Sekunden, für die vor dem Timeout gewartet werden muss, wenn der IdP-Server eine Antwort zurücksendet. Die Mindestanzahl von Sekunden muss 10 sein. Wenn es länger dauert, eine Verbindung mit dem Server herzustellen, als durch diesen Schwellenwert angegeben, wird die Verbindung abgebrochen. Dies gilt nur für das Browser SAML-Plug-in.
- Geben Sie unter Login-URL (Anmelde-URL) ***your-login-url*** ein. Dies gilt nur für das Browser SAML-Plug-in.

Bearbeiten Sie die `odbc.ini`-Datei unter Mac OS und Linux wie folgt:

> **Note**
>
> Bei allen Eingaben wird zwischen Groß- und Kleinschreibung unterschieden.

- Geben Sie für clusterid ***your-cluster-identifier*** ein. Dies ist der Name des erstellten Amazon-Redshift-Clusters.
- Geben Sie für Region ***your-cluster-region*** ein. Dies ist die AWS Region des erstellten Amazon Redshift Redshift-Clusters.
- Geben Sie für die database ***your-database-name*** ein. Dies ist der Name der Datenbank, auf die Sie im Amazon-Redshift-Cluster zugreifen möchten.
- Geben Sie für locale **`en-us`** ein. Dies ist die Sprache, in der Fehlermeldungen angezeigt werden.
- Geben Sie für iam **1** ein. Dieser Wert signalisiert dem Treiber, dass mit IAM-Anmeldeinformationen authentifiziert werden soll.
- Führen Sie für plugin_name einen der folgenden Schritte aus:
  - Geben Sie für die Ping Identity-Konfiguration ein **`BrowserSAML`**. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung bei Ping Identity verwendet.
  - Geben Sie für Ping Identity mit Single-Sign-On-Konfiguration **`Ping`** ein. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung mit Single Sign-On mit Ping Identity verwendet.
- Geben Sie für uid ***your-ping-username*** ein. Dies ist der Benutzername des Microsoft Azure-Kontos, das Sie für die einmalige Anmeldung (Single-Sign-On) verwenden und das über die Berechtigung für den Cluster verfügt, für den Sie sich authentifizieren möchten. Verwenden Sie dies nur, wenn plugin_name Ping ist.
- Geben Sie für pwd ***your-ping-password*** ein. Verwenden Sie dies nur, wenn plugin_name Ping ist.
- Geben Sie für login_url ***your-login-url*** ein. Dies ist die URL zur Initiierung von Single Sign-On, die die SAML-Antwort zurückgibt. Dies gilt nur für das Browser SAML-Plug-in.

- Geben Sie für idp_response_timeout ***the-number-of-seconds*** ein. Dies ist der angegebene Zeitraum in Sekunden, in dem auf eine Antwort von PingOne Identity gewartet werden soll. Dies gilt nur für das Browser SAML-Plug-in.
- Geben Sie bei listen_port „***your-listen-port***“ ein. Dies ist der Port, den der lokale Server überwacht. Der Standardwert ist 7890. Dies gilt nur für das Browser SAML-Plug-in.

Bearbeiten Sie unter macOS und Linux auch die Profileinstellungen, um folgende Exporte hinzuzufügen:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit Okta

Sie können Okta als Identitätsanbieter (IdP) verwenden, um auf Ihren Amazon-Redshift-Cluster zuzugreifen. Im Anschluss finden Sie eine Prozedur, die beschreibt, wie Sie eine Vertrauensstellung für diesen Zweck einrichten. Weitere Informationen zur Konfiguration AWS als Service Provider für Okta finden Sie unter Configuring Your SAML 2.0 IdP with Relying Party Trust und Adding Claims im IAM-Benutzerhandbuch.

So richten Sie Okta und Ihr AWS Konto so ein, dass sie sich gegenseitig vertrauen

1. Erstellen oder verwenden Sie einen vorhandenen Amazon-Redshift-Cluster, mit dem sich Ihre Okta-Benutzer verbinden können. Um die Verbindung zu konfigurieren, werden bestimmte Eigenschaften dieses Clusters benötigt, z. B. die Clusterkennung. Weitere Informationen finden Sie unter Erstellen eines Clusters.
2. Fügen Sie Amazon Redshift als neue Anwendung im Okta-Portal hinzu. Ausführliche Schritte finden Sie in der Okta-Dokumentation.
   - Wählen Sie Add Application (Anwendung hinzufügen).
   - Wählen Sie unter Add Application (Anwendung hinzufügen) die Option Create New App (Neue Anwendung erstellen).
   - Wählen Sie auf der Seite Create a New Add Application Integration (Neue „Anwendung hinzufügen“-Integration erstellen) unter Platform (Plattform) die Option Web.

- Wählen Sie unter Sign on method (Anmeldemethode) SAML v2.0.
- Geben Sie auf der Seite General Settings (Allgemeine Einstellungen) unter App name (Name der Anwendung) ***your-redshift-saml-sso-name*** ein. Der Name Ihrer Anwendung.
- Geben Sie auf der Seite SAML Settings (SAML-Einstellungen) unter Single sign-on URL (SSO-URL) ***your-redshift-local-host-url*** ein. Dies ist der lokale Host und Port, auf die die SAML-Zusicherung umgeleitet wird, z. B. `http://localhost:7890/redshift/`.

3. Verwenden Sie den Wert von Single Sign on URL (Single-Sign-On-URL) als Recipient URL (Empfänger-URL) und Destination URL (Ziel-URL).
4. Wählen Sie für Signing (Signieren) die Option Sign Assertion (Zusicherung signieren).
5. Geben Sie unter Audience URI (SP Entity ID) (Zielgruppen-URI (SP-Entitäts-ID)) **`urn:amazon:webservices`** für die Ansprüche ein, wie in der folgenden Tabelle dargestellt.
6. Geben Sie im Abschnitt Advanced Settings (Erweiterte Einstellungen) unter SAML Issuer ID (SAML-Aussteller-ID) ein ***your-Identity-Provider-Issuer-ID***, was Sie im Abschnitt View Setup Instructions (Einrichtungsanweisungen anzeigen) finden.
7. Erstellen Sie im Abschnitt Attribute Statements (Attributanweisungen) die Anträge, wie in der folgenden Tabelle dargestellt.

Name des Antrags	Wert
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam::*123456789012* :role/*Okta*,arn:aws:iam::*123456789012* :saml-provider/*Okta*
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.email
https://redshift.amazon.com/SAML/Attributes/AutoCreate	„true“
https://redshift.amazon.com/SAML/Attributes/DbUser	user.email

8. Suchen Sie im Abschnitt App Embed Link (Link zum Einbetten der App) nach der URL, die Sie als Anmelde-URL für das Browser-SAML-Plug-in verwenden können.
9. Erstellen Sie auf der IAM-Konsole einen IAM SAML-Identitätsanbieter. Das Metadatendokument, das Sie bereitstellen, ist die XML-Datei für Verbundmetadaten, die Sie beim Einrichten von Okta

gespeichert haben. Ausführliche Schritte finden Sie unter Erstellen und Verwalten eines IAM-Identitätsanbieters (Konsole) im IAM-Benutzerhandbuch.

10. Erstellen Sie auf der IAM-Konsole eine IAM-Rolle für SAML 2.0-Verbund. Detaillierte Schritte finden Sie unter Erstellen einer Rolle für SAML im IAM-Benutzerhandbuch.
11. Erstellen Sie eine IAM-Richtlinie, die Sie an die IAM-Rolle anhängen können, die Sie für den SAML 2.0-Verbund auf der IAM-Konsole erstellt haben. Ausführliche Schritte finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch. Ein Azure AD-Beispiel finden Sie unter Einrichten der JDBC- oder ODBC-Single-Sign-On-Authentifizierung mit Microsoft Azure AD.

So richten Sie JDBC für die Authentifizierung bei Okta ein:

- Konfigurieren Sie Ihren Datenbank-Client für die Verbindung mit Ihrem Cluster über JDBC mithilfe von Okta Single Sign-On.

  Sie können jeden Client verwenden, der mithilfe eines JDBC-Treibers eine Verbindung mit Okta Single Sign-On herstellt oder eine Sprache wie Java verwendet, um über ein Skript eine Verbindung herzustellen. Informationen zur Installation und Konfiguration finden Sie unter Konfigurieren einer Verbindung für JDBC-Treiberversion 2.1 für Amazon Redshift.

  Sie können beispielsweise SQLWorkbench/J als Client verwenden. Wenn Sie SQLWorkbench/J konfigurieren, verwendet die URL Ihrer Datenbank das folgende Format.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Wenn Sie SQLWorkbench/J als Client verwenden, führen Sie die folgenden Schritte aus:

  a. Starten Sie SQL Workbench/J. Fügen Sie auf der Seite Select Connection Profile (Verbindungsprofil auswählen) eine Profile Group (Profilgruppe) hinzu, z. B. **`Okta`**.

  b. Geben Sie unter Connection Profile (Verbindungsprofil) ***`your-connection-profile-name`*** ein, z. B. **`Okta`**.

  c. Wählen Sie Manage Drivers (Treiber verwalten) und dann Amazon Redshift aus. Wählen Sie das Symbol Open Folder (Ordner öffnen) neben Library (Bibliothek) und dann die entsprechende JDBC-JAR-Datei aus.

  d. Fügen Sie auf der Seite Select Connection Profile (Verbindungsprofil auswählen) dem Verbindungsprofil Informationen wie folgt hinzu:

- Geben Sie unter User (Benutzer) Ihren Okta-Benutzernamen ein. Dies ist der Benutzername des Okta-Kontos, das Sie für die einmalige Anmeldung (Single-Sign-On) verwenden, und das über die Berechtigung für den Cluster verfügt, für den Sie sich authentifizieren möchten.
- Geben Sie unter Password (Passwort) Ihr Okta-Passwort ein.
- Wählen Sie für Driver (Treiber) die Option Amazon Redshift (com.amazon.redshift.jdbc.Driver) aus.
- Geben Sie für URL **jdbc:redshift:iam://*your-cluster-identifier*:*your-cluster-region*/*your-database-name*** ein.

e. Wählen Sie Extended Properties (Erweiterte Eigenschaften), und führen Sie einen der folgenden Schritte aus:

- Geben Sie für login_url ***your-okta-sso-login-url*** ein. Dieser Wert gibt die URL an, die Single Sign-On als Authentifizierungsmethode für die Anmeldung bei Okta verwenden soll.
- Geben Sie für Okta Single Sign-On im Feld plugin_name den Wert **com.amazon.redshift.plugin.OktaCredentialsProvider** ein. Dieser Wert gibt an, dass der Treiber Okta Single Sign-On als Authentifizierungsmethode verwenden soll.
- Geben Sie für Okta Single Sign-On mit MFA im Feld plugin_name den Wert **com.amazon.redshift.plugin.BrowserSamlCredentialsProvider** ein. Dies signalisiert dem Treiber, dass Single Sign-On für Okta mit MFA als Authentifizierungsmethode verwendet werden soll.

So richten Sie ODBC für die Authentifizierung bei Okta ein:

- Konfigurieren Sie Ihren Datenbank-Client für die Verbindung mit Ihrem Cluster über ODBC mithilfe von Okta Single Sign-On.

  Amazon Redshift stellt ODBC-Treiber für Linux-, Windows- und macOS-Betriebssysteme bereit. Stellen Sie vor der Installation eines ODBC-Treibers fest, ob Ihr SQL-Client-Tool 32-Bit oder 64-Bit ist. Installieren Sie den ODBC-Treiber, der den Anforderungen Ihres SQL-Clienttools entspricht.

  Installieren und konfigurieren Sie außerdem den neuesten Amazon-Redshift-ODBC-Treiber für Ihr Betriebssystem wie folgt:

- Informationen für Windows finden Sie unter Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows.
- Informationen zu macOS finden Sie unter Installieren des Amazon-Redshift-ODBC-Treibers unter macOS X.
- Weitere Informationen für Linux finden Sie unter Installieren des Amazon-Redshift-ODBC-Treibers unter Linux.

Geben Sie unter Windows auf der Seite Amazon Redshift ODBC Driver DSN Setup (DSN-Setup für Amazon Redshift ODBC-Treiber) unter Connection Settings (Verbindungseinstellungen) die folgenden Informationen ein:

- Geben Sie für Data Source Name (Datenquellenname) ***your-DSN*** ein. Dies gibt den Datenquellennamen an, der als ODBC-Profilname verwendet wird.
- Führen Sie für Auth type (Authentifizierungstyp) eine der folgenden Aktionen aus:
  - Wählen Sie für die Konfiguration von Okta Single Sign-On **`Identity Provider: Okta`** aus. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung mit Okta Single Sign-On verwendet.
  - Wählen Sie für die Konfiguration von Okta Single Sign-On mit MFA-Konfiguration **`Identity Provider: Browser SAML`** aus. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung mit Okta Single Sign-On mit MFA verwendet.
- Geben Sie für Cluster ID (Cluster-ID) ***your-cluster-identifier*** ein.
- Geben Sie für Region ***your-cluster-region*** ein.
- Geben Sie für Database (Datenbank) ***your-database-name*** ein.
- Geben Sie für User (Benutzer) ***your-okta-username*** ein. Dies ist der Benutzername des Okta-Kontos, das Sie für Single Sign-On verwenden und das über die Berechtigung für den Cluster verfügt, für den Sie sich authentifizieren möchten. Verwenden Sie dies nur, wenn Auth type (Authentifizierungstyp) Identity Provider: Okta (Identitätsanbieter: Okta) ist.
- Geben Sie unter Password (Passwort) ***your-okta-password*** ein. Verwenden Sie dies nur, wenn Auth type (Authentifizierungstyp) Identity Provider: Okta (Identitätsanbieter: Okta) ist.

Bearbeiten Sie die `odbc.ini`-Datei unter Mac OS und Linux wie folgt:

> **Note**
>
> Bei allen Eingaben wird zwischen Groß- und Kleinschreibung unterschieden.

- Geben Sie für clusterid ***your-cluster-identifier*** ein. Dies ist der Name des erstellten Amazon-Redshift-Clusters.
- Geben Sie für Region ***your-cluster-region*** ein. Dies ist die AWS Region des erstellten Amazon Redshift Redshift-Clusters.
- Geben Sie für die database ***your-database-name*** ein. Dies ist der Name der Datenbank, auf die Sie im Amazon-Redshift-Cluster zugreifen möchten.
- Geben Sie für locale **en-us** ein. Dies ist die Sprache, in der Fehlermeldungen angezeigt werden.
- Geben Sie für iam **1** ein. Dieser Wert signalisiert dem Treiber, dass mit IAM-Anmeldeinformationen authentifiziert werden soll.
- Führen Sie für plugin_name einen der folgenden Schritte aus:
  - Geben Sie für Okta Single Sign-On mit MFA-Konfiguration **BrowserSAML** ein. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung bei Okta Single Sign-On mit MFA verwendet.
  - Geben Sie für die Konfiguration von Okta Single Sign-On **Okta** ein. Dies ist die Authentifizierungsmethode, die der ODBC-Treiber zur Authentifizierung mit Okta Single Sign-On verwendet.
- Geben Sie für uid ***your-okta-username*** ein. Dies ist der Benutzername des Okta-Kontos, das Sie für Single Sign-on verwenden und das über die Berechtigung für den Cluster verfügt, für den Sie sich authentifizieren möchten. Verwenden Sie dies nur, wenn plugin_name (Plug-In-Name) Okta ist.
- Geben Sie für pwd ***your-okta-password*** ein. Verwenden Sie dies nur, wenn plugin_name (Plug-In-Name) Okta ist.
- Geben Sie für login_url ***your-login-url*** ein. Dies ist die URL zur Initiierung von Single Sign-On, die die SAML-Antwort zurückgibt. Dies gilt nur für das Browser SAML-Plug-in.
- Geben Sie für idp_response_timeout ***the-number-of-seconds*** ein. Dies ist der angegebene Zeitraum in Sekunden, für den auf eine Antwort gewartet werden soll. PingOne Dies gilt nur für das Browser SAML-Plug-in.

- Geben Sie bei listen_port „***your-listen-port***“ ein. Dies ist der Port, den der lokale Server überwacht. Der Standardwert ist 7890. Dies gilt nur für das Browser SAML-Plug-in.

Bearbeiten Sie unter macOS und Linux auch die Profileinstellungen, um folgende Exporte hinzuzufügen:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

JDBC- und ODBC-Optionen zur Erstellung von Benutzeranmeldeinformationen für die Datenbank

Geben Sie den Datenbankbenutzernamen als JDBC- oder ODBC-Option an, um den Amazon-Redshift-JDBC- oder -ODBC-Treiber zum Erstellen von Datenbankbenutzer-Anmeldeinformationen zu verwenden. Optional können Sie den Treiber einen neuen Datenbankbenutzer erstellen lassen, wenn keiner vorhanden ist, und Sie können eine Liste von Datenbankbenutzergruppen angeben, denen der Benutzer bei der Anmeldung zugewiesen wird.

Wenn Sie einen Identitätsanbieter verwenden, kann Ihnen der Identitätsanbieteradministrator die korrekten Werte für diese Optionen verraten. Der Identitätsanbieteradministrator kann außerdem Ihren Identitätsanbieter so konfigurieren, dass er diese Optionen bereitstellt. In diesem Fall müssen Sie sie nicht als JDBC- oder ODBC-Optionen bereitstellen. Weitere Informationen finden Sie unter Konfigurieren von SAML-Zusicherungen für den Identitätsanbieter.

> **Note**
>
> Wenn Sie eine IAM-Richtlinienvariable verwenden, `${redshift:DbUser}`, wie in Ressourcenrichtlinien für GetClusterCredentials beschrieben, wird der Wert für `DbUser` durch den Wert ersetzt, der vom Abfragekontext der API-Operation abgerufen wird. Die Amazon-Redshift-Treiber verwenden den von der Verbindungs-URL bereitgestellten Wert für die `DbUser`-Variable, nicht den als SAML-Attribut bereitgestellten Wert.
> Wir empfehlen, für die Sicherstellung dieser Konfiguration eine Bedingung in einer IAM-Richtlinie zu verwenden, um den `DbUser`-Wert mit dem `RoleSessionName` zu validieren. Beispiele, wie Sie eine Bedingung in einer IAM-Richtlinie einrichten, finden Sie in Beispielrichtlinie für die Verwendung GetClusterCredentials.

In der folgenden Tabelle sind die Optionen für die Erstellung von Benutzeranmeldeinformationen für die Datenbank aufgeführt.

Option	Beschreibung
DbUser	Der Name eines Datenbankbenutzers. Wenn ein Benutzer mit dem Namen in der Datenbank DbUser vorhanden ist, haben die temporären Benutzeranmeldeinf ormationen dieselben Berechtigungen wie der vorhandene Benutzer. Wenn es in der Datenbank nicht DbUser existiert und wahr AutoCreate ist, DbUser wird ein neuer Benutzer mit dem Namen erstellt. Optional können Sie das Passwort eines bestehenden Benutzers deaktivieren. Weitere Informationen finden Sie unter ALTER_USER.
AutoCreat e	Geben Sie `true` an, dass ein Datenbankbenutzer mit dem angegebenen Namen erstellt werden soll, DbUser falls noch keiner existiert. Der Standardwert lautet „false“.
`DbGroups`	Eine durch Kommata abgegrenzte Liste der Namen bestehender Datenbankgruppen, denen der Datenbankbenutzer für die Dauer der aktuellen Sitzung zugewiesen wird. Standardmäßig werden neue Benutzer nur der Gruppe „PUBLIC“ hinzugefügt.

Generieren von Datenbankanmeldedaten für eine IAM-Identität mithilfe der Amazon Redshift CLI oder API

Um programmgesteuert temporäre Datenbank-Benutzeranmeldedaten zu generieren, stellt Amazon Redshift den get-cluster-credentialsBefehl für die AWS Command Line Interface (AWS CLI) - und die GetClusterCredentialsAPI-Operation bereit. Sie können Ihren SQL-Client auch mithilfe von Amazon-Redshift-JDBC- oder -ODBC-Treibern konfigurieren. Diese steuern das Aufrufen des `GetClusterCredentials`-Vorgangs, das Abrufen der Datenbank-Benutzeranmeldeinformationen und das Herstellen einer Verbindung zwischen dem SQL-Client und der Amazon-Redshift-Datenbank. Weitere Informationen finden Sie unter JDBC- und ODBC-Optionen zur Erstellung von Benutzeranmeldeinformationen für die Datenbank.

> **Note**
>
> Wir empfehlen die Verwendung von Amazon-Redshift-JDBC- oder -ODBC-Treibern zum Generieren von Benutzeranmeldeinformationen für die Datenbank.

In diesem Abschnitt finden Sie Schritte zum programmgesteuerten Aufrufen der `GetClusterCredentials` Operation oder des get-cluster-credentials Befehls, zum Abrufen von Datenbank-Benutzeranmeldedaten und zum Herstellen einer Verbindung mit der Datenbank.

Erstellen und verwenden Sie temporäre Datenbankanmeldeinformationen wie folgt:

1. Erstellen oder bearbeiten Sie einen Benutzer oder eine Rolle mit den erforderlichen Berechtigungen. Weitere Informationen zu IAM-Berechtigungen finden Sie unter Erstellen Sie eine IAM-Rolle mit Anrufberechtigungen GetClusterCredentials.
2. Führen Sie als Benutzer oder Rolle, die Sie im vorherigen Schritt autorisiert haben, den get-cluster-credentials CLI-Befehl aus oder rufen Sie den `GetClusterCredentials` API-Vorgang auf und geben Sie die folgenden Werte an:

   - Cluster identifier (Cluster-ID) – der Name des Clusters, der die Datenbank enthält.
   - Database user name (Datenbankbenutzername) – der Name eines bestehenden oder neuen Datenbankbenutzers.
     - Wenn der Benutzer nicht in der Datenbank existiert und den Wert true hat, AutoCreate wird ein neuer Benutzer mit deaktiviertem PASSWORD erstellt.
     - Wenn der Benutzer nicht existiert und AutoCreate den Wert False hat, schlägt die Anfrage fehl.
     - In diesem Beispiel lautet der Datenbankbenutzername `temp_creds_user`.
   - Autocreate (Automatisch erstellen) – (Optional) Erstellt einen neuen Benutzer, wenn der Datenbankbenutzername nicht vorhanden ist.
   - Database name (Datenbankname) – (Optional) Der Name der Datenbank, bei der der Benutzer zur Anmeldung autorisiert ist. Wenn kein Datenbankname angegeben ist, kann sich der Benutzer bei jeder Datenbank des Clusters anmelden.
   - Database groups (Datenbankgruppen) – (Optional) Eine Liste der vorhandenen Datenbankbenutzergruppen. Bei erfolgreicher Anmeldung wird der Datenbankbenutzer den angegebenen Benutzergruppen hinzugefügt. Wenn keine Gruppe angegeben wird, verfügt der Benutzer nur über PUBLIC-Berechtigungen. Die Benutzergruppennamen müssen mit den dbgroup-Ressourcen-ARNs übereinstimmen, die in der IAM-Richtlinie angegeben sind, die dem Benutzer bzw. der Rolle zugeordnet ist.
   - Expiration time (Ablaufzeit) – (Optional) Die Ablaufzeit der temporären Anmeldeinformationen in Sekunden. Sie können einen Wert zwischen 900 Sekunden (15 Minuten) und 3600 Sekunden (60 Minuten) auswählen. Standardmäßig ist ein Zeitraum von 900 Sekunden festgelegt.

3. Amazon Redshift verifiziert, dass der Benutzer zum Aufrufen der Operation `GetClusterCredentials` mit den angegebenen Ressourcen berechtigt ist.
4. Amazon Redshift gibt ein temporäres Passwort und den Datenbankbenutzernamen zurück.

   Im folgenden Beispiel wird die Amazon-Redshift-CLI zur Erstellung temporärer Datenbankanmeldeinformationen für einen vorhandenen Benutzer namens verwendet `temp_creds_user`.

   ```
   aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
    temp_creds_user --db-name exampledb --duration-seconds 3600
   ```

   Das Ergebnis ist wie folgt.

   ```
   {
     "DbUser": "IAM:temp_creds_user",
     "Expiration": "2016-12-08T21:12:53Z",
     "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpDHwXVPyJYBDm/
   gqX2Eeaq6P3DgTzgPg=="
   }
   ```

   Im folgenden Beispiel wird die Amazon-Redshift-CLI mit aktivierter AutoCreate-Funktion zur Erstellung temporärer Datenbankanmeldeinformationen für einen neuen Benutzer und zum Hinzufügen des Benutzers zur Gruppe verwendet `example_group`.

   ```
   aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
    temp_creds_user --auto-create --db-name exampledb --db-groups example_group --
   duration-seconds 3600
   ```

   Das Ergebnis ist wie folgt.

   ```
   {
     "DbUser": "IAMA:temp_creds_user:example_group",
     "Expiration": "2016-12-08T21:12:53Z",
     "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpDHwXVPyJYBDm/
   gqX2Eeaq6P3DgTzgPg=="
   }
   ```

5. Stellen Sie eine Verbindung mit Secure Socket Layer (SSL)-Authentifizierung mit dem Amazon-Redshift-Cluster her und senden Sie eine Anmeldungsanforderung mit dem Benutzernamen

und dem Passwort aus der `GetClusterCredentials`-Antwort. Geben Sie mit dem Benutzernamen das Präfix `IAM:` oder `IAMA:` an, zum Beispiel `IAM:temp_creds_user` oder `IAMA:temp_creds_user`.

> **Important**
>
> Konfigurieren Sie Ihren SQL-Client so, dass er SSL erfordert. Andernfalls greift Ihr SQL-Client auf Nicht-SSL-Verbindungen zurück, wenn er automatisch Verbindungen über SSL herstellen soll und dabei ein Fehler auftritt. In diesem Fall schlägt der erste Verbindungsversuch möglicherweise fehl, da die Anmeldeinformationen abgelaufen oder ungültig sind, dann schlägt der zweite Verbindungsversuch fehl, weil die Verbindung nicht mit SSL hergestellt wird. Falls dies passiert, wird die erste Fehlermeldung möglicherweise übersehen. Weitere Informationen zum Herstellen einer Verbindung zum Cluster mit SSL finden Sie unter Konfigurieren von Sicherheitsoptionen für Verbindungen.

6. Falls die Verbindung nicht mit SSL hergestellt wird, schlägt der Verbindungsversuch fehl.
7. Der Cluster übermittelt eine Anforderung auf `authentication` an den SQL-Client.
8. Der SQL-Client übermittelt daraufhin das temporäre Passwort an den Cluster.
9. Falls das Passwort gültig und nicht abgelaufen ist, stellt der Cluster die Verbindung her.

Amazon Redshift autorisieren, in Ihrem Namen auf andere AWS Dienste zuzugreifen

Für einige Amazon Redshift-Funktionen muss Amazon Redshift in Ihrem Namen auf andere AWS Dienste zugreifen. Beispielsweise können mit den Befehlen COPY und UNLOAD Daten unter Verwendung eines Amazon S3 Buckets in Ihren Amazon-Redshift-Cluster geladen bzw. entladen werden. Der Befehl CREATE EXTERNAL FUNCTION kann eine AWS Lambda-Funktion mithilfe einer skalaren benutzerdefinierten Lambda-Funktion (UDF) aufrufen. Amazon Redshift Spectrum kann einen Datenkatalog in Amazon Athena oder verwenden. AWS Glue Damit Ihre Amazon-Redshift-Cluster in Ihrem Namen agieren können, stellen Sie ihnen Sicherheitsanmeldeinformationen bereit. Zur Bereitstellung von Sicherheitsanmeldeinformationen geben Sie am besten eine AWS Identity and Access Management (IAM)-Rolle an. Für COPY und UNLOAD können Sie temporäre Anmeldeinformationen angeben.

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS Management Console Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
	die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	• Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldedaten im Benutzerhandbuch. AWS CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Im Folgenden erfahren Sie, wie Sie eine IAM-Rolle mit den entsprechenden Berechtigungen für den Zugriff auf andere Dienste erstellen. AWS Sie müssen dazu auch die Rolle Ihrem Cluster zuweisen und den Amazon-Ressourcennamen (ARN) der Rolle angeben, wenn Sie den Amazon-Redshift-Befehl ausführen. Weitere Informationen finden Sie unter Autorisieren der Vorgänge COPY, UNLOAD, CREATE EXTERNAL FUNCTION und CREATE EXTERNAL SCHEMA mithilfe von IAM-Rollen.

Darüber hinaus kann ein Superuser bestimmten Benutzern und Gruppen die Berechtigung ASSUMEROLE erteilen, um Zugriff auf eine Rolle für COPY- und UNLOAD-Vorgänge zu gewähren. Weitere Informationen finden Sie unter GRANT im Datenbankentwicklerhandbuch zu Amazon Redshift.

Erstellen einer IAM-Rolle, um Ihrem Amazon Redshift Redshift-Cluster den Zugriff auf Services zu ermöglichen AWS

Gehen Sie wie folgt vor, um eine IAM-Rolle zu erstellen, die Ihrem Amazon-Redshift-Cluster die Kommunikation mit anderen AWS -Services für Sie ermöglicht. Die in diesem Abschnitt verwendeten Werte sind Beispiele. Sie können Werte basierend auf Ihren Anforderungen auswählen.

Um eine IAM-Rolle zu erstellen, um Amazon Redshift den Zugriff auf Services zu ermöglichen AWS

1. Öffnen Sie die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Roles aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Wählen Sie AWS service und anschließend Redshift aus.
5. Wählen Sie unter Select your use case (Auswahl Ihres Anwendungsfalls) Redshift - Customizable (Redshift - Anpassbar) und dann Next: Permissions (Weiter: Berechtigungen) aus. Die Seite Attach permissions policy (Berechtigungsrichtlinie anfügen) wird angezeigt.
6. Zum Zugreifen auf Amazon S3 mithilfe von COPY können Sie beispielsweise **`AmazonS3ReadOnlyAccess`** und Anhängen verwenden. Zum Zugreifen auf Amazon S3 mit COPY oder UNLOAD empfehlen wir, verwaltete Richtlinien zu erstellen, die den Zugriff auf den gewünschten Bucket und das entsprechende Präfix beschränken. Für Lese- und Schreibvorgänge empfehlen wir, die minimalen Berechtigungen zu aktivieren und den Zugriff auf die Amazon S3 Buckets und Schlüsselpräfixe zu beschränken, die Amazon Redshift erfordert.

   Für Zugriff zum Aufrufen von Lambda-Funktionen für den Befehl CREATE EXTERNAL FUNCTION fügen Sie hinzu **`AWSLambdaRole`**.

   Für Redshift Spectrum, zusätzlich zum Zugriff auf Amazon S3, fügen Sie **`AWSGlueConsoleFullAccess`** oder **`AmazonAthenaFullAccess`** hinzu.

   Wählen Sie Next: Markierungen (Weiter: Markierungen).
7. Die Seite Add tags (Tags hinzufügen) wird angezeigt. Sie können optional Tags hinzufügen. Klicken Sie auf Next: Review (Weiter: Prüfen).
8. Geben Sie in Role name (Rollenname) einen Namen für die Rolle ein, z. B. **`RedshiftCopyUnload`**. Wählen Sie Create role (Rolle erstellen) aus.
9. Die neue Rolle ist für alle Benutzer auf Clustern verfügbar, die diese Rolle verwenden. Um den Zugriff auf bestimmte Benutzer auf bestimmten Clustern oder auf Clustern in bestimmten

Regionen zu beschränken, bearbeiten Sie das Vertrauensverhältnis für die Rolle. Weitere Informationen finden Sie unter Einschränken des Zugriffs auf IAM-Rollen.

10. Weisen Sie die Rolle zu Ihrem Cluster zu. Sie können eine IAM-Rolle einem Cluster zuweisen, wenn Sie den Cluster erstellen, Sie können sie aber auch einem vorhandenen Cluster zuweisen. Weitere Informationen finden Sie unter Verknüpfen von IAM-Rollen mit Clustern.

> **Note**
>
> Um den Zugriff auf bestimmte Daten zu beschränken, verwenden Sie eine IAM-Rolle, die die minimal erforderlichen Berechtigungen gewährt.

Einschränken des Zugriffs auf IAM-Rollen

Standardmäßig sind IAM-Rollen, die für ein Amazon-Redshift-Cluster verfügbar sind, für alle Benutzer dieses Clusters verfügbar. Sie können die IAM-Rollen auch auf bestimmte Amazon-Redshift-Datenbankbenutzer in bestimmten Clustern oder in bestimmten Regionen beschränken.

Gehen Sie wie folgt vor, um nur bestimmten Datenbankbenutzern zu erlauben, eine IAM-Rolle zu verwenden.

So identifizieren Sie bestimmte Datenbankbenutzer mit Zugriff auf eine IAM-Rolle:

1. Ermitteln Sie den Amazon-Ressourcennamen (ARN) für die Datenbankbenutzer in Ihrem Amazon-Redshift-Cluster. Der ARN für einen Datenbankbenutzer hat das folgende Format: `arn:aws:redshift:region:account-id:dbuser:cluster-name/user-name`.

   Verwenden Sie für Amazon Redshift Serverless das folgende ARN-Format. `arn:aws:redshift:region:account-id:dbuser:workgroup-name/user-name`
2. Öffnen Sie die IAM-Konsole.
3. Wählen Sie im Navigationsbereich Roles aus.
4. Wählen Sie die IAM-Rolle aus, die Sie auf bestimmte Amazon-Redshift-Datenbankbenutzer beschränken möchten.
5. Wählen Sie die Registerkarte Trust Relationships (Vertrauensstellungen) und anschließend Edit Trust Relationship (Vertrauensstellung bearbeiten) aus. Eine neue IAM-Rolle, die es Amazon Redshift ermöglicht, in Ihrem Namen auf andere AWS Services zuzugreifen, hat ein Vertrauensverhältnis wie folgt:

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

6. Fügen Sie dem Aktionsabschnitt `sts:AssumeRole` des Vertrauensverhältnisses eine Bedingung hinzu, die das Feld `sts:ExternalId` auf die von Ihnen angegebenen Werte beschränkt. Fügen Sie einen ARN für jeden Datenbankbenutzer hinzu, dem Sie den zugriff auf die Rolle gewähren möchten. Die externe ID kann eine beliebige eindeutige Zeichenfolge sein.

   Beispielsweise gibt das folgende Vertrauensverhältnis an, dass nur die Datenbankbenutzer `user1` und `user2` auf dem Cluster `my-cluster` in der Region `us-west-2` zur Verwendung dieser IAM-Rolle berechtigt sind.

```
{
  "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. Wählen Sie Update Trust Policy.

Beschränken einer IAM-Rolle auf eine AWS -Region

Sie können eine IAM-Rolle so einschränken, dass sie nur in einer bestimmten Region zugänglich ist. AWS Standardmäßig sind IAM-Rollen für Amazon Redshift nicht auf eine einzelne Region beschränkt.

Gehen Sie wie folgt vor, um die Nutzung einer IAM-Rolle nach Region einzuschränken.

So identifizieren Sie die zugelassenen Regionen für eine IAM-Rolle:

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich Roles.
3. Wählen Sie die Rolle, die Sie für bestimmte Regionen modifizieren möchten.
4. Wählen Sie die Registerkarte Trust Relationships (Vertrauensstellungen) und anschließend Edit Trust Relationship (Vertrauensstellung bearbeiten) aus. Eine neue IAM-Rolle, die es Amazon Redshift ermöglicht, in Ihrem Namen auf andere AWS Services zuzugreifen, hat ein Vertrauensverhältnis wie folgt:

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

5. Ändern Sie die `Service`-Liste für den `Principal` mit der Liste der Regionen, für die die Verwendung der Rolle erlaubt sein soll. Jede Region in der `Service`-Liste muss das folgende Format haben: `redshift.`*`region`*`.amazonaws.com`.

   Beispielsweise erlaubt das folgende bearbeitete Treuhandverhältnis die Verwendung der IAM-Rolle nur in den Regionen `us-east-1` und `us-west-2`.

```
{
  "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. Wählen Sie Update Trust Policy (Vetrauensrichtlinie aktualisieren)

Verketten von IAM-Rollen in Amazon Redshift

Wenn Sie Ihrem Cluster eine Rolle zuordnen, kann Ihr Cluster diese Rolle übernehmen, um auf Amazon S3, Amazon Athena und in AWS Lambda Ihrem Namen zuzugreifen. AWS Glue Wenn eine an den Cluster angefügte Rolle keinen Zugriff auf die erforderlichen Ressourcen hat, können Sie mit ihr eine andere Rolle verketten, die möglicherweise zu einem anderen Konto gehört. Ihr Cluster nimmt dann vorübergehend die verkettete Rolle an, um auf die Daten zuzugreifen. Sie können über verkettete Rollen auch kontoübergreifenden Zugriff gewähren. Jede Rolle in der Kette nimmt die nächste Rolle in der Kette an, bis hin zum Cluster, der die Rolle am Ende der Kette annimmt. Die maximale Anzahl von IAM-Rollen, die Sie zuordnen können, unterliegt einem Kontingent. Weitere Informationen finden Sie unter dem Kontingent „Cluster-IAM-Rollen für Amazon Redshift für den Zugriff auf andere AWS Dienste“ unter. Kontingente für Amazon-Redshift-Objekte

Nehmen wir zum Beispiel an, Unternehmen A möchte auf Daten in einem Amazon S3 S3-Bucket zugreifen, der zu Unternehmen B gehört. Unternehmen A erstellt eine AWS Servicerolle für Amazon Redshift mit dem Namen `RoleA` und fügt sie ihrem Cluster hinzu. Unternehmen B erstellt eine Rolle mit dem Namen `RoleB`, die berechtigt ist, auf die Daten des Buckets von Unternehmen B zuzugreifen. Um auf die Daten im Bucket von Unternehmen B zuzugreifen, führt Unternehmen A den Befehl COPY mit einem `iam_role`-Parameter aus, der `RoleA` und `RoleB` verkettet. Für die Dauer des COPY-Vorgangs übernimmt `RoleA` vorübergehend `RoleB`, um auf den Amazon S3 Bucket zuzugreifen.

Zum Verketten von Rollen richten Sie eine Vertrauensstellung zwischen den Rollen ein. Eine Rolle, die eine andere Rolle annimmt (z. B. `RoleA`), muss über eine Berechtigungsrichtlinie verfügen, die es ihr erlaubt, die nächste verkettete Rolle (z. B. `RoleB`) anzunehmen. Die Rolle, die Berechtigungen übergibt (`RoleB`), muss wiederum über eine Vertrauensstellung verfügen, die es ihr erlaubt, ihre Berechtigungen an die vorherige verkettete Rolle (`RoleA`) zu übergeben. Weitere Informationen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

Die erste Rolle in der Kette muss eine dem Cluster angefügte Rolle sein. Die erste und jede folgende Rolle, die die nächste Rolle in der Kette annimmt, muss über eine Richtlinie verfügen, die eine bestimmte Anweisung enthält. Diese Anweisung enthält die Auswirkung `Allow` auf die Aktion `sts:AssumeRole` und den Amazon-Ressourcennamen (ARN) der nächsten Rolle in einem `Resource`-Element. In unserem Beispiel verfügt `RoleA` über die folgende Berechtigungsrichtlinie, die es ihr erlaubt, `RoleB` zu übernehmen, die dem AWS -Konto `210987654321` gehört.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1487639602000",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::210987654321:role/RoleB"
       }
    ]
}
```

Eine Rolle, die an eine andere Rolle übergeht, muss eine Vertrauensbeziehung mit der Rolle aufbauen, die die Rolle übernimmt, oder mit dem AWS Konto, dem die Rolle gehört. In unserem Beispiel verfügt `RoleB` über die folgende Vertrauensrichtlinie zum Einrichten einer Vertrauensstellung mit `RoleA`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
```

```
        "AWS": "arn:aws:iam::role/RoleA"
      }
    }
  ]
}
```

Mit der folgenden Vertrauensrichtlinie wird eine Vertrauensbeziehung mit dem AWS Kontoinhaber hergestellt`123456789012`. `RoleA`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}
```

> **Note**
>
> Um die Autorisierung zur Rollenverkettung auf bestimmte Benutzer zu beschränken, definieren Sie eine Bedingung. Weitere Informationen finden Sie unter Einschränken des Zugriffs auf IAM-Rollen.

Wenn Sie den Befehl UNLOAD, COPY, CREATE EXTERNAL FUNCTION oder CREATE EXTERNAL SCHEMA ausführen, können Sie Rollen durch Einschließen einer durch Kommas getrennten Liste von Rollen-ARNs im `iam_role`-Parameter verketten. Nachfolgend finden Sie die Syntax für die Verkettung von Rollen im `iam_role`-Parameter.

```
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**
>
> Die gesamte Rollenkette ist in einfachen Anführungszeichen eingeschlossen und darf keine Leerzeichen enthalten.

In den folgenden Beispielen ist `RoleA` dem Cluster angefügt, der dem AWS -Konto `123456789012` gehört. `RoleB`, die dem Konto `210987654321` gehört, ist berechtigt, auf den Bucket mit dem Namen `s3://companyb/redshift/` zuzugreifen. Im folgenden Beispiel werden `RoleA` und `RoleB` verkettet, um Daten mit dem UNLOAD-Befehl im s3://companyb/redshift/-Bucket zu entladen.

```
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';
```

Das folgende Beispiel verwendet den COPY-Befehl zum Laden der Daten, die im vorherigen Beispiel entladen wurden.

```
copy venue
from 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

Im folgende Beispiel verwendet der CREATE EXTERNAL SCHEMA-Befehl verkettete Rollen, um die Rolle anzunehmen `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';
```

Im folgenden Beispiel verwendet der Befehl CREATE EXTERNAL FUNCTION verkettete Rollen, um die Rolle anzunehmen `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';
```

Zusätzliche Informationen

Weitere Informationen finden Sie auch unter Autorisieren der Vorgänge COPY, UNLOAD, CREATE EXTERNAL FUNCTION und CREATE EXTERNAL SCHEMA mithilfe von IAM-Rollen.

Autorisieren der Vorgänge COPY, UNLOAD, CREATE EXTERNAL FUNCTION und CREATE EXTERNAL SCHEMA mithilfe von IAM-Rollen

Sie können den Befehl COPY verwenden, um Daten in Amazon Redshift zu laden (oder zu importieren), und den Befehl UNLOAD, um Daten aus Amazon Redshift zu entladen (oder zu exportieren). Sie können den Befehl CREATE EXTERNAL FUNCTION verwenden, um benutzerdefinierte Funktionen zu erstellen, von denen aus Funktionen aufgerufen werden. AWS Lambda

Wenn Sie Amazon Redshift Spectrum verwenden, verwenden Sie den Befehl CREATE EXTERNAL SCHEMA, um den Speicherort eines Amazon S3 Buckets anzugeben, der Ihre Daten enthält. Wenn Sie die Befehle COPY, UNLOAD oder CREATE EXTERNAL SCHEMA ausführen, geben Sie Sicherheitsanmeldeinformationen an. Diese Anmeldeinformationen autorisieren Ihren Amazon-Redshift-Cluster zum Lesen oder Schreiben von Daten in und aus Ihrem Zielspeicherort, wie beispielsweise einem Amazon S3 Bucket.

Wenn Sie CREATE EXTERNAL FUNCTION ausführen, geben Sie Sicherheitsanmeldeinformationen mithilfe des IAM-Rollenparameters an. Diese Anmeldeinformationen autorisieren Ihren Amazon Redshift Redshift-Cluster, Lambda-Funktionen von aufzurufen. AWS Lambda Die bevorzugte Methode zur Bereitstellung von Sicherheitsanmeldedaten ist die Angabe einer AWS Identity and Access Management (IAM-) Rolle. Für COPY und UNLOAD können Sie temporäre Anmeldeinformationen angeben. Weitere Informationen zum Erstellen einer IAM-Rolle finden Sie unter Amazon Redshift autorisieren, in Ihrem Namen auf andere AWS Dienste zuzugreifen.

Benutzer benötigen programmgesteuerten Zugriff, wenn sie mit AWS außerhalb von interagieren möchten. AWS Management Console Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benut zeranmeldedaten im Benutzerhandbuch. AWS

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Eine IAM-Rolle wird wie folgt verwendet:

- Erstellen Sie eine IAM-Rolle zur Verwendung mit Ihrem Amazon-Redshift-Cluster.
- Verknüpfen Sie die IAM-Rolle mit dem Cluster.
- Schließen Sie den ARN der IAM-Rolle ein, wenn Sie den Befehl COPY, UNLOAD, CREATE EXTERNAL FUNCTION oder CREATE EXTERNAL SCHEMA aufrufen.

In diesem Thema erfahren Sie, wie Sie eine IAM-Rolle einem Amazon-Redshift-Cluster zuordnen.

Verknüpfen von IAM-Rollen mit Clustern

Nachdem Sie eine IAM-Rolle erstellt haben, die Amazon Redshift berechtigt, für Sie auf andere AWS -Services zuzugreifen, müssen Sie diese Rolle einem Amazon-Redshift-Cluster zuordnen. Dies ist Voraussetzung dafür, dass Sie die Rolle zum Laden oder Entladen von Daten verwenden können.

Für die Verknüpfung einer IAM-Rolle mit einem Cluster erforderliche Berechtigungen

Um eine IAM-Rolle mit einem Cluster verknüpfen zu können, muss ein Benutzer über die `iam:PassRole`-Berechtigung für diese IAM-Rolle verfügen. Mit dieser Berechtigung kann ein

Administrator einschränken, welche IAM-Rollen ein Benutzer Amazon-Redshift-Clustern zuordnen kann. Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Das folgende Beispiel zeigt eine IAM-Richtlinie, die mit einem Benutzer verbunden werden kann und diesem die Durchführung dieser Aktionen ermöglicht:

- Rufen Sie die Details für alle Amazon-Redshift-Cluster ab, die dem Konto dieses Benutzers gehören.
- Ordnen Sie eine von drei IAM-Rollen einem von zwei Amazon-Redshift-Clustern zu.

```
{
    "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"
             ]
        }
```

```
    ]
}
```

Nachdem ein Benutzer die entsprechenden Berechtigungen besitzt, kann er eine IAM-Rolle einem Amazon-Redshift-Cluster zuordnen. Die IAM-Rolle kann dann mit dem Befehl COPY oder UNLOAD oder anderen Amazon-Redshift-Befehlen verwendet werden.

Weitere Informationen zu IAM-Richtlinien finden Sie unter Übersicht über IAM-Richtlinien im IAM-Benutzerhandbuch.

Verwaltung der Verknüpfung einer IAM-Rolle mit einem Cluster

Sie können eine IAM-Rolle einem Amazon-Redshift-Cluster zuordnen, wenn Sie den Cluster erstellen. Oder Sie können einen bestehenden Cluster ändern und eine oder mehrere IAM-Rollenzuordnungen hinzufügen oder entfernen.

Achten Sie auf Folgendes:

- Die maximale Anzahl von IAM-Rollen, die Sie zuordnen können, unterliegt einem Kontingent.
- Eine IAM-Rolle kann mehreren Amazon-Redshift-Clustern zugeordnet werden.
- Eine IAM-Rolle kann nur dann einem Amazon Redshift Redshift-Cluster zugeordnet werden, wenn sowohl die IAM-Rolle als auch der Cluster demselben Konto gehören. AWS

Verwendung der Konsole zur Verwaltung der Verknüpfungen von IAM-Rollen

Sie können die Verknüpfungen von IAM-Rollen für einen Cluster in der folgenden Weise mithilfe der Konsole verwalten.

So verwalten Sie IAM-Rollenzuordnungen:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster aus, den Sie aktualisieren möchten.
3. Wählen Sie unter Actions (Aktionen) Manage IAM roles (IAM-Rollen verwalten) aus, um die aktuellen Liste der dem Cluster zugeordneten IAM-Rollen anzuzeigen.
4. Wählen Sie auf der Seite Manage IAM roles (IAM-Rollen verwalten) die verfügbaren IAM-Rollen aus, die hinzugefügt werden sollen. Wählen Sie dann Add IAM role (IAM-Rolle hinzufügen) aus.

5. Wählen Sie Done (Beenden), um Ihre Änderungen zu speichern.

Verwenden von AWS CLI zur Verwaltung von IAM-Rollenzuordnungen

Sie können IAM-Rollenzuordnungen für einen Cluster mit dem verwalten, AWS CLI indem Sie die folgenden Ansätze verwenden.

Zuordnen einer IAM-Rolle zu einem Cluster mithilfe der AWS CLI

Um eine IAM-Rolle mit einem Cluster bei dessen Erstellung zu verknüpfen, geben Sie den Amazon-Ressourcennamen (ARN) der IAM-Rolle als `--iam-role-arns`-Parameter des Befehls `create-cluster` an. Die maximale Anzahl von IAM-Rollen, die Sie beim Aufrufen des Befehls `create-cluster` hinzufügen können, unterliegt einem Kontingent.

Das Zuordnen von IAM-Rollen zu Amazon-Redshift-Clustern und das Aufheben der Zuordnungen sind asynchrone Prozesse. Mit dem Befehl `describe-clusters` können Sie den Status aller Verknüpfungen von IAM-Rollen mit Clustern abrufen.

Im folgenden Beispiel werden zwei IAM-Rollen mit dem neu erstellten Cluster verknüpft `my-redshift-cluster`.

```
aws redshift create-cluster \
    --cluster-identifier "my-redshift-cluster" \
    --node-type "dc1.large" \
    --number-of-nodes 16 \
    --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftCopyUnload" \
                    "arn:aws:iam::123456789012:role/SecondRedshiftRole"
```

Um eine IAM-Rolle einem bestehenden Amazon-Redshift-Cluster zuzuordnen, geben Sie den Amazon-Ressourcennnamen (ARN) der IAM-Rolle für den `--add-iam-roles`-Parameter des `modify-cluster-iam-roles`-Befehls an. Die maximale Anzahl von IAM-Rollen, die Sie beim Aufrufen des Befehls `modify-cluster-iam-roles` hinzufügen können, unterliegt einem Kontingent.

Im folgenden Beispiel wird eine IAM-Rolle mit dem bestehenden Cluster verknüpft `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier "my-redshift-cluster" \
    --add-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Aufheben der Zuordnung einer IAM-Rolle zu einem Cluster mithilfe der AWS CLI

Um die Verknüpfung einer IAM-Rolle mit einem Cluster aufzuheben, geben Sie den ARN der IAM-Rolle als Parameter `--remove-iam-roles` des Befehls `modify-cluster-iam-roles` an. `modify-cluster-iam-roles` Die maximale Anzahl von IAM-Rollen, die Sie beim Aufrufen des Befehls `modify-cluster-iam-roles` löschen können, unterliegt einem Kontingent.

Im folgenden Beispiel wird die Zuordnung für eine IAM-Rolle für das `123456789012` AWS Konto aus einem Cluster mit dem Namen entfernt. `my-redshift-cluster`

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier "my-redshift-cluster" \
    --remove-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Auflisten von IAM-Rollenzuordnungen für einen Cluster mithilfe von AWS CLI

Rufen Sie den Befehl `describe-clusters` auf, um eine Liste aller einem Amazon-Redshift-Cluster zugeordneten IAM-Rollen und den Status der IAM-Rollen-Zuordnung anzuzeigen. Der ARN jeder der mit dem Cluster verknüpften IAM-Rollen wird in der `IamRoles`-Liste aufgeführt, wie in der folgenden Beispielausgabe gezeigt.

Rollen, die mit dem Cluster verknüpft wurden, zeigen den Status `in-sync`. Rollen, deren Verknüpfung mit dem Cluster derzeit bearbeitet wird, zeigen den Status `adding`. Rollen, deren Verknüpfung mit dem Cluster derzeit aufgehoben wird, zeigen den Status `removing`.

```
{
    "Clusters": [
        {
            "ClusterIdentifier": "my-redshift-cluster",
            "NodeType": "dc1.large",
            "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": "dc1.large",
            "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"
                }
            ],
            ...
        }
    ]
}
```

Weitere Informationen zur Verwendung von finden Sie im AWS CLIAWS CLI Benutzerhandbuch.

Erstellen einer IAM-Rolle als Standard für Amazon Redshift

Wenn Sie IAM-Rollen über die Redshift-Konsole erstellen, erstellt Amazon Redshift programmgesteuert die Rollen in Ihren Rollen AWS-Konto und fügt ihnen automatisch bestehende verwaltete Richtlinien hinzu. AWS Bei dieser Methode können Sie in der Redshift-Konsole bleiben und müssen zur Rollenerstellung nicht zur IAM-Konsole wechseln. Für eine genauere Steuerung der Berechtigungen für eine vorhandene IAM-Rolle, die in der Amazon-Redshift-Konsole erstellt wurde, können Sie eine benutzerdefinierte verwaltete Richtlinie an die IAM-Rolle anhängen.

Überblick über in der Konsole erstellte IAM-Rollen

Wenn Sie die Amazon-Redshift-Konsole zum Erstellen von IAM-Rollen verwenden, verfolgt Amazon Redshift alle IAM-Rollen, die über die Konsole erstellt wurden. Amazon Redshift wählt zum Erstellen

aller neuen Cluster und zum Wiederherstellen von Clustern aus Snapshots von sich aus die neueste IAM-Standardrolle aus.

Über die Konsole können Sie eine IAM-Rolle erstellen, die über eine Richtlinie mit Berechtigungen zum Ausführen von SQL-Befehlen verfügt. Zu diesen Befehlen gehören COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL und CREATE LIBRARY. Optional können Sie den Benutzerzugriff auf Ihre AWS -Ressourcen noch genauer steuern, indem Sie benutzerdefinierte Richtlinien erstellen und sie an die IAM-Rolle anfügen.

Wenn Sie eine IAM-Rolle erstellt und sie mit der Konsole als Standard für den Cluster festgelegt haben, brauchen Sie den Amazon-Ressourcenname (ARN) der IAM-Rolle nicht anzugeben, um die Authentifizierung und Autorisierung durchzuführen.

Verwenden der IAM-Rollen, die in der Konsole erstellt wurden

Bei der IAM-Rolle, die Sie über die Konsole für Ihren Cluster erstellen, ist die verwaltete Richtlinie `AmazonRedshiftAllCommandsFullAccess` automatisch angefügt. Diese IAM-Rolle ermöglicht es Amazon Redshift, Daten für AWS Ressourcen in Ihrem IAM-Konto zu kopieren, zu entladen, abzufragen und zu analysieren. Die verwaltete Richtlinie bietet Zugriff auf die Operationen COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL SCHEMA, CREATE MODEL und CREATE LIBRARY. Die Richtlinie gewährt auch Berechtigungen zur Ausführung von SELECT-Anweisungen für verwandte AWS Dienste wie Amazon S3, Amazon CloudWatch Logs SageMaker, Amazon und AWS Glue.

Die Befehle CREATE EXTERNAL FUNCTION, CREATE EXTERNAL SCHEMA, CREATE MODEL und CREATE LIBRARY haben das Stichwort `default` (Standard). Gemäß diesem Stichwort verwendet Amazon Redshift die IAM-Rolle, die als Standard festgelegt und mit dem Cluster verknüpft ist, wenn der Befehl ausgeführt wird. Sie können mit dem Befehl DEFAULT_IAM_ROLE die aktuelle IAM-Standardrolle überprüfen, die an den Cluster angefügt ist.

Um die Zugriffsberechtigungen der IAM-Rolle zu steuern, die für Ihren Redshift-Cluster erstellt und als Standard festgelegt wurde, verwenden Sie die Berechtigung ASSUMEROLE. Diese Zugriffssteuerung gilt für Datenbankbenutzer und -gruppen, wenn sie Befehle wie die oben aufgeführten ausführen. Nachdem Sie einem Benutzer oder einer Gruppe die Berechtigung ASSUMEROLE für eine IAM-Rolle erteilt haben, kann der Benutzer oder die Gruppe diese Rolle übernehmen, wenn diese Befehle ausgeführt werden. Mit der Berechtigung ASSUMEROLE können Sie bei Bedarf Zugriff auf die entsprechenden Befehle gewähren.

Mit der Amazon-Redshift-Konsole können Sie Folgendes tun:

- Erstellen einer IAM-Rolle als Standard
- Entfernen von IAM-Rollen aus Ihrem Cluster
- Zuweisen von IAM-Rollen zum Cluster
- Festlegen einer IAM-Rolle als Standard
- Aufheben des Standardstatus bei einer IAM-Rolle im Cluster

Berechtigungen der AmazonRedshiftAllCommandsFullAccess verwalteten Richtlinie

Im folgenden Beispiel sehen Sie die Berechtigungen in der verwalteten Richtlinie `AmazonRedshiftAllCommandsFullAccess`, die bestimmte Aktionen für diejenige IAM-Rolle zulässt, die als Standard für Ihren Cluster festgelegt ist. Die IAM-Rolle mit angehängten Berechtigungsrichtlinien bestimmt, was ein Benutzer oder eine Gruppe tun kann und was nicht. Angesichts dieser Berechtigungen können Sie den Befehl COPY von Amazon S3 aus ausführen. Außerdem können Sie UNLOAD und CREATE MODEL verwenden.

```
{
            "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*/*"
            ]
```

```
}
```

Im folgenden Beispiel sehen Sie die Berechtigungen in der verwalteten Richtlinie `AmazonRedshiftAllCommandsFullAccess`, die bestimmte Aktionen für diejenige IAM-Rolle zulässt, die als Standard für den Cluster festgelegt ist. Die IAM-Rolle mit angehängten Berechtigungsrichtlinien bestimmt, was ein Benutzer oder eine Gruppe tun kann und was nicht. Mit den folgenden Berechtigungen können Sie den Befehl CREATE EXTERNAL FUNCTION ausführen.

```
{
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": "arn:aws:lambda:*:*:function:*redshift*"
}
```

Im folgenden Beispiel sehen Sie die Berechtigungen in der verwalteten Richtlinie `AmazonRedshiftAllCommandsFullAccess`, die bestimmte Aktionen für diejenige IAM-Rolle zulässt, die als Standard für den Cluster festgelegt ist. Die IAM-Rolle mit angehängten Berechtigungsrichtlinien bestimmt, was ein Benutzer oder eine Gruppe tun kann und was nicht. Angesichts der folgenden Berechtigungen können Sie die Befehle CREATE EXTERNAL SCHEMA und CREATE EXTERNAL TABLE ausführen, die für Amazon Redshift Spectrum benötigt werden.

```
{
            "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*"
            ]
}
```

Im folgenden Beispiel sehen Sie die Berechtigungen in der verwalteten Richtlinie `AmazonRedshiftAllCommandsFullAccess`, die bestimmte Aktionen für diejenige IAM-Rolle zulassen, die als Standard für den Cluster festgelegt ist. Die IAM-Rolle mit angehängten Berechtigungsrichtlinien bestimmt, was ein Benutzer oder eine Gruppe tun kann und was nicht. Angesichts der folgenden Berechtigungen können Sie den Befehl CREATE EXTERNAL SCHEMA mit Verbundabfragen ausführen.

```
{
            "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"
                }
            }
```

```
},
```

Verwalten von IAM-Rollen, die mit der Konsole für einen Cluster erstellt wurden

Um IAM-Rollen, die in der Amazon-Redshift-Konsole erstellt wurden, zu erstellen, zu ändern und zu entfernen, verwenden Sie den Abschnitt Cluster in der Konsole.

Erstellen einer IAM-Rolle als Standard

In der Konsole können Sie eine IAM-Rolle für Ihren Cluster erstellen, der die Richtlinie `AmazonRedshiftAllCommandsFullAccess` automatisch angefügt ist. Die neue IAM-Rolle ermöglicht es Amazon Redshift dann, Daten von Amazon-Ressourcen in Ihrem IAM-Konto zu kopieren, zu laden, abzufragen und zu analysieren.

Es kann nur eine IAM-Rolle als Standard für den Cluster festgelegt werden. Wenn Sie eine andere IAM-Rolle als Cluster-Standard erstellen und gerade eine vorhandene IAM-Rolle als Standard zugewiesen wird, ersetzt die neue IAM-Rolle die andere als Standard.

Einen neuen Cluster und eine IAM-Rolle erstellen, die als Standard für den neuen Cluster festgelegt ist

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Die aktuellen Cluster für Ihr Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie Create cluster (Cluster erstellen) aus, um einen Cluster zu erstellen.
4. Folgen Sie den Anweisungen auf der Konsolenseite, um die Eigenschaften für die Cluster configuration (Clusterkonfiguration) einzugeben. Weitere Informationen zu diesem Schritt finden Sie unter Erstellen eines Clusters.
5. (Optional) Wählen Sie Load sample data (Beispieldaten laden) aus, um den Beispieldatensatz in Ihren Amazon-Redshift-Cluster zu laden und mit dem Abfrage-Editor Daten abzufragen.

   Wenn Sie sich hinter einer Firewall befinden, muss der Datenbank-Port ein offener Port sein, der eingehende Verbindungen akzeptiert.
6. Folgen Sie den Anweisungen auf der Konsolenseite, um Eigenschaften für die Database configurations (Datenbankkonfiguration) einzugeben.

7. Unter Cluser permissions (Cluster-Berechtigungen) wählen Sie bei Manage IAM roles (IAM-Rollen verwalten) die Option Create IAM role (IAM-Rolle erstellen) aus.
8. Geben Sie einen Amazon S3 Bucket an, auf den die IAM-Rolle zugreifen soll, indem Sie eine der folgenden Methoden wählen:
   - Wählen Sie No additional Amazon S3 bucket (Kein zusätzlicher Amazon S3 Bucket) aus, um die IAM-Rolle zu erstellen, ohne bestimmte Amazon S3 Buckets anzugeben.
   - Wählen Sie Any Amazon S3 bucket (Jeder Amazon S3 Bucket) aus, damit Benutzer, die Zugriff auf Ihren Amazon-Redshift-Cluster haben, auch auf jeden Amazon S3 Bucket und dessen Inhalt in Ihrem AWS-Konto zugreifen können.
   - Wählen Sie Specific Amazon S3 buckets (Bestimmte Amazon S3 Buckets) aus, um einen oder mehrere Amazon S3 Buckets anzugeben, auf die die erstellte IAM-Rolle Zugriff hat. Wählen Sie dann einen oder mehrere Amazon S3 Buckets aus der Tabelle aus.
9. Wählen Sie Create IAM role as default (IAM-Rolle als Standard erstellen) aus. Amazon Redshift erstellt die IAM-Rolle und legt sie automatisch als Standard für Ihren Cluster fest.
10. Wählen Sie Create cluster (Cluster erstellen) aus, um den Cluster zu erstellen. Es kann einige Minuten dauern, bis der Cluster zur Verwendung bereit ist.

Entfernen von IAM-Rollen aus Ihrem Cluster

Sie können eine oder mehrere IAM-Rollen aus Ihrem Cluster entfernen.

IAM-Rollen aus dem Cluster entfernen

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Die aktuellen Cluster für Ihr Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie den Cluster aus, von dem Sie die IAM-Rolle entfernen möchten.
4. Wählen Sie unter Custer permissions (Cluster-Berechtigungen) eine oder mehrere IAM-Rollen aus, die Sie aus dem Cluster entfernen möchten.
5. Wählen Sie unter Manage IAM roles (IAM-Rollen verwalten) die Option Remove IAM roles (IAM-Rollen entfernen) aus.

Zuweisen von IAM-Rollen zum Cluster

Sie können Ihrem Cluster eine oder mehrere IAM-Rollen zuordnen.

IAM-Rollen dem Cluster zuweisen

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Die aktuellen Cluster für Ihr Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie den Cluster aus, dem Sie IAM-Rollen zuordnen möchten.
4. Wählen Sie unter Cluster permissions (Clusterberechtigungen) eine oder mehrere IAM-Rollen aus, die Sie dem Cluster zuordnen möchten.
5. Wählen Sie unter Manage IAM roles (IAM-Rollen verwalten) die Option Associate IAM roles (IAM-Rollen zuordnen) aus.
6. Wählen Sie eine oder mehrere IAM-Rollen aus, die Sie dem Cluster zuordnen möchten.
7. Wählen Sie dann Associate IAM role (IAM-Rolle zuordnen) aus.

Festlegen einer IAM-Rolle als Standard

Sie können eine IAM-Rolle als Standard für einen Cluster festlegen.

Eine IAM-Rolle zur Standardeinstellung für den Cluster machen

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Die aktuellen Cluster für Ihr Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie den Cluster aus, für den Sie eine IAM-Standardrolle festlegen möchten.
4. Wählen Sie unter Cluster permissions (Clusterberechtigungen) bei Associated IAM roles (Zugeordnete IAM-Rollen) eine IAM-Rolle aus, die Sie als Standard für den Cluster festlegen möchten.
5. Wählen Sie unter Set default (Standard festlegen) die Option Make default (Als Standard festlegen) aus.

6. Wählen Sie bei der entsprechenden Aufforderung Set default (Standard festlegen) aus, um zu bestätigen, dass die angegebene IAM-Rolle die Standardrolle sein soll.

Aufheben des Standardstatus bei einer IAM-Rolle im Cluster

Sie können einstellen, dass eine bestimmte IAM-Rolle nicht mehr die Standardrolle für Ihren Cluster sein soll.

Eine IAM-Rolle als Standard im Cluster löschen

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Die aktuellen Cluster für Ihr Konto AWS-Region sind aufgeführt. Eine Teilmenge der Eigenschaften jedes Clusters wird in den Spalten der Liste angezeigt.
3. Wählen Sie den Cluster aus, dem Sie IAM-Rollen zuordnen möchten.
4. Wählen Sie unter Cluster permissions (Clusterberechtigungen) bei Associated IAM roles (Zugeordnete IAM-Rollen) die Standard-IAM-Rolle aus.
5. Wählen Sie unter Set default (Standard festlegen) die Option Clear default (Standard löschen) aus.
6. Wählen Sie nach der Aufforderung Clear default (Standard löschen) aus, um zu bestätigen, dass die angegebene IAM-Rolle kein Standard mehr sein soll.

Verwaltung der auf dem Cluster erstellten IAM-Rollen mithilfe der AWS CLI

Sie können die AWS CLI nutzen, um IAM-Rollen zu verwalten, die im Cluster erstellt wurden.

Einen Amazon-Redshift-Cluster mit einer IAM-Rolle als Standard erstellen

Verwenden Sie den Befehl, um einen Amazon Redshift Redshift-Cluster mit einer IAM-Rolle als Standard für den Cluster zu erstellen. `aws redshift create-cluster` AWS CLI

Der folgende AWS CLI Befehl erstellt einen Amazon Redshift Redshift-Cluster und die IAM-Rolle mit dem Namen myrole1. Der AWS CLI Befehl legt außerdem myrole1 als Standard für den Cluster fest.

```
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'
```

Der folgende Codeausschnitt ist ein Beispiel für die Antwort.

```
{
    "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"
            }
        ]
        ...
    }
}
```

Einem Amazon-Redshift-Cluster eine oder mehrere IAM-Rollen hinzufügen

Verwenden Sie den Befehl, um eine oder mehrere dem Cluster zugeordnete IAM-Rollen hinzuzufügen. `aws redshift modify-cluster-iam-roles` AWS CLI

Der folgende AWS CLI Befehl fügt dem Cluster `myrole3` und `myrole4` hinzu.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3'
 'arn:aws:iam::012345678910:role/myrole4'
```

Der folgende Codeausschnitt ist ein Beispiel für die Antwort.

```
{
```

```
    "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"
            }
        ],
        ...
    }
}
```

Eine oder mehrere IAM-Rollen aus einem Amazon-Redshift-Cluster entfernen

Verwenden Sie den `aws redshift modify-cluster-iam-roles` AWS CLI Befehl, um eine oder mehrere dem Cluster zugeordnete IAM-Rollen zu entfernen.

Mit dem folgenden AWS CLI Befehl werden `myrole3` und `myrole4` aus dem Cluster entfernt.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --remove-iam-roles 'arn:aws:iam::012345678910:role/myrole3'
 'arn:aws:iam::012345678910:role/myrole4'
```

Der folgende Codeausschnitt ist ein Beispiel für die Antwort.

```
{
    "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"
            }
        ],
        ...
    }
}
```

Eine zugeordnete IAM-Rolle als Standard für den Cluster festlegen

Verwenden Sie den `aws redshift modify-cluster-iam-roles` AWS CLI Befehl, um eine zugeordnete IAM-Rolle als Standard für den Cluster festzulegen.

Der folgende AWS CLI Befehl ist `myrole2` der Standard für den Cluster.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole2'
```

Der folgende Codeausschnitt ist ein Beispiel für die Antwort.

```
{
    "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"
            }
        ],
        ...
    }
}
```

Eine nicht zugeordnete IAM-Rolle als Standard für den Cluster festlegen

Verwenden Sie den Befehl, um eine nicht zugeordnete IAM-Rolle als Standard für den Cluster festzulegen. `aws redshift modify-cluster-iam-roles` AWS CLI

Der folgende AWS CLI Befehl erweitert `myrole2` den Amazon Redshift Redshift-Cluster und legt ihn als Standard für den Cluster fest.

```
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'
```

Der folgende Codeausschnitt ist ein Beispiel für die Antwort.

```
{
    "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"
            }
        ],
        ...
    }
}
```

Einen Cluster aus einem Snapshot wieder herstellen und eine IAM-Rolle als Standard festlegen

Wenn Sie Ihren Cluster aus einem Snapshot wiederherstellen, können Sie entweder eine vorhandene IAM-Rolle zuordnen oder eine neue erstellen und als Standard für den Cluster festlegen.

Verwenden Sie den Befehl, um einen Amazon Redshift Redshift-Cluster aus einem Snapshot wiederherzustellen und eine IAM-Rolle als Cluster-Standard festzulegen. `aws redshift restore-from-cluster-snapshot` AWS CLI

Der folgende AWS CLI Befehl stellt den Cluster aus einem Snapshot wieder her und legt ihn `myrole2` als Standard für den Cluster fest.

```
aws redshift restore-from-cluster-snapshot \
    --cluster-identifier mycluster-clone \
    --snapshot-identifier my-snapshot-id
    --iam-roles 'arn:aws:iam::012345678910:role/myrole1'
 'arn:aws:iam::012345678910:role/myrole2' \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

Der folgende Codeausschnitt ist ein Beispiel für die Antwort.

```
{
    "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"
            }
        ],
        ...
    }
}
```

Verwenden einer Verbundidentität zur Verwaltung des Amazon-Redshift-Zugriffs auf lokale Ressourcen und externe Amazon-Redshift-Spectrum-Tabellen

Die Verwendung eines Identitätsverbunds AWS zusammen mit den von bereitgestellten Anmeldeinformationen `GetDatabaseCredentials` kann die Autorisierung und den Zugriff auf lokale Daten und externe Daten vereinfachen. Um Benutzern Zugriff auf externe Daten zu gewähren, die sich in Amazon S3 befinden, erstellen Sie derzeit eine IAM-Rolle mit Berechtigungen, die in einer Berechtigungsrichtlinie definiert sind. Anschließend können Benutzer mit der angehängten Rolle auf die externen Daten zugreifen. Dies funktioniert, aber wenn Sie detaillierte Regeln bereitstellen möchten, z. B. dass bestimmte Spalten für einen bestimmten Benutzer nicht verfügbar sind, müssen Sie möglicherweise eine zusätzliche Konfiguration für das externe Schema erstellen. In diesem Thema zeigen wir, wie Sie mithilfe eines AWS Identitätsverbunds Zugriff auf Ressourcen gewähren können, anstatt eine bestimmte IAM-Rolle zu verwenden. Ein Identitätsverbund mit Anmeldeinformationen, die von bereitgestellt werden`GetDatabaseCredentials`, kann den Zugriff auf AWS Glue und Redshift Spectrum-Ressourcen über detaillierte IAM-Regeln ermöglichen, die einfacher zu spezifizieren und zu ändern sind. Dies erleichtert das Anwenden eines Zugriffs, der Ihren Geschäftsregeln entspricht.

Die Verwendung von Verbundanmeldeinformationen bietet folgende Vorteile:

- Sie müssen keine an einen Cluster angefügten IAM-Rollen für Redshift Spectrum verwalten.
- Clusteradministratoren können ein externes Schema erstellen, auf das Nutzer mit unterschiedlichen IAM-Kontexten zugreifen können. Dies ist beispielsweise nützlich, um eine Spaltenfilterung für eine Tabelle durchzuführen, bei der verschiedene Nutzer dasselbe externe Schema abfragen und unterschiedliche Felder in zurückgegebenen Datensätzen erhalten.
- Sie können Amazon Redshift mit einem Benutzer mit IAM-Berechtigungen abfragen und nicht nur mit einer Rolle.

Vorbereiten einer Identität für die Anmeldung mit einer Verbundidentität

Bevor Sie sich mit einer Verbundidentität anmelden, müssen Sie mehrere vorbereitende Schritte ausführen. In diesen Anweisungen wird davon ausgegangen, dass ein externes Redshift-Spectrum-Schema vorhanden ist, das auf eine in einem Amazon-S3-Bucket gespeicherte Datendatei verweist, und dass sich der Bucket in demselben Konto befindet wie Ihr Amazon Redshift-Cluster oder Ihr Amazon Redshift Serverless Data Warehouse.

1. Erstellen Sie eine IAM-Identität. Dabei kann es sich um einen Benutzer oder eine IAM-Rolle handeln. Verwenden Sie einen beliebigen von IAM unterstützten Namen.
2. Hängen Sie Berechtigungsrichtlinien an eine Identität an. Geben Sie einen der folgenden Werte an:

   - `redshift:GetClusterCredentialsWithIAM` (für einen von Amazon Redshift bereitgestellten Cluster)
   - `redshift-serverless:GetCredentials` (für Amazon Redshift Serverless)

   Sie können über die IAM-Konsole Berechtigungen mit dem Richtlinien-Editor hinzufügen.

   Die IAM-Identität benötigt auch Berechtigungen für den Zugriff auf externe Daten. Gewähren Sie Zugriff auf Amazon S3, indem Sie die folgenden AWS verwalteten Richtlinien direkt hinzufügen:

   - `AmazonS3ReadOnlyAccess`
   - `AWSGlueConsoleFullAccess`

   Die zuletzt verwaltete Richtlinie ist erforderlich, wenn Sie sie AWS Glue zur Vorbereitung Ihrer externen Daten verwenden. Weitere Informationen zu den Schritten, mit denen Sie Zugriffs auf Amazon Redshift Spectrum gewähren, finden Sie in Erstellen einer IAM-Rolle für Amazon Redshift. Der Abschnitt ist Teil des Handbuchs „Erste Schritte für Amazon Redshift und Redshift Spectrum“. Darin finden Sie Schritte zum Hinzufügen von IAM-Richtlinien für den Zugriff auf Redshift Spectrum.
3. Richten Sie Ihren SQL-Client für die Verbindung zu Amazon Redshift ein. Verwenden Sie den Amazon-Redshift-JDBC-Treiber und fügen Sie die Anmeldeinformationen Ihres Benutzers den Anmeldeinformationen des Tools hinzu. Ein Client wie SQL Workbench/J ist dafür gut geeignet. Legen Sie die folgenden erweiterten Eigenschaften für Client-Verbindungen fest:

   - AccessKeyID — Ihre Zugriffsschlüssel-ID.

- SecretAccessKey— Ihr geheimer Zugangsschlüssel. (Beachten Sie das Sicherheitsrisiko bei der Übertragung des geheimen Schlüssels, wenn Sie keine Verschlüsselung verwenden.)
- SessionToken— Eine Reihe temporärer Anmeldeinformationen für eine IAM-Rolle.
- groupFederation — Legen Sie diese Option auf `true` fest, wenn Sie die Verbundidentität für einen bereitgestellten Cluster konfigurieren. Legen Sie diesen Parameter nicht fest, wenn Sie Amazon Redshift Serverless verwenden.
- LogLevel— Ganzzahlwert auf Protokollebene. Dieser Schritt ist optional.

4. Legen Sie die URL für den JDBC-Endpunkt fest, der sich in der Amazon-Redshift- oder Amazon-Redshift-Serverless-Konsole befindet. Ersetzen Sie Ihr URL-Schema durch jdbc:redshift:iam: und verwenden Sie diese Formatierung:

   - Format für einen von Amazon Redshift bereitgestellten Cluster: `jdbc:redshift:iam://<cluster_id>.<unique_suffix>.<region>.redshift.amazonaws.com:<port>/<database_name>`

     Beispiel: `jdbc:redshift:iam://test1.12345abcdefg.us-east-1.redshift.amazonaws.com:5439/dev`
   - Format für Amazon Redshift Serverless: `jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com:5439:<port>/<database_name>`

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

   Nachdem Sie mithilfe einer IAM-Identität zum ersten Mal eine Verbindung mit der Datenbank hergestellt haben, erstellt Amazon Redshift automatisch eine Amazon-Redshift-Identität mit demselben Namen, dem Präfix `IAM:` für einen Benutzer oder `IAMR:` für eine IAM-Rolle. Die verbleibenden Schritte in diesem Thema zeigen Beispiele für einen Benutzer.

   Wenn ein Redshift-Benutzer nicht automatisch erstellt wird, können Sie einen erstellen, indem Sie unter Verwendung eines Administratorkontos eine `CREATE USER`-Anweisung ausführen und den Benutzernamen im Format`IAM:<user name>` angeben.

5. Erteilen Sie als Amazon-Redshift-Clusteradministrator dem Redshift-Benutzer die erforderlichen Berechtigungen für den Zugriff auf das externe Schema.

```
GRANT ALL ON SCHEMA my_schema to "IAM:my_user";
```

Damit Ihr Redshift-Benutzer Tabellen im externen Schema erstellen kann, muss er ein Schemabesitzer sein. Beispielsweise:

```
ALTER SCHEMA my_schema owner to "IAM:my_user";
```

6. Zur Überprüfung der Konfiguration führen Sie mithilfe des SQL-Clients eine Abfrage als Benutzer aus, nachdem die Berechtigungen erteilt wurden. Dieses Abfragebeispiel ruft Daten aus einer externen Tabelle ab.

```
SELECT * FROM my_schema.my_table;
```

Erste Schritte bei der Identitäts- und Autorisierungsweitergabe an Redshift Spectrum

Um eine Verbundidentität an externe Abfragetabellen zu übergeben, legen Sie `SESSION` als Wert für den `IAM_ROLE`-Abfrageparameter von `CREATE EXTERNAL SCHEMA` fest. In den folgenden Schritten wird gezeigt, wie Sie `SESSION` einrichten und nutzen, um Abfragen im externen Schema zu autorisieren.

1. Erstellen Sie lokale Tabellen und externe Tabellen. Dafür eignen sich auch externe Tabellen, die mit AWS Glue katalogisiert wurden.
2. Stellen Sie mit Ihrer IAM-Identität eine Verbindung mit Amazon Redshift her. Wie im vorherigen Abschnitt erwähnt, wird ein Redshift-Datenbankbenutzer erstellt, wenn die Identität eine Verbindung mit Amazon Redshift herstellt. Der Benutzer wird erstellt, wenn er zuvor nicht vorhanden war. Wenn der Benutzer neu ist, muss der Administrator ihm Berechtigungen zum Ausführen von Aufgaben in Amazon Redshift gewähren, wie das Abfragen und Erstellen von Tabellen.
3. Stellen Sie mit Ihrem Administratorkonto eine Verbindung mit Redshift her. Führen Sie den Befehl aus, um ein externes Schema mit dem Wert „`SESSION`“ zu erstellen.

```
create external schema spectrum_schema from data catalog
database '<my_external_database>'
region '<my_region>'
iam_role 'SESSION'
catalog_id '<my_catalog_id>';
```

Beachten Sie, dass in diesem Fall „`catalog_id`“ festgelegt ist. Dies ist eine neue Einstellung, die mit der Funktion hinzugefügt wurde, da „`SESSION`“ eine bestimmte Rolle ersetzt.

In diesem Beispiel ahmen die Werte in der Abfrage nach, wie echte Werte angezeigt werden.

```
create external schema spectrum_schema from data catalog
database 'spectrum_db'
region 'us-east-1'
iam_role 'SESSION'
catalog_id '123456789012'
```

Der `catalog_id` Wert ist in diesem Fall Ihre AWS Konto-ID.

4. Führen Sie Abfragen aus, um auf Ihre externen Daten zuzugreifen. Verwenden Sie dabei die IAM-Identität, mit der Sie in Schritt 2 eine Verbindung hergestellt haben. Zum Beispiel:

```
select * from spectrum_schema.table1;
```

In diesem Fall kann `table1` beispielsweise in JSON formatierte Daten in einer Datei in einem Amazon-S3-Bucket, verwendet werden.

5. Wenn Sie bereits über ein externes Schema verfügen, das eine an einen Cluster angehängte IAM-Rolle verwendet und auf Ihre externe Datenbank oder Ihr externes Schema verweist, können Sie wie in diesen Schritten beschrieben entweder das vorhandene Schema ersetzen und eine Verbundidentität verwenden, oder eine neue erstellen.

`SESSION` gibt an, dass Anmeldeinformationen für die Verbundidentität verwendet werden, um das externe Schema abzufragen. Wenn Sie den Abfrageparameter „`SESSION`“ verwenden, stellen Sie sicher, dass Sie die „`catalog_id`“ festlegen. Sie ist erforderlich, da sie auf den für das Schema verwendeten Datenkatalog verweist. Zuvor wurde `catalog_id` aus dem Wert abgerufen, dem `iam_role` zugewiesen wurde. Wenn Sie die Identitäts- und Autorisierungspropagierung auf diese Weise übergeben, z. B. an Redshift Spectrum, indem Sie Verbundanmeldeinformationen zum Abfragen eines externen Schemas verwenden, ist eine Autorisierung über eine IAM-Rolle nicht erforderlich.

Nutzungshinweise

Ein häufiger Verbindungsfehler ist der folgende: IAM-Fehler beim Abrufen der temporären Anmeldeinformationen: Die Ausnahmeantwort konnte mit den bereitgestellten Unmarshallers nicht rückgängig gemacht werden. Dieser Fehler ist auf einen veralteten JDBC-Treiber zurückzuführen. Die Treiberversion, die für die Verbundidentität mindestens erforderlich ist, ist 2.1.0.9. Download the

Amazon Redshift JDBC driver, version 2.1Den JDBC-Treiber können Sie unter Herunterladen von Version 2.1 des JDBC-Treibers für Amazon Redshift abrufen.

Weitere Ressourcen

Diese Links bieten zusätzliche Informationen zur Verwaltung des Zugriffs auf externe Daten.

- Sie können weiterhin mithilfe einer IAM-Rolle auf Redshift-Spectrum-Daten zugreifen. Weitere Informationen finden Sie unter Amazon Redshift autorisieren, in Ihrem Namen auf andere AWS Dienste zuzugreifen.
- Wenn Sie den Zugriff auf externe Tabellen mit verwalten AWS Lake Formation, können Sie diese mithilfe von Redshift Spectrum mit föderierten IAM-Identitäten abfragen. Sie müssen keine an Cluster angeschlossenen IAM-Rollen mehr verwalten, damit Redshift Spectrum Daten abfragen kann, bei denen registriert wurde. AWS Lake Formation Weitere Informationen finden Sie unter Verwenden AWS Lake Formation mit Amazon Redshift Spectrum.

Verwaltung von Amazon Redshift Redshift-Administratorkennwörtern mit AWS Secrets Manager

Amazon Redshift kann integriert werden AWS Secrets Manager , um Ihre Administratoranmeldedaten innerhalb eines verschlüsselten Geheimnisses zu generieren und zu verwalten. Mit AWS Secrets Manager können Sie Ihre Administratorkennwörter durch einen API-Aufruf ersetzen, um das Geheimnis bei Bedarf programmgesteuert abzurufen. Die Verwendung von Secrets anstelle hartkodierter Anmeldeinformationen reduziert das Risiko für eine Offenlegung oder Kompromittierung dieser Anmeldeinformationen. Weitere Informationen zu AWS Secrets Manager finden Sie im AWS Secrets Manager Benutzerhandbuch.

Sie können angeben, dass Amazon Redshift Ihr Admin-Passwort verwaltet AWS Secrets Manager , indem Sie einen der folgenden Vorgänge ausführen:

- Erstellen eines bereitgestellten Clusters oder Serverless-Namespace
- Wiederherstellen eines Clusters oder Serverless-Namespace aus einem Snapshot

Wenn Sie angeben, dass Amazon Redshift das Administratorkennwort in verwaltet AWS Secrets Manager, generiert Amazon Redshift das Passwort und speichert es in Secrets Manager. Sie können direkt auf das Geheimnis zugreifen, AWS Secrets Manager um die Anmeldeinformationen für den Admin-Benutzer abzurufen. Optional können Sie einen vom Kunden verwalteten Schlüssel angeben,

um das Geheimnis zu verschlüsseln, falls Sie von einem anderen AWS Konto aus auf das Geheimnis zugreifen müssen. Sie können auch den KMS-Schlüssel verwenden, den AWS Secrets Manager bereitstellt.

Amazon Redshift verwaltet die Einstellungen für das Secret und rotiert das Secret standardmäßig alle 30 Tage. Sie können das Secret jederzeit manuell rotieren. Wenn Sie einen bereitgestellten Cluster oder serverlosen Namespace löschen, in dem ein geheimes Geheimnis verwaltet wird AWS Secrets Manager, werden das Geheimnis und die zugehörigen Metadaten ebenfalls gelöscht.

Um eine Verbindung zu einem Cluster oder einem Serverless-Namespace herzustellen, dessen Anmeldeinformationen in einem Secret verwaltet werden, können Sie das Secret über die Secrets-Manager-Konsole oder den Secret-Manager-API-Aufruf `GetSecretValue` aus AWS Secrets Manager abrufen. Weitere Informationen finden Sie im Benutzerhandbuch unter Abrufen von Geheimnissen aus AWS Secrets Manager und Herstellen einer Verbindung zu einer SQL-Datenbank mit Anmeldeinformationen in einem AWS Secrets Manager Geheimnis herstellen.AWS Secrets Manager

Für die AWS Secrets Manager Integration sind Berechtigungen erforderlich

Benutzer müssen über die erforderlichen Berechtigungen verfügen, um Vorgänge im Zusammenhang mit der AWS Secrets Manager Integration ausführen zu können. Sie können IAM-Richtlinien erstellen, die Berechtigungen zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die benötigt werden. Sie können diese Richtlinien dann den IAM-Berechtigungssätzen oder -Rollen anfügen, die diese Berechtigungen benötigen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Der Benutzer, der angibt, dass Amazon Redshift das Admin-Passwort verwaltet, AWS Secrets Manager muss über die erforderlichen Berechtigungen verfügen, um die folgenden Operationen durchzuführen:

- `secretsmanager:CreateSecret`
- `secretsmanager:RotateSecret`
- `secretsmanager:DescribeSecret`
- `secretsmanager:UpdateSecret`
- `secretsmanager:DeleteSecret`
- `secretsmanager:GetRandomPassword`
- `secretsmanager:TagResource`

Wenn der Benutzer im Parameter `MasterPasswordSecretKmsKeyId` für bereitgestellte Cluster oder im Parameter `AdminPasswordSecretKmsKeyId` für Serverless-Namespaces einen KMS-Schlüssel übergeben möchte, benötigt er zusätzlich zu den oben aufgeführten Berechtigungen die folgenden Berechtigungen.

- `kms:Decrypt`
- `kms:GenerateDataKey`
- `kms:CreateGrant`
- `kms:RetireGrant`

Rotieren des Secrets mit dem Administratorpasswort

Standardmäßig rotiert Amazon Redshift das Secret automatisch alle 30 Tage, um sicherzustellen, dass die Anmeldeinformationen nicht über einen längeren Zeitraum unverändert bleiben. Wenn Amazon Redshift ein geheimes Admin-Passwort rotiert, AWS Secrets Manager aktualisiert es das bestehende Secret, sodass es ein neues Admin-Passwort enthält. Amazon Redshift ändert das Administratorpasswort für den Cluster so, dass es mit dem Passwort im aktualisierten Secret übereinstimmt.

Sie können mit AWS Secrets Manager ein Secret sofort rotieren, anstatt auf eine geplante Rotation zu warten. Weitere Informationen zur Rotation von Geheimnissen finden Sie unter Rotation von AWS Secrets Manager Geheimnissen im AWS Secrets Manager Benutzerhandbuch.

Abrufen des Amazon-Ressourcennamens (ARN) des Secrets in Amazon Redshift

Sie können über die Amazon-Redshift-Konsole den Amazon-Ressourcennamen (ARN) aller Secrets anzeigen, die von AWS Secrets Manager verwaltet werden. Sobald Sie den ARN des Geheimnisses haben, können Sie Details zu Ihrem Geheimnis und den verschlüsselten Daten in Ihrem Geheimnis mithilfe von AWS Secrets Manager. Weitere Informationen zum Abrufen von Secrets mittels des ARN finden Sie unter Abrufen von Secrets im AWS Secrets Manager -Benutzerhandbuch.

Anzeigen der Details zu einem Secret für einen von Amazon Redshift bereitgestellten Cluster

So zeigen Sie den Amazon-Ressourcennamen (ARN) des Secrets Ihres Clusters über die Amazon-Redshift-Konsole an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Bereich Cluster-Übersicht den Cluster aus, dessen Secret Sie anzeigen möchten.
3. Wählen Sie die Registerkarte Eigenschaften aus.
4. Zeigen Sie unter Administrator-Anmeldeinformationen-ARN den ARN des Secrets an. Dieser ARN ist der Bezeichner für das Geheimnis, mit dem Sie AWS Secrets Manager die Details des Geheimnisses einsehen können.

Anzeigen der Details zu einem Secret für einen Amazon-Redshift-Serverless-Namespace

So zeigen Sie den Amazon-Ressourcennamen (ARN) des Secrets Ihres Serverless-Namespace über die Amazon-Redshift-Konsole an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Dashboard Bereitgestellte Cluster oben rechts auf der Seite die Option Zu Serverless aus.
3. Scrollen Sie im Serverless-Dashboard zum Bereich Namespaces/Arbeitsgruppen und wählen Sie den Namespace aus, dessen Secret Sie anzeigen möchten.
4. Zeigen Sie im Bereich Allgemeine Informationen den ARN des Secrets unter Administrator-Anmeldeinformationen-ARN an. Dieser ARN ist der Bezeichner für das Geheimnis, mit dem Sie AWS Secrets Manager die Details des Geheimnisses einsehen können.

Ein Geheimnis für Datenbankverbindungsdaten erstellen

Sie können ein Secrets Manager Manager-Geheimnis erstellen, um Anmeldeinformationen zu speichern, die für die Verbindung zu einem von Amazon Redshift bereitgestellten Cluster oder Redshift Serverless Namespace und einer Arbeitsgruppe verwendet werden.

Um einen geheimen Schlüssel zu erstellen, der für die Verbindung zu einer Datenbank in einem bereitgestellten Cluster verwendet wird

1. Öffnen Sie die Secrets Manager Manager-Konsole (https://console.aws.amazon.com/secretsmanager/).
2. Wählen Sie Store a new secret (Ein neues Secret speichern).
3. Wählen Sie Anmeldeinformationen für den Amazon Redshift Redshift-Cluster aus.

Geben Sie Informationen ein für:

- Benutzername
- Passwort
- Verschlüsselungsschlüssel

Wählen Sie einen Cluster aus, für den Sie geheime Anmeldeinformationen erstellen möchten.

4. Wählen Sie Weiter, um zum nächsten Bildschirm zu gelangen.
5. Fügen Sie einen Tag-Schlüssel hinzu, der mit der Zeichenfolge „Redshift“ beginnt.
6. Geben Sie auf mehreren Bildschirmen weitere Informationen über Ihr Geheimnis ein, bis Sie Ihre Änderungen speichern.

Vergewissern Sie sich, dass eine Meldung angezeigt wird, dass das Geheimnis erfolgreich gespeichert wurde. Sie können das Geheimnis auch in der Secrets Manager-Konsole anzeigen. Sie können dieses Geheimnis verwenden, um mithilfe der Verbindungsmethode eine Verbindung zu einer Datenbank in einem Cluster auf der Amazon Redshift Redshift-Konsole und dem Amazon Redshift-Abfrage-Editor v2 AWS Secrets Manager herzustellen. Das Secret muss einen Tag-Schlüssel haben, der mit der Zeichenfolge „Redshift“ beginnt, damit das Secret in der Query Editor v2-Webanwendung aufgeführt wird.

Um ein Geheimnis zu erstellen, das für die Verbindung zu einer Datenbank in einer Redshift Serverless-Arbeitsgruppe verwendet wird

1. Öffnen Sie die Redshift Serverless-Konsole.
2. Navigieren Sie zur Namespace-Konfiguration.
3. Wählen Sie einen Namespace aus, für den Sie geheime Anmeldeinformationen erstellen möchten.
4. Öffnen Sie „Aktionen“, „Administratoranmeldedaten bearbeiten“.
5. Wählen Sie unter Admin-Passwort die Option Administratoranmeldedaten verwalten aus AWS Secrets Manager.
6. Wählen Sie Änderungen speichern aus, um Ihre Änderungen zu speichern.

Vergewissern Sie sich, dass eine Meldung angezeigt wird, dass das Passwort erfolgreich geändert wurde. Sie können das Geheimnis auch in der Secrets Manager-Konsole anzeigen. Sie können

dieses Geheimnis verwenden, um mithilfe der Verbindungsmethode eine Verbindung zu einer Datenbank in einer Arbeitsgruppe in der Redshift Serverless-Konsole und im Amazon Redshift Query Editor v2 herzustellen. AWS Secrets Manager Das Secret muss einen Tag-Schlüssel haben, der mit der Zeichenfolge „Redshift“ beginnt, damit das Secret in der Query Editor v2-Webanwendung aufgeführt wird.

Überlegungen zur Verwendung AWS Secrets Manager mit Amazon Redshift

Beachten Sie Folgendes AWS Secrets Manager , wenn Sie die Administratoranmeldedaten Ihres bereitgestellten Clusters oder Serverless-Namespaces zur Verwaltung verwenden:

- Wenn Sie einen Cluster pausieren, dessen Administratoranmeldedaten verwaltet werden AWS Secrets Manager, wird der geheime Schlüssel Ihres Clusters nicht gelöscht und der geheime Schlüssel wird Ihnen weiterhin in Rechnung gestellt. Secrets werden nur gelöscht, wenn Sie den Cluster löschen.
- Wenn Ihr Cluster angehalten wird, während Amazon Redshift versucht, das angefügte Secret zu rotieren, schlägt die Rotation fehl. In diesem Fall stoppt Amazon Redshift die automatische Rotation und versucht die Rotation nicht erneut, auch dann nicht, wenn Sie die Ausführung des Clusters fortsetzen. Sie müssen den Zeitplan für die automatische Rotation mithilfe des `secretsmanager:RotateSecret` API-Aufrufs neu starten, damit Ihr Geheimnis weiterhin AWS Secrets Manager automatisch rotiert wird.
- Wenn Ihrem serverlosen Namespace keine Arbeitsgruppe zugeordnet ist, wenn Amazon Redshift die Rotation des Secrets versucht, schlägt die Rotation fehl und wird nicht erneut versucht, auch dann nicht, wenn Sie eine Arbeitsgruppe hinzufügen. Sie müssen den Zeitplan für die automatische Rotation mithilfe des `secretsmanager:RotateSecret` API-Aufrufs neu starten, damit Ihr Geheimnis weiterhin AWS Secrets Manager automatisch rotiert wird.

Protokollierung und Überwachung in Amazon Redshift

Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Redshift und Ihrer AWS-Lösungen aufrechtzuerhalten. Sie können Überwachungsdaten aller Bestandteile Ihrer AWS-Lösung erfassen, damit Sie Ausfälle an mehreren Punkten leichter debuggen können. AWS bietet mehrere Tools für die Überwachung Ihrer Amazon-Redshift-Ressourcen und die Reaktion auf mögliche Vorfälle:

Amazon CloudWatch-Alarme

Mit Amazon-CloudWatch-Alarmen überwachen Sie eine Metrik über einen von Ihnen definierten Zeitraum. Wenn die Metrik einen bestimmten Schwellenwert überschreitet, wird eine Benachrichtigung an ein Amazon SNS-Thema oder eine AWS Auto Scaling-Richtlinie gesendet. CloudWatch-Alarme rufen keine Aktionen auf, nur weil sie einen besonderen Status haben. Der Status muss sich stattdessen geändert haben und für eine festgelegte Anzahl an Zeiträumen aufrechterhalten worden sein. Weitere Informationen finden Sie unter Verwalten von Alarmen. Eine Liste der -Metriken finden Sie unter Überwachung von Amazon Redshift mithilfe von Metriken CloudWatch .

AWS CloudTrail-Protokolle

CloudTrail bietet eine Aufzeichnung der von einem Benutzer, einer IAM-Rolle oder einem AWS-Service in Amazon Redshift durchgeführten API-Vorgänge. Mit den von CloudTrail gesammelten Informationen können Sie die an Amazon Redshift gestellte Anforderung, die IP-Adresse, von der die Anforderung gestellt wurde, den Initiator der Anforderung, den Zeitpunkt der Anforderung und weitere Angaben ermitteln. Weitere Informationen finden Sie unter Protokollieren mit CloudTrail.

Datenbank-Prüfungsprotokollierung

Amazon-Redshift-Protokolle stellen Informationen zu Verbindungen und Benutzeraktivitäten in Ihrer Datenbank bereit. Diese Protokolle helfen Ihnen, die Datenbank zu Sicherheits- und Fehlerbehebungszwecken zu überwachen. Dieser Prozess wird häufig als Datenbankprüfung bezeichnet. Die Protokolle können an folgenden Orten gespeichert werden:

- Amazon-S3-Buckets – Diese bieten Benutzern, die für die Überwachung der Aktivitäten in der Datenbank verantwortlich sind, Zugriff mit Datensicherheitsfunktionen.
- Amazon CloudWatch — Mithilfe der integrierten Funktionen, z. B. Visualisierungsfunktionen und Einstellungsaktionen CloudWatch, können Sie Daten zur Auditprotokollierung anzeigen.

> **Note**
>
> SYS_CONNECTION_LOG sammelt Verbindungsprotokolldaten für Amazon Redshift Serverless. Beachten Sie, dass Audit-Logging-Daten für Amazon Redshift Serverless nicht an Protokolldateien gesendet werden können, sondern nur an. CloudWatch

Themen

- Amazon-Redshift-Protokolle
- Aktivieren der Protokollierung
- Audit-Logs an Amazon senden CloudWatch
- Verwalten von Protokolldateien in Amazon S3
- Fehlerbehebung der Amazon-Redshift-Prüfungsprotokollierung in Amazon S3
- Protokollieren Amazon Redshift Redshift-API-Aufrufen mit AWS CloudTrail
- Konfigurieren von Prüfungen über die Konsole
- Konfiguration der Protokollierung mithilfe der AWS CLI Amazon Redshift Redshift-API

Amazon-Redshift-Protokolle

Amazon Redshift protokolliert Informationen in den folgenden Protokolldateien:

- Verbindungsprotokoll – Protokolliert Authentifizierungsversuche, Verbindungen und Verbindungstrennungen.
- Benutzerprotokoll – Protokolliert Informationen über Änderungen an Datenbankbenutzerdefinitionen.
- Benutzeraktivitätenprotokoll – Protokolliert jede Abfrage vor ihrer Ausführung in der Datenbank.

Die Verbindungs- und Benutzerprotokolle sind vor allem aus Zwecken der Sicherheit nützlich. Mit dem Verbindungsprotokoll können Sie Informationen über die Benutzer, die sich mit der Datenbank verbinden, und die zugehörigen Verbindungsinformationen überwachen. Diese Informationen können ihre IP-Adresse beim Stellen der Anfrage, die Art der verwendeten Authentifizierung und vieles mehr sein. Sie können das Benutzerprotokoll verwenden, um Änderungen der Definitionen von Datenbankbenutzern zu überwachen.

Das Benutzeraktivitätsprotokoll ist vor allem aus Zwecken der Fehlerbehebung nützlich. Es verfolgt Informationen über die Arten von Abfragen nach, die von Benutzern und vom System in der Datenbank ausgeführt werden.

Das Verbindungsprotokoll und das Benutzerprotokoll korrespondieren mit Informationen, die in den Systemtabellen in Ihrer Datenbank gespeichert sind. Sie können dieselben Informationen auch über die Systemtabellen erhalten. Die Protokolldateien bieten jedoch einen einfacheren Mechanismus für Abruf und Prüfung. Die Protokolldateien sind von Amazon-S3-Berechtigungen

anstatt Datenbankberechtigungen abhängig, um Abfragen für die Tabellen ausführen zu können. Zusätzlich reduzieren Sie die Auswirkungen von Interaktionen auf die Datenbank, da Sie die Informationen in Protokolldateien anzeigen, statt Abfragen für die Systemtabellen auszuführen.

> **Note**
>
> Protokolldateien sind nicht so aktuell wie die Systemprotokolltabellen STL_USERLOG und STL_CONNECTION_LOG. Datensätze, die älter sind als, aber nicht einschließlich, der letzte Datensatz, der in Protokolldateien kopiert wurde.

> **Note**
>
> Für Amazon Redshift Serverless sammelt SYS_CONNECTION_LOG Verbindungsprotokolldaten. Wenn Sie Auditprotokollierungsdaten für Amazon Redshift Serverless sammeln, können diese nicht an Protokolldateien gesendet werden, sondern nur an. CloudWatch

Verbindungsprotokoll

Protokolliert Authentifizierungsversuche sowie Verbindungen und Verbindungstrennungen. Die folgende Tabelle beschreibt die Informationen im Verbindungsprotokoll. Weitere Informationen zu diesen Feldern finden Sie unter STL_CONNECTION_LOG im Datenbankentwicklerhandbuch zu Amazon Redshift. Weitere Informationen zu gesammelten Verbindungsprotokolldaten für Amazon Redshift Serverless finden Sie unter SYS_CONNECTION_LOG.

Spaltenname	Beschreibung
event	Verbindungs- oder Authentifizierungsereignis.
recordtime	Uhrzeit, zu der das Ereignis aufgetreten ist.
remotehost	Name oder IP-Adresse des Remote-Hosts.
remoteport	Portnummer für den Remote-Host.
pid	Die mit der Anweisung verbundene Prozess-ID.

Spaltenname	Beschreibung
dbname	Datenbankname.
username	Benutzername.
authmethod	Authentifizierungsmethode.
duration	Dauer der Verbindung in Mikrosekunden.
sslversion	Secure Sockets Layer (SSL)-Version.
sslcipher	SSL-Verschlüsselungsverfahren.
mtu	Maximum Transmission Unit (MTU).
sslcompression	SSL-Kompressionstyp.
sslexpansion	SSL-Expansionstyp.
iamauthguid	Die AWS Identity and Access Management (IAM-) Authentifizierungs-ID für die Anfrage. AWS CloudTrail Dies ist die Kennung für den GetClusterCredentialsAPI-Aufruf zur Erstellung der Anmeldeinformationen, die für eine bestimmte Verbindung verwendet werden.
application_name	Der ursprüngliche oder aktualisierte Name der Anwendung für eine Sitzung.
os_version	Die Version des Betriebssystems, das sich auf dem Clientcomputer befindet, der eine Verbindung zu Ihrem Amazon-Redshift-Cluster herstellt.
driver_version	Die Version des ODBC- oder JDBC-Treibers, die von Ihren SQL-Client-Tools von Drittanbietern eine Verbindung zu Ihrem Amazon-Redshift-Cluster herstellt.
plugin_name	Der Name des Plug-Ins, mit dem Sie eine Verbindung zu Ihrem Amazon-Redshift-Cluster herstellen.
protocol_version	Die interne Protokollversion, die der Amazon-Redshift-Treiber beim Herstellen der Verbindung mit dem Server verwendet.
sessionid	Der global eindeutige Bezeichner für die aktuelle Sitzung.

Spaltenname	Beschreibung
Kompression	Der für die Verbindung verwendete Komprimierungsalgorithmus.

Benutzerprotokoll

Zeichnet die Details der folgenden Änderungen an einem Datenbankbenutzer auf:

- Benutzer erstellen
- Benutzer entfernen
- Benutzer ändern (umbenennen)
- Benutzer ändern (Eigenschaften ändern)

Spaltenname	Beschreibung
userid	ID des von der Änderung betroffenen Benutzers.
username	Benutzername des von der Änderung betroffenen Benutzers.
oldusername	Bei einer Umbenennungsaktion der ursprüngliche Benutzername. Bei anderen Aktionen ist dieses Feld leer.
Aktion	Erfolgte Aktion. Zulässige Werte: • Ändern • Erstellen • Entfernen • Umbenennen
usecreatedb	„True“ (1) zeigt an, dass der Benutzer über Berechtigungen zum Erstellen von Datenbanken verfügt.
usesuper	„True“ (1) zeigt an, dass es sich um einen Superuser handelt.
usecatupd	„True“ (1) zeigt an, dass der Benutzer Systemkataloge aktualisieren kann.
valuntil	Ablaufdatum des Passworts.

Spaltenname	Beschreibung
pid	Prozess-ID.
xid	Transaktions-ID.
recordtime	Zeitpunkt des Beginns der Abfrage, nach UTC.

Fragen Sie die SYS_USERLOG-Systemansicht ab, um zusätzliche Informationen über Änderungen für Benutzer zu finden. Diese Ansicht enthält Protokolldaten von Amazon Redshift Serverless.

Benutzeraktivitätsprotokoll

Protokolliert jede Abfrage vor ihrer Ausführung in der Datenbank.

Spaltenname	Beschreibung
recordtime	Uhrzeit, zu der das Ereignis aufgetreten ist.
db	Database name (Datenbankname).
user	Benutzername.
pid	Die mit der Anweisung verbundene Prozess-ID.
userid	Benutzer-ID.
xid	Transaktions-ID.
query	Ein Präfix von LOG: gefolgt vom Text der Abfrage einschließlich neuer Zeilen.

Aktivieren der Protokollierung

Prüfungsprotokollierung ist in Amazon Redshift standardmäßig nicht aktiviert. Wenn Sie die Protokollierung in Ihrem Cluster aktivieren, exportiert Amazon Redshift Protokolle nach Amazon CloudWatch oder erstellt und lädt Protokolle auf Amazon S3 hoch, die Daten vom Zeitpunkt der Aktivierung der Audit-Protokollierung bis heute erfassen. Jedes Protokollierungsupdate stellt eine Fortsetzung der vorherigen Protokolle dar.

Die Audit-Protokollierung bei CloudWatch oder in Amazon S3 ist ein optionaler Prozess. Die Protokollierung in Systemtabellen ist nicht optional und erfolgt automatisch. Weitere Informationen zur Protokollierung in Systemtabellen finden Sie in der Systemtabellenreferenz im Datenbankentwicklerhandbuch zu Amazon Redshift.

Das Verbindungsprotokoll, das Benutzerprotokoll und das Benutzeraktivitätsprotokoll werden zusammen mithilfe der AWS Management Console, der Amazon Redshift API-Referenz oder der AWS Command Line Interface (AWS CLI) aktiviert. Im Fall des Benutzeraktivitätsprotokolls müssen Sie auch den `enable_user_activity_logging`-Datenbankparameter aktivieren. Wenn Sie nur die Prüfprotokollierungsfunktion, aber nicht den zugehörigen Parameter aktivieren, protokolliert der Datenbank-Audit die Protokollinformationen nur für das Verbindungsprotokoll und das Benutzerprotokoll, nicht aber für das Protokoll der Benutzeraktivität. Der Parameter `enable_user_activity_logging` ist standardmäßig nicht aktiviert (`false`). Sie können ihn auf `true` festlegen, um das Benutzeraktivitätsprotokoll zu aktivieren. Weitere Informationen finden Sie unter Amazon-Redshift-Parametergruppen.

Audit-Logs an Amazon senden CloudWatch

Wenn Sie die Protokollierung aktivieren CloudWatch, exportiert Amazon Redshift Cluster-Verbindungs-, Benutzer- und Benutzeraktivitätsprotokolldaten in eine Amazon CloudWatch Logs-Protokollgruppe. Die Protokolldaten ändern sich in Bezug auf das Schema nicht. CloudWatch wurde für die Überwachung von Anwendungen entwickelt, und Sie können damit Echtzeitanalysen durchführen oder es so einrichten, dass Aktionen ausgeführt werden. Sie können Amazon CloudWatch Logs auch verwenden, um Ihre Protokolldatensätze in einem dauerhaften Speicher zu speichern.

Die Verwendung CloudWatch zum Anzeigen von Protokollen ist eine empfohlene Alternative zum Speichern von Protokolldateien in Amazon S3. Es ist kein großer Konfigurationsaufwand erforderlich, zudem kommt dies möglicherweise Ihren Überwachungsanforderungen zugute, insbesondere wenn Sie das Tool bereits zur Überwachung anderer Services und Anwendungen verwenden.

Gruppen protokollieren und Ereignisse in Amazon protokollieren CloudWatch

Nachdem Sie ausgewählt haben, welche Amazon Redshift Redshift-Protokolle exportiert werden sollen, können Sie Protokollereignisse in Amazon CloudWatch Logs überwachen. Eine neue Protokollgruppe für Amazon Redshift Serverless wird automatisch mit folgendem Präfix erstellt. `log_type` steht dabei für den Protokolltyp.

```
/aws/redshift/cluster/<cluster_name>/<log_type>
```

Wenn Sie beispielsweise das Verbindungsprotokoll exportieren möchten, werden die Protokolldaten in der folgenden Protokollgruppe gespeichert.

```
/aws/redshift/cluster/cluster1/connectionlog
```

Protokollereignisse werden mithilfe des Protokollstreams in eine Protokollgruppe exportiert. Um in Protokollereignissen für Ihren serverlosen Endpunkt nach Informationen zu suchen, verwenden Sie die Amazon CloudWatch Logs-Konsole AWS CLI, die oder die Amazon CloudWatch Logs-API. Weitere Informationen zum Suchen und Filtern von Protokolldaten finden Sie unter Erstellen von Metriken aus Protokollereignissen mithilfe von Filtern.

In CloudWatch können Sie Ihre Protokolldaten mit einer Abfragesyntax durchsuchen, die für Granularität und Flexibilität sorgt. Weitere Informationen finden Sie unter CloudWatch Logs Insights-Abfragesyntax.

Migration zu Amazon CloudWatch Audit Logging

In allen Fällen, in denen Sie Protokolle an Amazon S3 senden und die Konfiguration ändern, z. B. um Protokolle an zu senden, sind Protokolle CloudWatch, die in Amazon S3 verbleiben, davon nicht betroffen. Sie können die Protokolldaten weiterhin in den Amazon-S3-Buckets abfragen, in denen sie sich befinden.

Verwalten von Protokolldateien in Amazon S3

Die Anzahl und die Größe der Amazon-Redshift-Protokolldateien in Amazon S3 ist stark von der Aktivität in Ihrem Cluster abhängig. Wenn der Cluster aktiv ist und eine große Zahl von Protokollen generiert, erstellt Amazon Redshift die Protokolldateien möglicherweise häufiger. Sie erhalten möglicherweise eine Reihe von Protokolldateien für dieselbe Art von Aktivität, beispielsweise mehrere Verbindungsprotokolle innerhalb einer Stunde.

Wenn Amazon Redshift Amazon S3 zum Speichern von Protokollen nutzt, fallen Kosten für den Speicher an, den Sie in Amazon S3 nutzen. Bevor Sie die Protokollierung in Amazon S3 konfigurieren, sollten Sie einplanen, wie lange Sie die Protokolldateien speichern müssen. Finden Sie in diesem Zusammenhang heraus, wann die Protokolldateien Ihren Prüfungsanforderungen entsprechend gelöscht oder archiviert werden können. Der von Ihnen erstellte Plan ist stark von der Art der gespeicherten Daten abhängig, beispielsweise Daten, die Compliance- oder regulatorischen Anforderungen unterliegen. Weitere Informationen über die Amazon-S3-Preise finden Sie unter Amazon Simple Storage Service (S3) – Preise.

Einschränkungen bei der Aktivierung der Protokollierung in Amazon S3

Für die Audit-Protokollierung gelten folgende Einschränkungen:

- Derzeit können Sie nur die Verschlüsselung (AES-256) der von Amazon S3 verwalteten Schlüssel (SSE-S3) verwenden.
- Für die Amazon-S3-Buckets muss die S3-Objektsperre-Funktion deaktiviert sein.

Bucket-Berechtigungen für die Amazon-Redshift-Prüfungsprotokollierung

Wenn Sie die Protokollierung in Amazon S3 aktivieren, sammelt Amazon Redshift Protokollinformationen und lädt sie in Protokolldateien hoch, die in Amazon S3 gespeichert werden. Sie können einen vorhandenen oder einen neuen Bucket verwenden. Amazon Redshift setzt die folgenden IAM-Berechtigungen für den Bucket voraus:

- `s3:GetBucketAcl` Der Service erfordert Leseberechtigungen für den Amazon S3 Bucket, um den Bucket-Eigentümer identifizieren zu können.
- `s3:PutObject` Der Service benötigt Put-Objekt-Berechtigungen, um die Protokolle hochladen zu können. Außerdem muss der Benutzer oder die IAM-Rolle, die die Protokollierung aktiviert, die `s3:PutObject`-Berechtigung für den Amazon-S3-Bucket besitzen. Bei jedem Hochladen von Protokollen legt der Service, ob der aktuelle Bucket-Eigentümer mit dem Bucket-Eigentümer zum Zeitpunkt der Aktivierung der Protokollierung übereinstimmt. Wenn diese Besitzer nicht übereinstimmen, erhalten Sie einen Fehler.

Wenn Sie beim Aktivieren der Prüfungsprotokollierung die Option zum Erstellen eines neuen Buckets auswählen, werden die korrekten Berechtigungen für ihn angewendet. Wenn Sie Ihren eigenen Bucket in Amazon S3 erstellen oder einen vorhandenen Bucket verwenden, müssen Sie jedoch eine Bucket-Richtlinie hinzufügen, die den Namen des Buckets enthält. Protokolle werden mit Service-Prinzipal-Anmeldeinformationen geliefert. *In den meisten Fällen AWS-Regionen fügen Sie den Redshift-Serviceprinzipalnamen redshift.amazonaws.com hinzu.*

Die Bucket-Richtlinie verwendet das folgende Format. *ServiceName*und sind Platzhalter für Ihre eigenen Werte. *BucketName* Geben Sie auch die zugehörigen Aktionen und Ressourcen in der Bucket-Richtlinie an.

```
{
    "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/*"
            ]
        }
    ]
}
```

Im folgenden Beispiel sehen Sie eine Bucket-Richtlinie für die Region USA Ost (Nord-Virginia) und einen Bucket namens `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/*"
            ]
        }
    ]
}
```

Regionen, die standardmäßig nicht aktiviert sind, auch als „Opt-In-Regionen“ bezeichnet, benötigen einen regionsspezifischen Service-Prinzipal-Namen. Für diese enthält der Service-Prinzipal-Name die Region im Format `redshift.region.amazonaws.com`. Beispiel: *redshift.ap-east-1.amazonaws.com* für die Region Asien-Pazifik (Hongkong). Eine Liste der Regionen, die standardmäßig nicht aktiviert sind, finden Sie unter Verwalten von AWS-Regionen in der Allgemeine AWS-Referenz.

> **Note**
>
> Der regionsspezifische Service-Prinzipal-Name entspricht der Region, in der sich der Cluster befindet.

Bewährte Methoden für Protokolldateien

Wenn Redshift Protokolldateien auf Amazon S3 hochlädt, können große Dateien in Teilen hochgeladen werden. Wenn ein mehrteiliger Upload nicht erfolgreich ist, können Teile einer Datei im Amazon S3 Bucket verbleiben. Dies kann zu zusätzlichen Speicherkosten führen. Daher ist es wichtig zu verstehen, was passiert, wenn ein mehrteiliger Upload fehlschlägt. Eine ausführliche Erklärung zum mehrteiligen Upload für Prüfungsprotokolle finden Sie unter Hochladen und Kopieren von Objekten mit mehrteiligen Uploads und Abbrechen eines mehrteiligen Uploads.

Weitere Informationen zum Erstellen von S3 Buckets und zum Hinzufügen von Bucket-Richtlinien finden Sie unter Erstellen eines Buckets und Bearbeiten von Bucket-Berechtigungen im Amazon-Simple-Storage-Service-Benutzerhandbuch.

Bucket-Struktur für die Amazon-Redshift-Prüfungsprotokollierung

Standardmäßig organisiert Amazon Redshift die Protokolldateien im Amazon-S3-Bucket unter Verwendung der folgenden Bucket- und Objektstruktur:

`AWSLogs/AccountID/ServiceName/Region/Year/Month/Day/AccountID_ServiceName_Region`

Ein Beispiel ist: `AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

Wenn Sie ein Amazon-S3-Schlüsselpräfix bereitstellen, stellen Sie das Präfix an den Anfang des Schlüssels.

Wenn Sie beispielsweise ein Präfix oder eigenes Präfix angeben: `myprefix/AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

Das Amazon-S3-Schlüsselpräfix darf nicht mehr als 512 Zeichen enthalten. Es darf keine Leerzeichen ( ), doppelten Anführungszeichen (“), einzelne Anführungszeichen (‘) oder Backslashes (\)enthalten. Einige Sonderzeichen und Steuerzeichen sind ebenfalls nicht zulässig. Die Hexadezimalcodes für diese Zeichen sind:

- x00 bis x20
- x 22 %
- x 27 %
- x5c
- x7f oder höher

Fehlerbehebung der Amazon-Redshift-Prüfungsprotokollierung in Amazon S3

Die Amazon-Redshift-Prüfungsprotokollierung kann aus folgenden Gründen unterbrochen werden:

- Amazon Redshift verfügt nicht über die Berechtigung, Protokolle in den Amazon S3 Bucket hochzuladen. Überprüfen Sie, ob der Bucket mit der richtigen IAM-Richtlinie konfiguriert wurde. Weitere Informationen finden Sie unter Bucket-Berechtigungen für die Amazon-Redshift-Prüfungsprotokollierung.
- Der Bucket-Eigentümer hat gewechselt. Amazon Redshift überprüft beim Hochladen von Protokollen, ob der Bucket-Eigentümer derselbe wie zum Zeitpunkt der Aktivierung der Protokollierung ist. Wenn sich der Bucket-Eigentümer geändert hat, kann Amazon Redshift keine Protokolle hochladen, bis Sie einen anderen Bucket für die Prüfungsprotokollierung konfiguriert haben.
- Der Bucket kann nicht gefunden werden. Wenn der Bucket in Amazon S3 gelöscht wird, kann Amazon Redshift keine Protokolle hochladen. Sie müssen den Bucket entweder neu erstellen oder Amazon Redshift so konfigurieren, dass Protokolle in einen anderen Bucket hochgeladen werden.

Protokollieren Amazon Redshift Redshift-API-Aufrufen mit AWS CloudTrail

Amazon Redshift ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in Amazon Redshift ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Amazon Redshift als Ereignisse. Weitere Informationen zur Amazon Redshift Redshift-Integration mit finden Sie AWS CloudTrail unter Logging with CloudTrail.

Sie können die Audit-Protokollierung der Amazon Redshift-Datenbank CloudTrail unabhängig oder zusätzlich zur Amazon Redshift Redshift-Datenbank verwenden.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Konfigurieren von Prüfungen über die Konsole

Konfigurieren Sie Amazon Redshift so, dass Prüfungsprotokolldaten exportiert werden. Protokolle können in oder als Dateien in Amazon S3 S3-Buckets exportiert werden. CloudWatch

Aktivieren der Prüfungsprotokollierung über die Konsole

Schritte in der Konsole

So aktivieren Sie die Prüfprotokollierung für einen Cluster:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster aus, den Sie aktualisieren möchten.
3. Wählen Sie die Registerkarte Properties (Eigenschaften) aus. Wählen Sie auf der Seite Database configurations (Datenbankkonfigurationen) Edit (Bearbeiten) und dann Edit audit logging (Prüfungsprotokollierung bearbeiten) aus.
4. Wählen Sie auf der Seite „Audit-Protokollierung bearbeiten“ die Option Einschalten und wählen Sie S3-Bucket oder CloudWatchaus. Wir empfehlen die Verwendung CloudWatch , da die Verwaltung einfach ist und hilfreiche Funktionen für die Datenvisualisierung bietet.
5. Wählen Sie aus, welche Protokolle exportiert werden sollen.
6. Wählen Sie Save changes (Änderungen speichern) aus, um Ihre Änderungen zu speichern.

Konfiguration der Protokollierung mithilfe der AWS CLI Amazon Redshift Redshift-API

Sie können die folgenden Amazon-Redshift-CLI-Vorgänge verwenden, um die Prüfungsprotokollierung zu konfigurieren:

- describe-logging-status
- disable-logging
- enable-logging

Sie können die folgenden Amazon-Redshift-API-Vorgänge verwenden, um die Prüfungsprotokollierung zu konfigurieren:

- DescribeLoggingStatus
- DisableLogging
- EnableLogging

Protokollieren mit CloudTrail

Protokollieren von Aufrufen mit AWS CloudTrail

Amazon Redshift, die Datenfreigabe, Amazon Redshift Serverless, die Amazon-Redshift-Daten-API und der Abfrage-Editor v2 sind alle in integriertAWS CloudTrail. CloudTrail ist ein Service, der die Aktionen eines Benutzers, einer Rolle oder eines -AWSServices in Amazon Redshift aufzeichnet. CloudTrail erfasst alle API-Aufrufe für Amazon Redshift als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Redshift-Konsole und Codeaufrufe der Redshift-Vorgänge.

Wenn Sie einen CloudTrail Trail erstellen, können Sie CloudTrail Ereignisse kontinuierlich an einen Amazon S3-Bucket übermitteln, einschließlich Ereignissen für Redshift. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie bestimmte Dinge bestimmen. Dazu gehören die Anforderung, die an Redshift gestellt wurde, die IP-Adresse, von der aus die Anforderung gestellt wurde, wer die Anforderung gestellt hat, wann sie gestellt wurde und weitere Details.

Sie können CloudTrail unabhängig von oder zusätzlich zur Prüfungsprotokollierung der Amazon-Redshift-Datenbank verwenden.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

Arbeiten mit Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine Aktivität auftritt, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen -AWSServiceereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf im AWS CloudTrail -Benutzerhandbuch.

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich Ereignissen für Redshift, einen Trail. CloudTrail verwendet Trails, um Protokolldateien an einen Amazon S3-Bucket zu übermitteln. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere -AWSServices konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail-Benutzerhandbuch:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien aus mehreren Konten

Alle Aktionen von Amazon Redshift, Amazon Redshift Serverless, Data API, Data Sharing und Query Editor v2 werden von protokolliert CloudTrail. Aufrufe der `CreateConnection` Aktionen `AuthorizeDatashare`, `ExecuteStatement`, und erzeugen beispielsweise Einträge in den `CreateNamespace` CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anforderung mit Root- oder -Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail userIdentity Element im AWS CloudTrail - Benutzerhandbuch.

Grundlagen zu Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail -Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Amazon Redshift Datashare – Beispiel

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die -`AuthorizeDataShare`Operation veranschaulicht.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
                "arn": "arn:aws:sts::111122223333:user/janedoe",
                "accountId": "111122223333",
                "userName": "janedoe"
            },
            "attributes": {
                "creationDate": "2021-08-02T23:40:45Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-08-02T23:40:58Z",
    "eventSource": "redshift.amazonaws.com",
```

```
    "eventName": "AuthorizeDataShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.227.36.75",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "consumerIdentifier": "555555555555"
    },
    "responseElements": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "producerNamespaceArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "producerArn": "arn:aws:redshift:us-
east-1:111122223333:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "allowPubliclyAccessibleConsumers": true,
        "dataShareAssociations": [
            {
                "consumerIdentifier": "555555555555",
                "status": "AUTHORIZED",
                "createdDate": "Aug 2, 2021 11:40:56 PM",
                "statusChangeDate": "Aug 2, 2021 11:40:57 PM"
            }
        ]
    },
    "requestID": "87ee1c99-9e41-42be-a5c4-00495f928422",
    "eventID": "03a3d818-37c8-46a6-aad5-0151803bdb09",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Amazon Redshift Serverless – Beispiel

Amazon Redshift Serverless ist in integriertAWS CloudTrail, um eine Aufzeichnung der in Amazon Redshift Serverless durchgeführten Aktionen bereitzustellen. CloudTrail erfasst alle API-Aufrufe für Amazon Redshift Serverless als Ereignisse. Weitere Informationen zu den Funktionen von Amazon Redshift Serverless finden Sie unter Übersicht über die Funktionen von Amazon Redshift Serverless.

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `CreateNamespace` Aktion demonstriert.


```
{
    "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",
}
```

Amazon-Redshift-Daten-API – Beispiele

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `ExecuteStatement` Aktion demonstriert.

```
{
    "eventVersion":"1.05",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn":"arn:aws:sts::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
        "userName": "janedoe"
    },
    "eventTime":"2020-08-19T17:55:59Z",
    "eventSource":"redshift-data.amazonaws.com",
    "eventName":"ExecuteStatement",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"192.0.2.0",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters":{
        "clusterIdentifier":"example-cluster-identifier",
```

```
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "sql":"***OMITTED***"
    },
    "responseElements":{
        "clusterIdentifier":"example-cluster-identifier",
        "createdAt":"Aug 19, 2020 5:55:58 PM",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "id":"5c52b37b-9e07-40c1-98de-12ccd1419be7"
    },
    "requestID":"00c924d3-652e-4939-8a7a-cd0612eeb8ac",
    "eventID":"c1fb7076-102f-43e5-9ec9-40820bcc1175",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "recipientAccountId":"123456789012"
}
```

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `ExecuteStatement` Aktion veranschaulicht, die die für Idempotenz `clientToken` verwendete zeigt.

```
{
    "eventVersion":"1.05",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn":"arn:aws:sts::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
        "userName": "janedoe"
    },
    "eventTime":"2020-08-19T17:55:59Z",
    "eventSource":"redshift-data.amazonaws.com",
    "eventName":"ExecuteStatement",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"192.0.2.0",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters":{
        "clusterIdentifier":"example-cluster-identifier",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "sql":"***OMITTED***",
```

```
        "clientToken":"32db2e10-69ac-4534-b3fc-a191052616ce"
    },
    "responseElements":{
        "clusterIdentifier":"example-cluster-identifier",
        "createdAt":"Aug 19, 2020 5:55:58 PM",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "id":"5c52b37b-9e07-40c1-98de-12ccd1419be7"
    },
    "requestID":"00c924d3-652e-4939-8a7a-cd0612eeb8ac",
    "eventID":"c1fb7076-102f-43e5-9ec9-40820bcc1175",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "recipientAccountId":"123456789012"
}
```

Beispiel für den Abfrage-Editor v2 von Amazon Redshift

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `CreateConnection` Aktion demonstriert.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAKEOFPINEXAMPLE:session",
        "arn": "arn:aws:sts::123456789012:assumed-role/MyRole/session",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAKEOFPINEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/MyRole",
                "accountId": "123456789012",
                "userName": "MyRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-09-21T17:19:02Z",
                "mfaAuthenticated": "false"
            }
        }
```

```
    },
    "eventTime": "2022-09-21T22:22:05Z",
    "eventSource": "sqlworkbench.amazonaws.com",
    "eventName": "CreateConnection",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "192.2.0.2",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0)
 Gecko/20100101 Firefox/102.0",
    "requestParameters": {
        "password": "***",
        "databaseName": "***",
        "isServerless": false,
        "name": "***",
        "host": "redshift-cluster-2.c8robpbxvbf9.ca-central-1.redshift.amazonaws.com",
        "authenticationType": "***",
        "clusterId": "redshift-cluster-2",
        "username": "***",
        "tags": {
            "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
        }
    },
    "responseElements": {
        "result": true,
        "code": "",
        "data": {
            "id": "arn:aws:sqlworkbench:ca-central-1:123456789012:connection/ce56b1be-
dd65-4bfb-8b17-12345123456",
            "name": "***",
            "authenticationType": "***",
            "databaseName": "***",
            "secretArn": "arn:aws:secretsmanager:ca-
central-1:123456789012:secret:sqlworkbench!7da333b4-9a07-4917-b1dc-12345123456-qTCoFm",
            "clusterId": "redshift-cluster-2",
            "dbUser": "***",
            "userSettings": "***",
            "recordDate": "2022-09-21 22:22:05",
            "updatedDate": "2022-09-21 22:22:05",
            "accountId": "123456789012",
            "tags": {
                "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
            },
            "isServerless": false
        }
    },
```

```
    "requestID": "9b82f483-9c03-4cdd-bb49-a7009e7da714",
    "eventID": "a7cdd442-e92f-46a2-bc82-2325588d41c3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Amazon-Redshift-Konto-IDs inAWS CloudTrail-Protokollen

Wenn Amazon Redshift einen anderen AWS-Service für Sie aufruft, wird der Aufruf mit einer Konto-ID protokolliert, die zu Amazon Redshift gehört. Er wird nicht mit Ihrer Konto-ID protokolliert. Angenommen, Amazon Redshift ruft zum Beispiel AWS Key Management Service (AWS KMS)-Operationen wie `CreateGrant`, `Decrypt`, `Encrypt` und `RetireGrant` auf, um die Verschlüsselung in Ihrem Cluster zu verwalten. In diesem Fall werden die Aufrufe von AWS CloudTrail mit einer Amazon-Redshift-Konto-ID protokolliert.

Amazon Redshift verwendet beim Aufrufen anderer AWS-Services die Konto-IDs in der folgenden Tabelle.

Region	Region	Konto-ID
Region USA Ost (Nord-Virginia)	us-east-1	368064434614
Region USA Ost (Ohio)	us-east-2	790247189693
Region US West (N. California)	us-west-1	703715109447
Region USA West (Oregon)	us-west-2	473191095985
Region Afrika (Kapstadt)	af-south-1	420376844563
Region Asien-Pazifik (Hongkong)	ap-east-1	651179539253
Region Asien-Pazifik (Hyderabad)	ap-south-2	297058826802
Region Asien-Pazifik (Jakarta)	ap-southeast-3	623197973179

Region	Region	Konto-ID
Region Asien-Pazifik (Melbourne)	ap-southeast-4	945512339897
Region Asien-Pazifik (Mumbai)	ap-south-1	408097707231
Region Asien-Pazifik (Osaka)	ap-northeast-3	398671365691
Region Asien-Pazifik (Seoul)	ap-northeast-2	713597048934
Region Asien-Pazifik (Singapur)	ap-southeast-1	960118270566
Region Asien-Pazifik (Sydney)	ap-southeast-2	485979073181
Region Asien-Pazifik (Tokio)	ap-northeast-1	615915377779
Region Kanada (Zentral)	ca-central-1	764870610256
Region Kanada West (Calgary)	ca-west-1	830903446466
Region Europa (Frankfurt)	eu-central-1	434091160558
Region Europa (Irland)	eu-west-1	246478207311
Region Europa (London)	eu-west-2	885798887673
Region Europa (Mailand)	eu-south-1	041313461515
Region Europa (Paris)	eu-west-3	694668203235
Region Europa (Spanien)	eu-south-2	028811157404
Region Europa (Stockholm)	eu-north-1	553461782468
Region Europa (Zürich)	eu-central-2	668912161003
Region Israel (Tel Aviv)	il-central-1	901883065212
Region Naher Osten (Bahrain)	me-south-1	051362938876
Region Naher Osten (VAE)	me-central-1	595013617770

Region	Region	Konto-ID
Region Südamerika (São Paulo)	sa-east-1	392442076723

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für die AWS KMS Decrypt-Operation, die von Amazon Redshift aufgerufen wurde.

```
{

    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAI5QPCMKLTL4VHFCYY:i-0f53e22dbe5df8a89",
        "arn": "arn:aws:sts::790247189693:assumed-role/prod-23264-role-wp/
i-0f53e22dbe5df8a89",
        "accountId": "790247189693",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2017-03-03T16:24:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAI5QPCMKLTL4VHFCYY",
                "arn": "arn:aws:iam::790247189693:role/prod-23264-role-wp",
                "accountId": "790247189693",
                "userName": "prod-23264-role-wp"
            }
        }
    },
    "eventTime": "2017-03-03T17:16:51Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "52.14.143.61",
    "userAgent": "aws-internal/3",
    "requestParameters": {
        "encryptionContext": {
            "aws:redshift:createtime": "20170303T1710Z",
            "aws:redshift:arn": "arn:aws:redshift:us-east-2:123456789012:cluster:my-dw-
instance-2"
```

```
        }
    },
    "responseElements": null,
    "requestID": "30d2fe51-0035-11e7-ab67-17595a8411c8",
    "eventID": "619bad54-1764-4de4-a786-8898b0a7f40c",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/f8f4f94f-e588-4254-
b7e8-078b99270be7",
            "accountId": "123456789012",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012",
    "sharedEventID": "c1daefea-a5c2-4fab-b6f4-d8eaa1e522dc"

}
```


Compliance-Validierung für Amazon Redshift

Externe Prüfer bewerten im Rahmen verschiedener AWS-Compliance-Programme die Sicherheit und Compliance von Amazon Redshift. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS-Services, die in den Geltungsbereich bestimmter Compliance-Programme fallen, finden Sie auf der Seite AWS-Services in Scope nach Compliance-Programm. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Die Auditberichte von Drittanbietern lassen sich mit AWS Artifact herunterladen. Weitere Informationen finden Sie unter Herunterladen von Berichten in AWS Artifact.

Welche Compliance-Verpflichtungen Sie bei der Nutzung von Amazon Redshift haben, hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Wenn Ihre Nutzung von Amazon Redshift der Einhaltung von Standards wie HIPAA, PCI oder FedRAMP unterliegt, stellt AWS Ressourcen zur Unterstützung bereit:

- Kurzanleitungen für Sicherheit und Compliance, die wichtige Punkte zur Architektur sowie die Schritte zur Bereitstellung von Sicherheits- und Compliance-orientierten Basisumgebungen in AWS erläutern.

- Whitepaper zur Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance, das beschreibt, wie Unternehmen mithilfe von AWS HIPAA-konforme Anwendungen erstellen können.
- AWS-Compliance-Ressourcen, Arbeitsbücher und Leitfäden, die für Ihre Branche und Ihren Standort möglicherweise relevant sind.
- AWS Config, ein AWS-Service, kann bewerten, wie gut Ihre Ressourcenkonfigurationen den internen Verfahren, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub, ein AWS-Service, bietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. So können Sie Ihre Compliance mit Branchen-Sicherheitsstandards und bewährten Methoden abgleichen. Security Hub verwendet Sicherheitskontrollen für die Bewertung von Ressourcenkonfigurationen und Sicherheitsstandards, um Sie bei der Einhaltung verschiedener Compliance-Frameworks zu unterstützen. Weitere Informationen zur Verwendung von Security Hub zur Bewertung von Amazon-Redshift-Ressourcen finden Sie unter Amazon-Redshift-Steuerelemente im AWS Security Hub-Benutzerhandbuch.

Die folgenden Compliance- und Sicherheitsdokumente decken Amazon Redshift ab und sind auf Anfrage über AWS Artifact verfügbar. Weitere Informationen finden Sie unter AWS Artifact.

- Cloud Computing Compliance Controls Catalogue (C5)
- ISO 27001:2013 Erklärung zur Anwendbarkeit (SoA)
- ISO 27001:2013 Zertifizierung
- ISO 27017:2015 Erklärung zur Anwendbarkeit (SoA)
- ISO 27017:2015 Zertifizierung
- ISO 27018:2015 Erklärung zur Anwendbarkeit (SoA)
- ISO 27018:2014 Zertifizierung
- ISO 9001:2015 Zertifizierung
- PCI-DSS-Compliance-Nachweis (AOC) und Zusammenfassung der Verantwortlichkeiten
- Service Organization Controls (SOC)-Bericht 1
- Service Organization Controls (SOC)-Bericht 2
- Service Organization Controls (SOC)-Bericht 2 zur Vertraulichkeit

Ausfallsicherheit in Amazon Redshift

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und Availability Zones (AZs). AWS -Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind hochverfügbarer, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Fast alle AWS-Regionen verfügen über mehrere Availability Zones und Rechenzentren. Sie können Ihre Anwendungen über mehrere Availability Zones in derselben Region bereitstellen, um eine bessere Fehlertoleranz und niedriger Latenz zu erzielen.

Wenn Sie einen Cluster ohne Datenverlust oder Änderungen an Ihren Anwendungen in eine andere Availability Zone verschieben möchten, können Sie eine Verlagerung für Ihren Cluster einrichten. Mit der Verschiebung können Sie den Betrieb mit minimalen Auswirkungen fortsetzen, wenn es eine Serviceunterbrechung für den Cluster gibt. Wenn Clusterverschiebung aktiviert ist, kann Amazon Redshift in einigen Situationen entscheiden, Cluster zu verschieben. Weitere Informationen zum Verlagern in Amazon Redshift finden Sie unter Ihren Cluster verlagern.

Für Fehlersituationen, in denen ein unerwartetes Ereignis in der Availability Zone auftritt, können Sie mehrere Availability Zones (Multi-AZ)-Bereitstellung einrichten, damit Ihr Amazon Redshift Data Warehouse in Betrieb bleibt. Amazon Redshift stellt gleiche Rechenressourcen in zwei Availability Zones bereit, auf die über einen einzelnen Endpunkt zugegriffen werden kann. Bei einem Ausfall einer gesamten Availability Zone stehen die verbleibenden Rechenressourcen in der zweiten Availability Zone zur weiteren Verarbeitung von Workloads zur Verfügung. Weitere Informationen zu Multi-AZ-Bereitstellungen finden Sie unter Konfigurieren einer Multi-AZ-Bereitstellung.

Weitere Informationen zu AWS-Regionen und Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Infrastruktursicherheit in Amazon Redshift

Als verwalteter Service ist Amazon Redshift durch die globale Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand

der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden von AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon Redshift zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Netzwerkisolierung

Eine Virtual Private Cloud (VPC), die auf dem Amazon-VPC-Service basiert, ist Ihr privates, logisch isoliertes Netzwerk in der AWS-Cloud. Sie können einen Amazon-Redshift-Cluster in einer VPC bereitstellen, indem Sie die folgenden Schritte ausführen:

- Erstellen Sie eine VPC in einer AWS-Region. Weitere Informationen finden Sie unter Was ist Amazon VPC? im Amazon-VPC-Benutzerhandbuch.
- Erstellen Sie zwei oder mehr private VPC-Subnetze. Weitere Informationen finden Sie unter VPCs und Subnetze im Amazon-VPC-Benutzerhandbuch.
- Stellen Sie einen Amazon-Redshift-Cluster bereit. Weitere Informationen finden Sie unter Amazon-Redshift-Cluster-Subnetzgruppen.

Ein Amazon-Redshift-Cluster ist bei der Bereitstellung standardmäßig gesperrt. Um eingehenden Netzwerkverkehr von Amazon-Redshift-Clients zuzulassen, ordnen Sie eine VPC-Sicherheitsgruppe einem Amazon-Redshift-Cluster zu. Weitere Informationen finden Sie unter Amazon-Redshift-Cluster-Subnetzgruppen.

Um Datenverkehr nur in oder von bestimmten IP-Adressbereichen zuzulassen, aktualisieren Sie die Sicherheitsgruppen mit Ihrer VPC. Ein Beispiel ist, Datenverkehr nur von oder zu Ihrem Unternehmensnetzwerk zuzulassen.

Stellen Sie beim Konfigurieren von Netzwerk-Zugriffssteuerungslisten, die den Subnetzen zugeordnet sind, mit denen Ihr Amazon-Redshift-Cluster gekennzeichnet ist, sicher, dass die S3-CIDR-Bereiche der jeweiligen AWS-Region zur Zulassungsliste für Eingangs- und Ausgangsregeln hinzugefügt werden. Auf diese Weise können Sie S3-basierte Vorgänge wie Redshift Spectrum, COPY und UNLOAD ohne Unterbrechungen ausführen.

Der folgende Beispielbefehl analysiert die JSON-Antwort für alle IPv4-Adressen, die in Amazon S3 in der Region us-east-1 verwendet werden.

```
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
```

Anweisungen zum Abrufen von S3-IP-Bereichen für eine bestimmte Region finden Sie unter AWS-IP-Adressbereiche.

Amazon Redshift unterstützt die Bereitstellung von Clustern in Dedicated-Tenancy-VPCs. Weitere Informationen finden Sie unter Dedicated Instances im Amazon EC2-Benutzerhandbuch.

Amazon-Redshift-Cluster-Sicherheitsgruppen

Wenn Sie einen Amazon-Redshift-Cluster bereitstellen, ist dieser standardmäßig gesperrt, so dass niemand darauf zugreifen kann. Um anderen Benutzern eingehenden Zugriff auf einen Amazon-Redshift-Cluster zu gewähren, ordnen Sie den Cluster einer Sicherheitsgruppe zu. Wenn Sie auf der EC2-VPC-Plattform arbeiten, können Sie eine vorhandene Amazon-VPC-Sicherheitsgruppe verwenden oder eine neue definieren und diese dann einem Cluster zuordnen. Weitere Informationen zur Verwaltung eines Clusters auf der EC2-VPC-Plattform finden Sie unter Verwaltung von Clustern in einer VPC.

Wenn Sie auf der EC2 Classic-Plattform arbeiten, definieren Sie eine Cluster-Sicherheitsgruppe und verbinden sie mit einem Cluster. Die EC2-Classic-Plattform wird außer Betrieb genommen. Wir empfehlen, dass Sie Ihren Cluster auf einer EC2-VPC-Plattform anstelle einer EC2-Classic-Plattform starten. Sie können mit der Amazon-Redshift-Konsole jedoch einen EC2-Classic-Snapshot auf einen EC2-VPC-Cluster wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot.

Verbinden mit Amazon Redshift über einen Schnittstellen-VPC-Endpunkt

Sie können sich über einen Schnittstellen-VPC-Endpunkt (AWS PrivateLink) in Ihrer Virtual Private Cloud (VPC) direkt mit der Amazon Redshift API verbinden, anstatt eine Verbindung über das Internet herzustellen. Weitere Informationen zu den Amazon Redshift API-Aktionen finden Sie unter Aktionen in der Amazon-Redshift-API-Referenz. Weitere Informationen über AWS PrivateLink finden Sie unter Schnittstellen-VPC-Endpunkte (AWS PrivateLink)im Amazon-VPC-Benutzerhandbuch. Beachten Sie, dass die JDBC/ODBC-Verbindung zum Cluster nicht Bestandteil des Amazon Redshift API-Services ist.

Wenn Sie einen Schnittstellen-VPC-Endpunkt verwenden, findet die Kommunikation zwischen Ihrer VPC und Amazon Redshift vollständig innerhalb des AWS-Netzwerks statt, was die Sicherheit erhöhen kann. Jeder VPC-Endpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen mit privaten IP-Adressen in Ihren VPC-Subnetzen repräsentiert. Weitere Informationen zu Elastic-Network-Schnittstellen finden Sie unter Elastic-Network-Schnittstellen im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Ein Schnittstellen-VPC Endpunkt verbindet Ihre VPC direkt mit Amazon Redshift. Er verwendet kein Internet-Gateway, kein Network Address Translation (NAT)-Gerät, keine Virtual Private Network (VPN)-Verbindung und keine AWS Direct Connect-Verbindung. Die Instances in Ihrer VPC benötigen für die Kommunikation mit der Amazon Redshift API keine öffentlichen IP-Adressen.

Um Amazon Redshift über Ihre VPC zu verwenden, haben Sie zwei Optionen. Eine besteht darin, eine Verbindung von einer Instance innerhalb Ihrer VPC herzustellen. Die andere ist, Ihr privates Netzwerk mithilfe einer AWS VPN-Option oder AWS Direct Connect mit Ihrer VPC zu verbinden. Weitere Informationen zu AWS VPN-Optionen finden Sie unter VPN-Verbindungen im Amazon-VPC-Benutzerhandbuch. Informationen zu AWS Direct Connect finden Sie unter Erstellen einer Verbindung im AWS Direct Connect-Benutzerhandbuch.

Sie können über die AWS Management Console oder AWS Command Line Interface (AWS CLI)-Befehle einen Schnittstellen-VPC-Endpunkt erstellen, um eine Verbindung zu Amazon Redshift herzustellen. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts.

Nachdem Sie einen Schnittstellen-VPC-Endpunkt erstellt haben, können Sie private DNS-Hostnamen für den Endpunkt aktivieren. Wenn Sie dies tun, wird der standardmäßige Amazon-Redshift-Endpunkt (`https://redshift.Region.amazonaws.com`) zu Ihrem VPC-Endpunkt aufgelöst.

Wenn Sie private DNS-Hostnamen nicht aktivieren, stellt Amazon VPC einen DNS-Endpunktnamen bereit, den Sie im folgenden Format verwenden können.

```
VPC_endpoint_ID.redshift.Region.vpce.amazonaws.com
```

Weitere Informationen finden Sie unter Schnittstellen-VPC-Endpunkte (AWS PrivateLink) im Amazon-VPC-Benutzerhandbuch.

Amazon Redshift unterstützt Aufrufe an alle API-Vorgänge in Ihrer VPC.

Sie können VPC-Endpunktrichtlinien an einen VPC-Endpunkt anfügen, um den Zugriff für AWS Identity and Access Management (IAM)-Prinzipale zu steuern. Sie können einem VPC-Endpunkt auch Sicherheitsgruppen zuordnen, um den eingehenden und ausgehenden Zugriff basierend auf Quelle und Ziel des Netzwerkdatenverkehrs zu steuern. Ein Beispiel ist ein IP-Adressbereich. Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon VPC User Guide.

Erstellen einer VPC-Endpunktrichtlinie für Amazon Redshift

Sie können eine Richtlinie für VPC-Endpunkte für Amazon Redshift erstellen, in der Sie Folgendes angeben:

- Prinzipal, der Aktionen ausführen bzw. nicht ausführen kann
- Aktionen, die ausgeführt werden können
- Ressourcen, für die Aktionen ausgeführt werden können

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Im Folgenden finden Sie Beispiele für VPC-Endpunktrichtlinien.

Themen

- Beispiel: VPC-Endpunktrichtlinie, die den gesamten Zugriff über ein angegebenes AWS-Konto verweigert
- Beispiel: VPC-Endpunktrichtlinie, die nur einer angegebenen IAM-Rolle VPC-Zugriff gewährt
- Beispiel: VPC-Endpunktrichtlinie, die nur einem angegebenen IAM-Prinzipal (Benutzer) VPC-Zugriff gewährt
- Beispiel: VPC-Endpunktrichtlinie zum Zulassen schreibgeschützter Amazon-Redshift-Vorgänge
- Beispiel: VPC-Endpunktrichtlinie, die den Zugriff auf einen angegebenen Cluster verweigert

Beispiel: VPC-Endpunktrichtlinie, die den gesamten Zugriff über ein angegebenes AWS-Konto verweigert

Die folgende VPC-Endpunktrichtlinie verweigert dem AWS-Konto *123456789012* jeglichen Zugriff auf Ressourcen, die diesen Endpunkt verwenden.

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Beispiel: VPC-Endpunktrichtlinie, die nur einer angegebenen IAM-Rolle VPC-Zugriff gewährt

Die folgende VPC-Endpunktrichtlinie gewährt nur dem IAM-Benutzer *redshiftrole* im AWS-Konto *123456789012* vollen Zugriff. Allen anderen IAM-Prinzipalen wird der Zugriff über den Endpunkt verweigert.

```
   {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
```

```
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:role/redshiftrole"
                ]
            }
        }]
}
```

Dies ist nur ein Beispiel. In den meisten Anwendungsfällen empfehlen wir, Berechtigungen für bestimmte Aktionen anzufügen, um den Umfang der Berechtigungen einzuschränken.

Beispiel: VPC-Endpunktrichtlinie, die nur einem angegebenen IAM-Prinzipal (Benutzer) VPC-Zugriff gewährt

Die folgende VPC-Endpunktrichtlinie gewährt nur dem IAM-Benutzer *redshiftadmin* im AWS-Konto *123456789012* vollen Zugriff. Allen anderen IAM-Prinzipalen wird der Zugriff über den Endpunkt verweigert.

```
   {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:user/redshiftadmin"
                ]
            }
        }]
}
```

Dies ist nur ein Beispiel. In den meisten Anwendungsfällen empfehlen wir, einer Rolle Berechtigungen anzufügen, bevor Sie sie einem Benutzer zuweisen. Darüber hinaus empfehlen wir, spezifische Aktionen zu verwenden, um den Umfang der Berechtigungen einzuschränken.

Beispiel: VPC-Endpunktrichtlinie zum Zulassen schreibgeschützter Amazon-Redshift-Vorgänge

Die folgende VPC-Endpunktrichtlinie erlaubt nur dem AWS-Konto *123456789012* das Ausführen der angegebenen Amazon-Redshift-Aktionen.

Die angegebenen Aktionen stellen das Äquivalent von schreibgeschütztem Zugriff für Amazon Redshift dar. Alle anderen Aktionen in der VPC werden dem angegebenen Konto verweigert. Allen anderen Konten wird außerdem jeglicher Zugriff verweigert. Eine Liste der Amazon-Redshift-Aktionen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Redshift im IAM-Benutzerhandbuch.

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

Beispiel: VPC-Endpunktrichtlinie, die den Zugriff auf einen angegebenen Cluster verweigert

Die folgende VPC-Endpunktrichtlinie gewährt vollen Zugriff für alle Konten und Prinzipale. Gleichzeitig verweigert sie jeglichen Zugriff für das AWS-Konto *123456789012* auf Aktionen, die auf dem Amazon-Redshift-Cluster mit der Cluster-ID *my-redshift-cluster* ausgeführt werden. Andere Amazon-Redshift-Aktionen, die keine Berechtigungen auf Ressourcenebene für Cluster unterstützen, sind weiterhin zulässig. Eine Liste der Amazon-Redshift-Aktionen und ihrer entsprechenden Ressourcentypen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Redshift im IAM-Benutzerhandbuch.

```
 {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-
cluster",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Konfigurations- und Schwachstellenanalyse in Amazon Redshift

AWS übernimmt grundlegende Sicherheitsaufgaben wie Gastbetriebssystem- und Datenbank-Patching, Firewall-Konfiguration und Notfallwiederherstellung. Diese Verfahren wurden von qualifizierten Dritten überprüft und zertifiziert. Weitere Informationen finden Sie unter Compliance-Validierung für Amazon Redshift, Modell der geteilten Verantwortlichkeit und Bewährte Methoden für Sicherheit, Identität und Compliance.

Amazon Redshift wendet automatisch Upgrades und Patches für Ihr Data Warehouse an, sodass Sie sich auf Ihre Anwendung konzentrieren können und nicht auf ihre Administration. Die Patches und Upgrades werden in einem konfigurierbaren Wartungsfenster angewendet. Weitere Informationen finden Sie unter Wartungsfenster.

Der Amazon-Redshift-Abfrage-Editor v2 ist eine von AWS verwaltete Anwendung. Alle Patches und Updates werden von AWS nach Bedarf aufgespielt.

Netzwerkaufgaben

Sie können Netzwerkaufgaben wie das Anpassen Ihrer Verbindung zu einer Redshift-Datenbank ausführen. Sie können auch DNS-bezogene Aufgaben ausführen, z. B. das Einrichten eines benutzerdefinierten Domainnamens. Diese Konfigurationsaufgaben stehen Ihnen zur Verfügung, wenn Sie über einen von Amazon Redshift bereitgestellten Cluster oder über eine Amazon Redshift Serverless-Arbeitsgruppe verfügen.

Themen

- Verwenden eines benutzerdefinierten Domain-Namens für Client-Verbindungen
- Arbeiten mit von RedShift verwalteten VPC-Endpunkten
- Enhanced VPC Routing in Amazon Redshift

Verwenden eines benutzerdefinierten Domain-Namens für Client-Verbindungen

Sie können sowohl für Ihren Amazon-Redshift-Cluster als auch für Ihre Amazon-Redshift-Serverless-Arbeitsgruppe einen benutzerdefinierten Domain-Namen, auch als benutzerdefinierte URL bezeichnet, erstellen. Es handelt sich um einen easy-to-read DNS-Datensatz, der SQL-Client-Verbindungen an Ihren Endpunkt weiterleitet. Sie können ihn jederzeit für einen vorhandenen Cluster oder eine vorhandene Arbeitsgruppe konfigurieren. Er bietet mehrere Vorteile:

- Der benutzerdefinierte Domain-Name ist eine einfachere Zeichenfolge als die Standard-URL, die in der Regel den Cluster-Namen oder den Arbeitsgruppennamen und die Region enthält. Er ist einfacher abzurufen und zu verwenden.
- Im Falle eines Failovers beispielsweise können Sie den Datenverkehr schnell an einen neuen Cluster oder eine neue Arbeitsgruppe weiterleiten. Dadurch müssen Clients keine Konfigurationsänderung vornehmen, wenn sie erneut eine Verbindung herstellen. Verbindungen können zentral und mit minimaler Unterbrechung umgeleitet werden.
- Sie müssen keine privaten Informationen wie z. B. Servernamen in einer Verbindungs-URL weitergeben. Sie können diese in einer benutzerdefinierten URL verbergen.

Wenn Sie einen benutzerdefinierten Domain-Namen mithilfe eines CNAME einrichten, fallen bei Amazon Redshift keine zusätzlichen Gebühren an. Möglicherweise wird Ihnen von Ihrem DNS-

Anbieter ein Domain-Name in Rechnung gestellt, wenn Sie einen neuen erstellen, aber diese Kosten sind in der Regel gering. Weitere Informationen finden Sie unter Erstellen eines benutzerdefinierten Domain-Namens.

Sicherheit für einen benutzerdefinierten Domain-Namen

Amazon Redshift oder Amazon Redshift Serverless benötigt ein validiertes SSL-Zertifikat (Secure Sockets Layer) für einen benutzerdefinierten Endpunkt, um die Kommunikation zu sichern und die Inhaberschaft des Domain-Namens zu verifizieren. Sie können Ihr AWS Certificate Manager-Konto mit einem AWS KMS key zur sicheren Zertifikatsverwaltung verwenden. Die Sicherheitsvalidierung beinhaltet die vollständige Überprüfung des Hostnamens (sslmode=verify-full).

Erneuern eines Zertifikats

Zertifikatserneuerungen werden von Amazon Redshift nur dann verwaltet, wenn Sie sich für die DNS-Validierung und nicht für die E-Mail-Validierung entscheiden. Wenn Sie die E-Mail-Validierung nutzen, können Sie das Zertifikat verwenden, müssen die Verlängerung jedoch selbst durchführen, bevor es abläuft. Wir empfehlen, dass Sie die DNS-Validierung für Ihr Zertifikat wählen. Sie können die Ablaufdaten importierter Zertifikate in AWS Certificate Manager überwachen.

Einrichten eines benutzerdefinierten Domain-Namens

Zum Einrichten des benutzerdefinierten Domain-Namens müssen mehrere Aufgaben ausgeführt werden: unter anderem muss der Domain-Name bei Ihrem DNS-Anbieter registriert werden und es muss ein Zertifikat erstellt werden. Nachdem Sie diese Aufgaben ausgeführt haben, konfigurieren Sie den benutzerdefinierten Domain-Namen in der Amazon-Redshift-Konsole bzw. der Amazon-Redshift-Serverless-Konsole oder mithilfe von AWS CLI-Befehlen. Details zu den Schritten finden Sie in den folgenden Abschnitten.

Einen Domain-Namen registrieren und ein Zertifikat wählen

Sie müssen über einen registrierten Internet-Domain-Namen verfügen, um einen benutzerdefinierten Domain-Namen in Amazon Redshift zu konfigurieren. Sie können eine Internet-Domain mit Route 53 oder über einen externen Domain-Anbieter registrieren. Diese Aufgaben führen Sie außerhalb der Amazon-Redshift-Konsole aus. Eine registrierte Domain ist eine Voraussetzung für die Ausführung der verbleibenden Verfahren zum Erstellen einer benutzerdefinierten Domain.

> **Note**
>
> Wenn Sie einen bereitgestellten Cluster verwenden, muss die Verschiebung aktiviert werden, bevor Sie die Schritte zur Konfiguration des benutzerdefinierten Domain-Namens ausführen. Weitere Informationen finden Sie unter Ihren Cluster verlagern. Dieser Schritt ist für Amazon Redshift Serverless nicht erforderlich.

Der benutzerdefinierte Domain-Name umfasst in der Regel die Stamm-Domain und eine Sub-Domain, wie `mycluster.example.com`. Um ihn zu konfigurieren, führen Sie die folgenden Schritte aus:

Einen DNS-CNAME-Eintrag für Ihren benutzerdefinierten Domain-Namen erstellen

1. Registrieren Sie eine Stamm-Domain, zum Beispiel `example.com`. Sie können wahlweise auch einen vorhandene Domain verwenden. Ihr benutzerdefinierter Name kann durch ein Verbot bestimmter Zeichen oder andere Namensvalidierungen eingeschränkt sein. Weitere Informationen zum Registrieren eines Domain-Namens finden Sie unter Registrieren einer neuen Domain.
2. Fügen Sie einen DNS CNAME-Datensatz hinzu, der Ihren benutzerdefinierten Domain-Namen auf den Redshift-Endpunkt für Ihren Cluster oder Ihre Arbeitsgruppe verweist. Sie finden den Endpunkt in den Eigenschaften für den Cluster oder die Arbeitsgruppe, in der Redshift-Konsole oder in der Amazon-Redshift-Serverless-Konsole. Kopieren Sie die JDBC-URL, die in den Cluster- oder Arbeitsgruppeneigenschaften enthalten ist, unter Allgemeine Informationen. Die URLs sehen wie folgt aus:

   - Für einen Amazon-Redshift-Cluster: `redshift-cluster-sample.abc123456.us-east-1.redshift.amazonaws.com`
   - Für eine Amazon-Redshift-Serverless-Arbeitsgruppe: `endpoint-name.012345678901.us-east-1-dev.redshift-serverless-dev.amazonaws.com`

   Wenn die URL über ein JDBC-Präfix verfügt, entfernen Sie dieses.

> **Note**
>
> DNS-Datensätze unterliegen der Verfügbarkeit, da jeder Name eindeutig und zur Verwendung in Ihrer Organisation verfügbar sein muss.

Einschränkungen

Beim Erstellen von CNAME-Datensätzen für eine benutzerdefinierte Domain sind einige Einschränkungen zu beachten:

- Das Erstellen mehrerer benutzerdefinierter Domain-Namen für denselben bereitgestellten Cluster oder dieselbe Amazon-Redshift-Serverless-Arbeitsgruppe wird nicht unterstützt. Sie können nur einen CNAME-Datensatz zuordnen.
- Die Zuordnung eines CNAME-Datensatzes zu mehreren Clustern oder Arbeitsgruppen wird nicht unterstützt. Der CNAME für jede Redshift-Ressource muss eindeutig sein.

Nachdem Sie Ihre Domain registriert und den CNAME-Datensatz erstellt haben, wählen Sie ein neues oder ein vorhandenes Zertifikat aus. Sie führen diesen Schritt mit AWS Certificate Manager aus:

Ein Zertifikat von ACM für einen Domain-Namen anfordern

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die ACM-Konsole unter https://console.aws.amazon.com/acm/.
2. Wählen Sie Request a certificate aus.
3. Geben Sie in das Feld Domain name (Domain-Name) den Namen Ihrer benutzerdefinierten Domain ein.

> **Note**
>
> Sie können zusätzlich zur Zertifikats-Domain viele Präfixe angeben, um ein einzelnes Zertifikat für mehrere benutzerdefinierte Domain-Datensätze zu verwenden. Zur Veranschaulichung: Sie können zusätzliche Datensätze wie `one.example.com` und `two.example.com` oder einen Wildcard-DNS-Datensatz wie `*.example.com` mit demselben Zertifikat verwenden.

4. Wählen Sie Review and request.
5. Wählen Sie Confirm and request.
6. Damit eine Anforderung gültig ist, muss der registrierte Besitzer einer Internet-Domain der Anforderung vor der Ausstellung des Zertifikats durch ACM zustimmen. Stellen Sie sicher, dass der Status in der ACM-Konsole als Issued angezeigt wird, wenn Sie mit den Schritten fertig sind.

Wir empfehlen Ihnen, ein DNS-validiertes Zertifikat zu erstellen, das die Voraussetzungen für eine verwaltete Erneuerung erfüllt, die mit AWS Certificate Manager verfügbar ist. Eine verwaltete Erneuerung bedeutet, dass ACM Ihre Zertifikate entweder automatisch erneuert oder Ihnen E-Mail-Benachrichtigungen zusendet, wenn sich der Ablaufzeitpunkt nähert. Weitere Informationen finden Sie unter Verwaltete Erneuerung für ACM-Zertifikate.

Erstellen der benutzerdefinierten Domain

Sie können die Amazon-Redshift- oder Amazon-Redshift-Serverless-Konsole verwenden, um Ihre benutzerdefinierte Domain-URL zu erstellen. Wenn Sie sie nicht konfiguriert haben, wird die Eigenschaft Benutzerdefinierter Domain-Name als Bindestrich (–) unter Allgemeine Informationen angezeigt. Nachdem Sie Ihren CNAME-Datensatz und das Zertifikat erstellt haben, weisen Sie den benutzerdefinierten Domain-Namen für den Cluster oder die Arbeitsgruppe zu.

Um eine benutzerdefinierte Domain-Zuordnung zu erstellen, sind die folgenden IAM-Berechtigungen erforderlich:

- `redshift:CreateCustomDomainAssociation` – Sie können die Berechtigung auf einen bestimmten Cluster einschränken, indem Sie dessen ARN hinzufügen.
- `redshiftServerless:CreateCustomDomainAssociation` – Sie können die Berechtigung auf eine bestimmte Arbeitsgruppe einschränken, indem Sie deren ARN hinzufügen.
- `acm:DescribeCertificate`

Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Sie weisen den benutzerdefinierten Domain-Namen zu, indem Sie die folgenden Schritte ausführen.

1. Wählen Sie den Cluster in der Redshift-Konsole oder die Arbeitsgruppe in der Amazon-Redshift-Serverless-Konsole aus und wählen Sie dann im Menü Aktion die Option Benutzerdefinierten Domänennamen erstellen aus. Es wird ein Dialogfeld angezeigt.
2. Geben Sie den benutzerdefinierten Domain-Namen ein.
3. Wählen Sie den ARN von AWS Certificate Manager für das ACM-Zertifikat aus. Bestätigen Sie die Änderungen. Gemäß den Anweisungen in den Schritten, die Sie zum Erstellen des Zertifikats ausgeführt haben, empfehlen wir Ihnen, ein DNS-validiertes Zertifikat zu wählen, das für eine verwaltete Erneuerung durch AWS Certificate Manager infrage kommt.
4. Stellen Sie in den Cluster-Eigenschaften sicher, dass das Feld für den benutzerdefinierten Domain-Namen und den ARN des benutzerdefinierten Domain-Zertifikats mit Ihren Einträgen gefüllt sind. Das Ablaufdatum des Zertifikats der benutzerdefinierten Domain ist ebenfalls aufgeführt.

Nachdem die benutzerdefinierte Domain konfiguriert wurde, kann `sslmode=verify-full` nur für die neue, benutzerdefinierte Domain verwendet werden. Für den Standardendpunkt funktioniert dieser Modus nicht. Sie können jedoch weiterhin eine Verbindung zum Standardendpunkt herstellen, indem Sie andere SSL-Modi verwenden wie `sslmode=verify-ca`.

Umbenennen eines Clusters mit zugewiesener benutzerdefinierte Domain über die Konsole

> **Note**
>
> Diese Schritte gelten nicht für eine Amazon-Redshift-Serverless-Arbeitsgruppe. Sie können den Namen der Arbeitsgruppe nicht ändern.

Um einen Cluster mit einem benutzerdefinierten Domain-Namen umzubenennen, ist die IAM-Berechtigung `acm:DescribeCertificate` erforderlich.

1. Gehen Sie zur Amazon-Redshift-Konsole und wählen Sie den Cluster aus, dessen Namen Sie ändern möchten. Wählen Sie Edit, um die Cluster-Eigenschaften zu bearbeiten.
2. Bearbeiten Sie die Cluster-ID. Sie können auch andere Eigenschaften für den Cluster ändern. Wählen Sie dann Save changes (Änderungen speichern).
3. Nachdem der Cluster umbenannt wurde, müssen Sie den DNS-Datensatz aktualisieren, d. h. den CNAME-Eintrag für die benutzerdefinierte Domain so ändern, dass sie auf den aktualisierten Amazon-Redshift-Endpunkt verweist.

Aktualisieren des CNAME-Datensatzes im Falle einer Notfallwiederherstellung

Die Verwendung eines CNAME-Datensatzes zum Erstellen einer benutzerdefinierten Domain kann bei einer Notfallwiederherstellung hilfreich sein. Wenn der Zugriff auf Ihr Data Warehouse nicht möglich ist, beschreibt das folgende Verfahren, welche Maßnahmen Sie ergreifen können, falls Sie nicht auf Ihren primären Datenbank-Cluster oder Ihre primäre Arbeitsgruppe zugreifen können.

Wir gehen dabei davon aus, dass Sie Verfahren zur Gewährleistung von Hochverfügbarkeit befolgen und über sekundäre Ressourcen verfügen. In diesem Fall könnten Sie beispielsweise über einen Warm-Standby-Cluster oder eine Warm-Standby-Arbeitsgruppe verfügen, die regelmäßig wiederhergestellte Daten vom primären Cluster empfängt. Dieses Backup-Data-Warehouse könnte sich in einer anderen AWS Availability Zone oder in einer separaten Region befinden. Sie können Clients dorthin weiterleiten, indem Sie folgende Schritte ausführen:

1. Bei diesem Schritt wird davon ausgegangen, dass Ihr Cluster oder Ihre Arbeitsgruppe in der Konsole verfügbar ist. Ist dies nicht der Fall, können Sie diesen Schritt überspringen: Wählen Sie den primären Cluster in der Amazon-Redshift-Konsole bzw. die primäre Arbeitsgruppe in der Amazon-Redshift-Serverless-Konsole aus. Der benutzerdefinierte Domain-Name wird in den Eigenschaften angezeigt. Wählen Sie im Menü Aktionen die Option Benutzerdefinierten Domänennamen löschen aus. Geben Sie in dem daraufhin angezeigten Fenster zur Bestätigung delete ein und wählen Sie Löschen aus.
2. Wählen Sie den neuen Cluster oder die neue Arbeitsgruppe aus. Führen Sie die Schritte unter diesem Thema aus, um einen benutzerdefinierten Domain-Name zu erstellen. Verwenden Sie denselben Domain-Namen und wählen Sie denselben CNAME-Datensatz aus, den Sie für den primären Cluster oder die primäre Arbeitsgruppe verwendet haben. Wenn sich Ihre sekundäre Ressource in einer neuen Region befindet, müssen Sie ein neues Zertifikat erstellen und verwenden.
3. Wechseln Sie zu Ihrem Anbieter für die Domain-Registrierung. Dies kann Route 53 oder ein Drittanbieter sein. Wählen Sie den CNAME-Datensatz aus, den Sie ursprünglich erstellt haben. Bei der Erstellung haben Sie den Datensatz so eingestellt, dass er den Datenverkehr an die Endpunkt-URL Ihres primären Clusters oder Ihrer primären Arbeitsgruppe weiterleitet. Ändern Sie den Wert in die Endpunkt-URL Ihres Standby-Clusters oder Ihrer Standby-Arbeitsgruppe. Nachdem Sie die Änderung gespeichert haben, wird der Datenverkehr an die neue Ressource weitergeleitet. Beachten Sie, dass Sie möglicherweise auf die DNS-Weitergabe warten müssen.
4. Dies ist ein optionaler Schritt: Ändern Sie die Regeln für den eingehenden und ausgehenden Netzwerkverkehr in Sicherheitsgruppen, um den Datenverkehr an Ihren Standby-Cluster oder Ihre Standby-Arbeitsgruppe weiterzuleiten. Wenn Sie die Standby-Ressource aktivieren, wird

außerdem davon ausgegangen, dass Sie bereits Wiederherstellungsvorgänge ausgeführt haben oder dies planen, um die Standby-Daten mit den Produktionsdaten in Einklang zu bringen.

Wenn der Wert der Endpunkt-URL geändert wird, um den Datenverkehr umzuleiten, hat dies u. a. den Vorteil, dass für Clients, die Ihren benutzerdefinierten Domain-Namen verwenden, keine Konfigurationsänderungen erforderlich sind. Ihre Verbindungseigenschaften müssen sich nicht ändern.

Beachten Sie, dass alle Maßnahmen zur Notfallwiederherstellung, die Sie ergreifen, im Einklang mit Ihrem bestehenden Verfügbarkeitsplan stehen sollten. Andere Strategien für Ausfallsicherheit, wie z. B. die Bereitstellung von Ressourcen in mehreren Regionen oder komplexe Backup-Techniken, können in diesem Dokument nicht erörtert werden.

> **Note**
>
> Zur Erinnerung: Die Cluster-Verschiebung ist keine Voraussetzung für die Konfiguration von zusätzlichen Redshift-Netzwerk-Features, wie beispielsweise den Features, die für die Notfallwiederherstellung oder andere Zwecke verwendet werden. Sie müssen sie nicht aktivieren, um Folgendes zu ermöglichen:
>
> - Verbindung von einer konto- oder regionsübergreifenden VPC zu Redshift – Sie können eine Verbindung von einer AWS Virtual Private Cloud (VPC) zu einer anderen herstellen, die eine Redshift-Datenbank enthält. Dies erleichtert beispielsweise die Verwaltung des Client-Zugriffs von unterschiedlichen Konten oder VPCs aus, ohne dass lokaler VPC-Zugriff auf Identitäten bereitgestellt werden muss, die eine Verbindung zur Datenbank herstellen. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Amazon Redshift Serverless von einem Redshift-VPC-Endpunkt in einem anderen Konto oder einer anderen Region aus.
> - Einrichtung eines benutzerdefinierten Domain-Namens – Sie können, wie in diesem Thema beschrieben, einen benutzerdefinierten Domain-Namen erstellen, um den Endpunktnamen aussagekräftiger und einfacher zu gestalten.

Beschreiben von benutzerdefinierten Domain-Zuordnungen mithilfe von CLI-Befehlen

Verwenden Sie die Befehle in diesem Abschnitt, um eine Liste mit benutzerdefinierten Domain-Namen abzurufen, die einem bestimmten bereitgestellten Cluster oder einer Amazon-Redshift-Serverless-Arbeitsgruppe zugeordnet sind.

Sie benötigen die folgenden Berechtigungen:

- Für einen bereitgestellten Cluster: `redshift:DescribeCustomDomainAssociations`
- Für eine Amazon-Redshift-Serverless-Arbeitsgruppe: `redshiftServerless:ListCnameAssociations`

Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Im Folgenden ist ein Beispielbefehl zum Auflisten der benutzerdefinierten Domain-Namen für einen bestimmten Amazon-Redshift-Cluster zu sehen:

```
aws redshift describe-custom-domain-association --cluster-id redshiftclustersample --
custom-domain-name customdomainname
```

Sie können diesen Befehl ausführen, wenn Sie einen benutzerdefinierten Domain-Namen aktiviert haben, um die dem Cluster zugeordneten benutzerdefinierten Domain-Namen zu ermitteln. Weitere Informationen zum CLI-Befehl für zum Beschreiben von benutzerdefinierten Domänenzuordnungen finden Sie unter describe-custom-domain-associations.

Im Folgenden ist ein Beispielbefehl zum Auflisten der benutzerdefinierten Domain-Namen für eine bestimmte Amazon-Redshift-Serverless-Arbeitsgruppe zu sehen: Hierbei gibt es verschiedene Möglichkeiten. Sie können nur den benutzerdefinierten Domain-Namen angeben:

```
aws redshift-serverless list-cname-associations --custom-domain-
name customdomainnamesample
```

Sie können auch die Zuordnungen abrufen, indem Sie nur den Arbeitsgruppennamen angeben:

```
aws redshift-serverless list-cname-associations --workgroup-name workgroupnamesample
```

Sie können auch die Zuordnungen abrufen, indem Sie nur den Zertifikat-ARN angeben:

```
aws redshift-serverless list-cname-associations --custom-certificate-
arn certificatearnsample
```

Sie können diese Befehle ausführen, wenn Sie einen benutzerdefinierten Domain-Namen aktiviert haben, um die der Arbeitsgruppe zugeordneten benutzerdefinierten Domain-Namen zu

ermitteln. Sie können auch einen Befehl ausführen, um die Eigenschaften einer benutzerdefinierten Domain-Zuordnung abzurufen. Hierfür müssen Sie den benutzerdefinierten Domain-Namen und den Arbeitsgruppennamen als Parameter angeben. Der Befehl gibt den Zertifikat-ARN, den Arbeitsgruppennamen und den Ablaufzeitpunkt des Zertifikats der benutzerdefinierten Domain zurück:

```
aws redshift-serverless get-custom-domain-association --workgroup-
name workgroupnamesample --custom-domain-name customdomainnamesample
```

Weitere Informationen zu verfügbaren CLI-Referenzbefehlen für Amazon Redshift Serverless finden Sie unter redshift-serverless.

Zuordnen der benutzerdefinierten Domain zu einem anderen Zertifikat

Um die Zertifikatszuordnung für einen benutzerdefinierten Domain-Namen zu ändern, sind die folgenden IAM-Berechtigungen erforderlich:

- `redshift:ModifyCustomDomainAssociation`
- `acm:DescribeCertificate`

Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Verwenden Sie den folgenden Befehl, um die benutzerdefinierte Domain einem anderen Zertifikat zuzuordnen. Die Argumente `--custom-domain-name` und `custom-domain-certificate-arn` sind obligatorisch. Der ARN für das neue Zertifikat muss sich vom vorhandenen ARN unterscheiden.

```
aws redshift modify-custom-domain-association --cluster-id redshiftclustersample --
custom-domain-name customdomainnamesample --custom-domain-certificate-arn ARNsample
```

Das folgende Beispiel zeigt, wie die benutzerdefinierte Domain einem anderen Zertifikat für eine Amazon-Redshift-Serverless-Arbeitsgruppe zugeordnet wird.

```
aws redshift-serverless modify-custom-domain-association --workgroup-
name redshiftworkgroupsample --custom-domain-name customdomainnamesample --custom-
domain-certificate-arn ARNsample
```

Es dauert maximal 30 Sekunden, bis Sie eine Verbindung zum Cluster herstellen können. Ein Teil der Verzögerung tritt auf, wenn der Amazon-Redshift-Cluster seine Eigenschaften aktualisiert, und es gibt eine zusätzliche Verzögerung, wenn DNS aktualisiert wird. Weitere Informationen zur API und den einzelnen Eigenschaftseinstellungen finden Sie unter ModifyCustomDomainAssociation.

Löschen der benutzerdefinierten Domain

Um den benutzerdefinierten Domain-Namen zu löschen, muss der Benutzer über Berechtigungen für die folgenden Aktionen verfügen:

- Für einen bereitgestellten Cluster: `redshift:DeleteCustomDomainAssociation`
- Für eine Amazon-Redshift-Serverless-Arbeitsgruppe: `redshiftServerless:DeleteCustomDomainAssociation`

In der Konsole

Sie können den benutzerdefinierten Domain-Namen löschen, indem Sie die Schaltfläche Aktionen und anschließend Benutzerdefinierten Domänennamen löschen auswählen. Danach können Sie immer noch eine Verbindung zum Server herstellen, indem Sie Ihre Tools so aktualisieren, dass sie die in der Konsole aufgeführten Endpunkte verwenden.

Mithilfe eines CLI-Befehls

Das folgende Beispiel zeigt, wie der benutzerdefinierte Domain-Name gelöscht wird. Für den Löschvorgang müssen Sie den vorhandenen benutzerdefinierten Domain-Namen für den Cluster angeben.

```
aws redshift delete-custom-domain-association --cluster-id redshiftclustersample --
custom-domain-name customdomainnamesample
```

Das folgende Beispiel zeigt, wie der benutzerdefinierte Domain-Name für eine Amazon-Redshift-Serverless-Arbeitsgruppe gelöscht wird. Der benutzerdefinierte Domain-Name ist ein erforderlicher Parameter.

```
aws redshift-serverless delete-custom-domain-association --workgroup-name workgroupname
 --custom-domain-name customdomainname
```

Weitere Informationen finden Sie unter DeleteCustomDomainAssociation.

Herstellen einer Verbindung zu Ihrem Cluster oder Ihrer Arbeitsgruppe mit einem benutzerdefinierten Domain-Namen unter Verwendung eines SQL-Clients

Um eine Verbindung mit einem benutzerdefinierten Domain-Namen herzustellen, sind die folgenden IAM-Berechtigungen für einen bereitgestellten Cluster erforderlich: `redshift:DescribeCustomDomainAssociations` Für Amazon Redshift Serverless müssen Sie keine Berechtigungen hinzufügen.

Als bewährte Methode empfehlen wir, einer IAM-Rolle Berechtigungsrichtlinien anzufügen und sie dann nach Bedarf Benutzern und Gruppen zuzuweisen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon Redshift.

Wenn Sie die Schritte zur Erstellung Ihres CNAME abgeschlossen haben und diesen Ihrem Cluster oder Ihrer Arbeitsgruppe in der Konsole zuweisen, können Sie die benutzerdefinierte URL in den Verbindungseigenschaften Ihres SQL-Clients angeben. Beachten Sie, dass es unmittelbar nach der Erstellung eines CNAME-Datensatzes zu Verzögerungen bei der DNS-Propagierung kommen kann.

1. Öffnen Sie einen SQL-Client. Sie können beispielsweise SQL/Workbench J verwenden. Öffnen Sie die Eigenschaften für eine Verbindung und fügen Sie den benutzerdefinierten Domain-Namen für die Verbindungszeichenfolge hinzu. Beispiel: `jdbc:redshift://mycluster.example.com:5439/dev?sslmode=verify-full` In diesem Beispiel gibt `dev` die Standarddatenbank an.
2. Fügen Sie den Benutzernamen und das Passwort für Ihren Datenbankbenutzer hinzu.
3. Testen Sie die Verbindung. Ihre Fähigkeit, Datenbankressourcen wie bestimmte Tabellen abzufragen, kann je nach den Berechtigungen, die dem Datenbankbenutzer oder den zugewiesenen Amazon-Redshift-Datenbankrollen gewährt wurden, variieren.

   Beachten Sie, dass Sie Ihren Cluster oder Ihre Arbeitsgruppe möglicherweise so einrichten müssen, dass er/sie öffentlich zugänglich ist, um eine Verbindung zu ihm/ihr herzustellen, wenn er/sie sich in einer VPC befindet. Sie können diese Einstellung in den Netzwerkeigenschaften ändern.

> **Note**
>
> Verbindungen zu einem benutzerdefinierten Domain-Namen werden mit JDBC- und Python-Treibern unterstützt. ODBC-Verbindungen werden nicht unterstützt.

Arbeiten mit von RedShift verwalteten VPC-Endpunkten

Standardmäßig wird ein Amazon Redshift-Cluster oder eine Amazon Redshift Serverless-Arbeitsgruppe in einer Virtual Private Cloud (VPC) bereitgestellt. Auf die VPC kann von einer anderen VPC oder einem anderen Subnetz aus zugegriffen werden, wenn Sie entweder den öffentlichen Zugriff zulassen oder ein Internet-Gateway, ein NAT-Gerät oder eine AWS Direct Connect Verbindung einrichten, um den Verkehr dorthin weiterzuleiten. Sie können auch auf einen Cluster oder eine Arbeitsgruppe zugreifen, indem Sie einen von Redshift verwalteten VPC-Endpunkt (powered by) einrichten. AWS PrivateLink

Sie können einen von Redshift verwalteten VPC-Endpunkt als private Verbindung zwischen einer VPC, die einen Cluster oder eine Arbeitsgruppe enthält, und einer VPC, auf der ein Client-Tool ausgeführt wird, einrichten. Wenn sich der Cluster oder die Arbeitsgruppe in einem anderen Konto befindet, muss der Kontoinhaber (Gewährer) Zugriff auf das Verbindungskonto (Empfänger) gewähren. Mit diesem Ansatz können Sie auf das Data Warehouse zugreifen, ohne eine öffentliche IP-Adresse zu verwenden oder den Datenverkehr über das Internet weiterzuleiten.

Dies sind häufige Gründe dafür, den Zugriff über einen von Redshift verwalteten VPC-Endpunkt zuzulassen:

- AWS Konto A möchte einer VPC in AWS Konto B Zugriff auf einen Cluster oder eine Arbeitsgruppe gewähren.
- AWS Konto A möchte einer VPC, die sich auch in AWS Konto A befindet, Zugriff auf einen Cluster oder eine Arbeitsgruppe gewähren.
- AWS Konto A möchte einem anderen Subnetz in der VPC innerhalb von AWS Konto A Zugriff auf einen Cluster oder eine Arbeitsgruppe gewähren.

Der Workflow zum Einrichten eines von Redshift verwalteten VPC-Endpunkts für den Zugriff auf einen Cluster oder eine Arbeitsgruppe in einem anderen Konto lautet wie folgt:

1. Das Besitzerkonto gewährt einem anderen Konto die Zugriffsberechtigung und gibt die AWS Konto-ID und VPC-ID (oder alle VPCs) des Empfängers an.
2. Das Konto des Berechtigungsempfängers wird benachrichtigt, dass er die Berechtigung zum Erstellen eines von RedShift verwalteten VPC-Endpunkts besitzt.
3. Das Konto des Berechtigungsempfängers erstellt einen von RedShift verwalteten VPC-Endpunkt.
4. Das Empfängerkonto greift über den von Redshift verwalteten VPC-Endpunkt auf den Cluster oder die Arbeitsgruppe des Besitzerkontos zu.

Sie können dies mit der Amazon Redshift Redshift-Konsole AWS CLI, der oder der Amazon Redshift Redshift-API tun.

Überlegungen bei der Verwendung von RedShift-verwalteten VPC-Endpunkten

> **Note**
>
> Um von Redshift verwaltete VPC-Endpoints zu erstellen oder zu ändern, benötigen Sie zusätzlich zu anderen `ec2:ModifyVpcEndpoint` in der verwalteten Richtlinie angegebenen Berechtigungen die entsprechende Genehmigung `ec2:CreateVpcEndpoint` oder in Ihrer IAM-Richtlinie. AWS `AmazonRedshiftFullAccess`

Berücksichtigen Sie bei der Verwendung von RedShift-verwalteten VPC-Endpunkten Folgendes:

- Stellen Sie sicher, dass es sich bei dem Cluster um einen RA3-Knotentyp handelt. Eine Amazon Redshift Serverless-Arbeitsgruppe funktioniert auch dafür.
- Stellen Sie bei bereitgestellten Clustern sicher, dass für den Cluster, auf den zugegriffen werden soll, die Cluster-Verlagerung aktiviert ist. Informationen zu den Anforderungen zum Aktivieren der Clusterverschiebung finden Sie unter Ihren Cluster verlagern.
- Stellen Sie sicher, dass der Cluster oder die Arbeitsgruppe, auf den über die Sicherheitsgruppe zugegriffen werden soll, innerhalb der gültigen Portbereiche 5431-5455 und 8191-8215 verfügbar ist. Der Standardwert ist 5439.
- Sie können die VPC-Sicherheitsgruppen ändern, die einem vorhandenen RedShift-verwalteten VPC-Endpunkt zugeordnet sind. Um andere Einstellungen zu ändern, löschen Sie den aktuellen RedShift-verwalteten VPC-Endpunkt und erstellen Sie einen neuen.
- Die Anzahl der von RedShift verwalteten VPC-Endpunkte, die Sie erstellen können, ist durch Ihr VPC-Endpunktkontingent beschränkt.
- Auf die RedShift-verwalteten VPC-Endpunkte kann nicht über das Internet zugegriffen werden. Auf einen von Redshift verwalteten VPC-Endpunkt kann nur innerhalb der VPC zugegriffen werden, in der der Endpunkt bereitgestellt wird, oder von allen VPCs, die mit der VPC gepeert werden, in der der Endpunkt bereitgestellt wird, wie es die Routing-Tabellen und Sicherheitsgruppen zulassen.
- Sie können die Amazon-VPC-Konsole nicht zum Verwalten der von Redshift verwalteten VPC-Endpunkte verwenden.

- Wenn Sie einen von Redshift verwalteten VPC-Endpunkt für einen bereitgestellten Cluster erstellen, muss die von Ihnen gewählte VPC über eine Subnetzgruppe verfügen. Informationen zum Erstellen einer Subnetzgruppe finden Sie unter. Verwalten von Cluster-Subnetzgruppen über die Konsole

Hinweise zu Kontingenten und Benennungseinschränkungen finden Sie unter Kontingente und Limits in Amazon Redshift.

Informationen zu Preisen finden Sie unter AWS PrivateLink -Preise.

Verwaltung von Redshift-verwalteten VPC-Endpunkten mithilfe der Konsole

Sie können die Verwendung von RedShift-verwalteten VPC-Endpunkten mithilfe der Amazon-Redshift-Konsole konfigurieren.

Gewähren von -Zugriff

Wenn sich die VPC, auf die Sie auf Ihren Cluster oder Ihre Arbeitsgruppe zugreifen möchten, in einem anderen AWS Konto befindet, stellen Sie sicher, dass Sie sie über das Konto des Besitzers (Grantors) autorisieren.

Um einer VPC in einem anderen AWS Konto den Zugriff auf Ihren Cluster oder Ihre Arbeitsgruppe zu ermöglichen

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Wählen Sie für Amazon Redshift Serverless Serverless das Serverless-Dashboard.
3. Für einen Cluster, auf den Sie Zugriff gewähren möchten, zeigen Sie die Details an, indem Sie den Clusternamen auswählen. Wählen Sie die Registerkarte Properties (Eigenschaften) für den Cluster aus.

   Im Abschnitt Granted accounts (Berechtigte Konten) werden die Konten und die entsprechenden VPCs angezeigt, die Zugriff auf Ihren Cluster haben. Wählen Sie für eine Amazon Redshift Serverless-Arbeitsgruppe die Arbeitsgruppe aus. Erteilte Konten sind auf der Registerkarte Datenzugriff verfügbar.
4. Klicken Sie auf Grant access (Zugriff gewähren), um ein Formular zum Eingeben der Grantee information (Berechtigungsinformationen) anzuzeigen.

5. Geben Sie als AWS -Konto-ID die ID des Kontos ein, dem Sie den Zugriff gewähren möchten. Sie können Zugriff auf bestimmte VPCs oder alle VPCs im angegebenen Konto gewähren.
6. Klicken Sie auf Grant access (Zugriff gewähren), um die Zugriffsberechtigung zu erteilen.

Erstellen eines mit RedShift verwalteten VPC-Endpunkts

Wenn Sie einen Cluster oder eine Arbeitsgruppe besitzen oder Ihnen Zugriff auf deren Verwaltung gewährt wurde, können Sie dafür einen von Redshift verwalteten VPC-Endpunkt erstellen.

So erstellen Sie einen mit RedShift verwalteten VPC-Endpunkt

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Configurations (Konfigurationen) aus.

   Die Seite Configurations (Konfigurationen) zeigt die von RedShift verwalteten VPC-Endpunkte an, die erstellt wurden. Um Details für einen Endpunkt anzuzeigen, wählen Sie den Namen des Endpunkts. Für Amazon Redshift Serverless befinden sich die VPC-Endpunkte auf der Registerkarte Datenzugriff, wenn Sie die Arbeitsgruppe auswählen.
3. Klicken Sie auf Create endpoint (Endpunkt erstellen), um ein Formular zum Eingeben von Informationen über den hinzuzufügenden Endpunkt anzuzeigen.
4. Geben Sie Werte für den Endpunktnamen, die 12-stellige AWS Konto-ID, die Virtual Private Cloud (VPC), in der sich der Endpunkt befindet, das Subnetz und die VPC-Sicherheitsgruppe ein.

   Das Subnetz in Subnet definiert die Subnetze und IP-Adressen, in denen Amazon Redshift den Endpunkt bereitstellt. Amazon Redshift wählt ein Subnetz mit IP-Adressen für die dem Endpunkt zugeordnete Netzwerkschnittstelle.

   Die Sicherheitsgruppenregeln in der VPC-Sicherheitsgruppe definieren die Ports, Protokolle und Quellen für eingehenden Datenverkehr, den Sie für Ihren Endpunkt autorisieren. Sie erlauben den Zugriff auf den ausgewählten Port über die Sicherheitsgruppe oder den CIDR-Bereich, in dem Ihre Workloads ausgeführt werden.
5. Klicken Sie auf Create endpoint (Endpunkt erstellen), um den Endpunkt zu erstellen.

Nachdem Ihr Endpunkt erstellt wurde, können Sie über die URL, die in den Konfigurationseinstellungen für Ihren von Redshift verwalteten VPC-Endpunkt unter Endpunkt-URL angezeigt wird, auf den Cluster oder die Arbeitsgruppe zugreifen.

Verwaltung von Redshift-verwalteten VPC-Endpunkten mit dem AWS CLI

Sie können die folgenden Amazon-Redshift-CLI-Operationen für die Arbeit mit RedShift-verwalteten VPC-Endpunkten verwenden. Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

- authorize-endpoint-access
- revoke-endpoint-access
- create-endpoint-access
- modify-endpoint-access
- delete-endpoint-access
- describe-endpoint-access
- describe-endpoint-authorization

Verwalten von RedShift-verwalteten VPC-Endpunkten mit Amazon-RedShift-API-Operationen

Sie können die folgenden Amazon-Redshift-API-Operationen für die Arbeit mit RedShift-verwalteten VPC-Endpunkten verwenden. Weitere Informationen finden Sie in der Amazon-Redshift-API-Referenz.

- AuthorizeEndpointAccess
- RevokeEndpointAccess
- CreateEndpointAccess
- ModifyEndpointAccess
- DeleteEndpointAccess
- DescribeEndpointAccess
- DescribeEndpointAuthorization

Verwaltung von Redshift-verwalteten VPC-Endpunkten mit AWS CloudFormation

Informationen zum AWS CloudFormation Ressourcentyp, mit dem ein Redshift-verwalteter VPC-Endpunkt erstellt werden soll AWS CloudFormation, finden Sie AWS::Redshift::EndpointAccessim Benutzerhandbuch.AWS CloudFormation

Enhanced VPC Routing in Amazon Redshift

Wenn Sie Enhanced VPC Routing für Amazon Redshift verwenden, erzwingt Amazon Redshift, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Ihren Datenrepositorys über Ihre Virtual Private Cloud (VPC) erfolgt, die auf dem Amazon-VPC-Service basiert. Enhanced VPC Routing ermöglicht, Standard-VPC-Funktionen, beispielsweise VPC-Sicherheitsgruppen, Netzwerk-Zugriffskontrolllisten, VPC-Endpunkte, VPC-Endpunktrichtlinien, Internet-Gateways und Domain Name System (DNS)-Server, wie im Amazon-VPC-Benutzerhandbuch beschrieben zu verwenden. Sie können mit diesen Funktionen den Datenfluss zwischen dem Amazon-Redshift-Cluster und anderen Ressourcen fein abgestimmt verwalten. Wenn Sie Enhanced VPC Routing zur Weiterleitung des Datenverkehrs durch Ihre VPC verwenden, können Sie auch VPC-Flussprotokolle verwenden, um den COPY- und UNLOAD-Datenverkehr zu überwachen.

Amazon-Redshift-Cluster und Amazon Redshift-Serverless-Arbeitsgruppen unterstützen Enhanced VPC Routing. Sie können Enhanced VPC Routing nicht mit Redshift Spectrum verwenden. Weitere Informationen finden Sie unter Redshift Spectrum und Enhanced VPC Routing.

Wenn das erweiterte VPC-Routing nicht aktiviert ist, leitet Amazon Redshift den Datenverkehr über das Internet weiter, einschließlich des Datenverkehrs zu anderen Diensten innerhalb des AWS Netzwerks.

> **Important**
>
> Da Enhanced VPC Routing sich darauf auswirkt, wie Amazon Redshift auf andere Ressourcen zugreift, schlagen COPY- und UNLOAD-Befehle möglicherweise fehl, wenn Ihre VPC nicht ordnungsgemäß konfiguriert wurde. Sie müssen speziell einen Netzwerkpfad zwischen Ihrem VPC-Cluster und Ihren Datenressourcen erstellen, wie nachfolgend beschrieben.

Wenn Sie einen COPY- oder UNLOAD-Befehl auf einem Cluster mit aktiviertem Enhanced VPC Routing ausführen, leitet Ihre VPC den Datenverkehr über den strengsten bzw. spezifischsten verfügbaren Netzwerkpfad zu der angegebenen Ressource.

Sie können beispielsweise die folgenden Wege in Ihrer VPC konfigurieren:

- VPC-Endpunkte — Für Traffic zu einem Amazon S3 S3-Bucket in derselben AWS Region wie Ihr Cluster können Sie einen VPC-Endpunkt erstellen, um den Datenverkehr direkt an den Bucket weiterzuleiten. Wenn Sie VPC-Endpunkte verwenden, können Sie eine Endpunktrichtlinie anfügen, um den Zugriff auf Amazon S3 zu verwalten. Weitere Informationen zur Verwendung von Endpunkten mit Amazon Redshift finden Sie unter Arbeiten mit VPC-Endpunkten. Wenn Sie Lake Formation verwenden, finden Sie weitere Informationen zum Herstellen einer privaten Verbindung zwischen Ihrer VPC und AWS Lake Formation at AWS Lake Formation und zu den VPC-Schnittstellen-Endpunkten ().AWS PrivateLink
- NAT-Gateway — Sie können eine Verbindung zu einem Amazon S3 S3-Bucket in einer anderen AWS Region herstellen, und Sie können eine Verbindung zu einem anderen Service innerhalb des AWS Netzwerks herstellen. Sie können auch auf eine Host-Instance außerhalb des AWS Netzwerks zugreifen. Dazu müssen Sie ein Network Address Translation (NAT)-Gateway erstellen, wie im Amazon-VPC-Benutzerhandbuch beschrieben.
- Internet-Gateway – Zum Verbinden mit AWS -Services außerhalb Ihrer VPC können Sie ein Internet-Gateway an Ihr VPC-Subnetz anfügen, wie im Amazon-VPC-Benutzerhandbuch beschrieben. Zur Verwendung eines Internet-Gateways muss Ihr Cluster eine öffentliche IP haben, damit andere Services mit ihm kommunizieren können.

Weitere Informationen finden Sie unter VPC-Endpunkte im Amazon-VPC-Benutzerhandbuch.

Für die Nutzung von Enhanced VPC Routing fallen keine zusätzlichen Gebühren an. Möglicherweise fallen bei bestimmten Operationen Datenübertragungskosten an. Dazu gehören Operationen wie UNLOAD to Amazon S3 in einer anderen AWS Region. COPY aus Amazon EMR oder Secure Shell (SSH) mit öffentlichen IP-Adressen. Weitere Informationen zu Preisen finden Sie unter Amazon EC2 – Preise.

Themen

- Arbeiten mit VPC-Endpunkten
- Enhanced VPC routing (Erweitertes VPC-Routing
- Redshift Spectrum und Enhanced VPC Routing

Arbeiten mit VPC-Endpunkten

Sie können einen VPC-Endpunkt verwenden, um eine verwaltete Verbindung zwischen Ihrem Amazon-Redshift-Cluster in einer VPC und Amazon Simple Storage Service (Amazon S3) herzustellen. Wenn Sie dies tun, bleibt der COPY- und UNLOAD-Datenverkehr zwischen Ihrer Datenbank und Ihren Daten in Amazon S3 in Ihrer Amazon VPC. Sie können eine Endpunktrichtlinie mit Ihrem Endpunkt verbinden, um den Zugriff auf Ihre Daten besser verwalten zu können. Beispielsweise können Sie Ihrem VPC-Endpunkt eine Richtlinie hinzufügen, die das Entladen von Daten nur zu einem bestimmten Amazon-S3-Bucket in Ihrem Konto erlaubt.

> **Important**
>
> Derzeit unterstützt Amazon Redshift VPC-Endpunkte nur für die Verbindung mit Amazon S3. Wenn Amazon VPC Unterstützung für andere AWS Services zur Nutzung von VPC-Endpunkten hinzufügt, unterstützt Amazon Redshift auch diese VPC-Endpunktverbindungen. Um über einen VPC-Endpunkt eine Verbindung zu einem Amazon S3 S3-Bucket herzustellen, müssen sich der Amazon Redshift Redshift-Cluster und der Amazon S3 S3-Bucket, mit dem er eine Verbindung herstellt, in derselben AWS Region befinden.

Erstellen Sie zur Verwendung von VPC-Endpunkten einen VPC-Endpunkt für die VPC, in der sich Ihr Data Warehouse befindet, und aktivieren Sie dann Enhanced VPC Routing. Sie können Enhanced VPC Routing aktivieren, wenn Sie Ihren Cluster oder Ihre Arbeitsgruppe erstellen, oder Sie können einen Cluster oder eine Arbeitsgruppe in einer VPC so modifizieren, dass er/sie Enhanced VPC Routing verwendet.

Ein VPC-Endpunkt verwendet Routing-Tabellen zum Steuern der Weiterleitung des Datenverkehrs zwischen einem Cluster oder einer Arbeitsgruppe in der VPC und Amazon S3. Alle Cluster und Arbeitsgruppen in mit den angegebenen Routing-Tabellen verbundenen Subnetzen verwenden automatisch diesen Endpunkt zum Zugriff auf den Service.

Ihre VPC verwendet die am meisten spezifische bzw. restriktive Route, die dem Datenverkehr entspricht, um zu bestimmen, wie der Datenverkehr weitergeleitet werden soll. Angenommen, es gibt eine Route in Ihrer Routing-Tabelle für den gesamten Internetdatenverkehr (0.0.0.0/0), die auf ein Internet-Gateway und einen Amazon-S3-Endpunkt verweist. In diesem Fall erhält die Endpunktroute Vorrang für den gesamten für Amazon S3 bestimmten Datenverkehr. Der Grund dafür ist, dass der IP-Adressbereich für den Amazon-S3-Service eine spezifischere Angabe als 0.0.0.0/0 ist. In

diesem Beispiel wird der gesamte sonstige Internetdatenverkehr einschließlich des Datenverkehrs zu Amazon-S3-Buckets in anderen AWS-Regionenüber das Internet-Gateway geleitet.

Weitere Informationen zum Erstellen von VPC-Endpunkten finden Sie unter Erstellen eines VPC-Endpunkts im VPC-Benutzerhandbuch.

Sie verwenden Endpunktrichtlinien zur Steuerung des Zugriffs von Ihrem Cluster oder Ihrer Arbeitsgruppe auf die Amazon-S3-Buckets, die Ihre Datendateien enthalten. Um eine spezifischere Steuerung zu erzielen, können Sie optional eine benutzerdefinierte Endpunktrichtlinie hinzufügen. Weitere Informationen finden Sie unter Steuern des Zugriffs auf Services mit Endpunktrichtlinien im AWS PrivateLink -Leitfaden.

Für die Nutzung von Endpunkten fallen keine zusätzlichen Gebühren an. Für die Datenübertragung und Ressourcennutzung fallen die Standardgebühren an. Weitere Informationen zu Preisen finden Sie unter Amazon EC2 – Preise.

Enhanced VPC routing (Erweitertes VPC-Routing

Sie können Enhanced VPC Routing aktivieren, wenn Sie einen Cluster erstellen oder ändern und wenn Sie eine Amazon-Redshift-Serverless-Arbeitsgruppe erstellen oder ändern.

Zum Arbeiten mit Enhanced VPC Routing für einen Cluster muss Ihr Cluster den folgenden Voraussetzungen und Einschränkungen entsprechen:

- Ihr Cluster muss sich in einer VPC befinden.

  Wenn Sie einen Amazon S3 S3-VPC-Endpunkt anhängen, verwendet Ihr Cluster den VPC-Endpunkt nur für den Zugriff auf Amazon S3 S3-Buckets in derselben Region. AWS Um auf Buckets in einer anderen AWS Region zuzugreifen (ohne den VPC-Endpunkt zu verwenden) oder auf andere AWS Dienste zuzugreifen, machen Sie Ihren Cluster öffentlich zugänglich oder verwenden Sie ein Network Address Translation (NAT) -Gateway. Weitere Informationen finden Sie unter Erstellen eines Clusters in einer VPC.
- Sie müssen in Ihrer VPC die DSN-Namensauflösung aktivieren. Alternativ müssen Sie, wenn Sie einen eigenen DNS-Server betreiben, sicherstellen, dass DNS-Anforderungen an Amazon S3 korrekt in die von AWS gepflegten IP-Adressen aufgelöst werden. Weitere Informationen finden Sie unter Verwendung von DNS in Ihrer VPC im Amazon VPC Benutzerhandbuch.
- In Ihrer VPC müssen DNS-Hostnamen aktiviert sein. DNS-Hostnamen werden standardmäßig aktiviert.

- Ihre VPC-Endpunktrichtlinien müssen den Zugriff auf alle mit COPY-, UNLOAD- oder CREATE LIBRARY-Aufrufen in Amazon Redshift verwendeten Amazon-S3-Buckets zulassen, einschließlich Zugriff auf eventuell vorhandene Manifestdateien. Für COPY von Remote-Hosts müssen Ihre Endpunktrichtlinien den Zugriff auf jeden Hostcomputer zulassen. Weitere Informationen finden Sie unter IAM-Berechtigungen für COPY, UNLOAD und CREATE LIBRARY im Datenbankentwicklerhandbuch zu Amazon Redshift.

So erstellen Sie einen Cluster mit erweitertem VPC-Routing:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Provisioned clusters dashboard (Dashboard für bereitgestellte Cluster) und dann Create cluster (Cluster erstellen) aus und geben Sie die Eigenschaften unter Cluster details (Cluster-Details) ein.
3. Um den Abschnitt Additional configurations (Zusätzliche Konfigurationen) anzuzeigen, deaktivieren Sie Use defaults (Standardeinstellungen verwenden).
4. Navigieren Sie zum Abschnitt Network and security (Netzwerk und Sicherheit).
5. Um Enhanced VPC Routing zu aktivieren, wählen Sie Turn on (Aktivieren) aus, um den Cluster-Datenverkehr über die VPC zu erzwingen.
6. Wählen Sie Create cluster (Cluster erstellen) aus, um den Cluster zu erstellen. Es kann einige Minuten dauern, bis der Cluster zur Verwendung bereit ist.

So erstellen Sie eine Arbeitsgruppe in Amazon Redshift Serverless mit Enhanced VPC Routing

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Serverless Dashboard und anschließend Create Workgroup (Arbeitsgruppe erstellen) aus und geben Sie die Eigenschaften für Ihre Arbeitsgruppe ein.
3. Navigieren Sie zum Abschnitt Network and security (Netzwerk und Sicherheit).
4. Wählen Sie Turn on Enhanced VPC Routing (Enhanced VPC Routing aktivieren) aus, um den Netzwerkdatenverkehr über die VPC zu leiten.
5. Wählen Sie Next (Weiter) aus und beenden Sie die Eingabe Ihrer Arbeitsgruppeneigenschaften, bis Sie die Arbeitsgruppe erstellen (Create).

Redshift Spectrum und Enhanced VPC Routing

Amazon Redshift Spectrum bietet keine Unterstützung für Enhanced VPC Routing mit bereitgestellten Clustern. Enhanced VPC Routing für Amazon Redshift leitet bestimmten Datenverkehr über Ihre VPC. Der gesamte Datenverkehr zwischen Ihrem Cluster und Ihren Amazon-S3-Buckets wird erzwungenermaßen über Ihre Amazon VPC geleitet. Redshift Spectrum läuft auf AWS verwalteten Ressourcen, die Amazon Redshift gehören. Da sich diese Ressourcen außerhalb Ihrer VPC befinden, verwendet Redshift Spectrum das Enhanced VPC Routing nicht.

Der Datenverkehr zwischen Redshift Spectrum und Amazon S3 wird sicher über das AWS private Netzwerk außerhalb Ihrer VPC geleitet. Eingehender Datenverkehr wird mit dem Amazon Signature Version 4-Protokoll (SIGv4) signiert und mit HTTPS verschlüsselt. Dieser Datenverkehr wird auf der Grundlage der IAM-Rolle autorisiert, die Ihrem Amazon-Redshift-Cluster angefügt ist. Um den Redshift-Spectrum-Datenverkehr weiter zu verwalten, können Sie die IAM-Rolle Ihres Clusters und Ihre an den Amazon-S3-Bucket angehängte Richtlinie ändern. Möglicherweise müssen Sie Ihre VPC auch so konfigurieren, dass Ihr Cluster auf Athena zugreifen AWS Glue kann, wie im Folgenden beschrieben.

Da Enhanced VPC Routing sich darauf auswirkt, wie Amazon Redshift auf andere Ressourcen zugreift, schlagen Abfragen möglicherweise fehl, wenn Ihre VPC nicht ordnungsgemäß konfiguriert wurde. Weitere Informationen finden Sie unter Enhanced VPC Routing in Amazon Redshift. Hier wird die Erstellung eines VPC-Endpunkts, eines NAT-Gateways und anderer Netzwerkressourcen zum Umleiten des Datenverkehrs auf Ihre Amazon-S3-Buckets ausführlicher beschrieben.

> **Note**
>
> Amazon Redshift Serverless unterstützt Enhanced VPC Routing für Abfragen an externe Tabellen in Amazon S3.

Überlegungen zur Verwendung von Amazon Redshift Spectrum

Nachfolgend finden Sie einige Überlegungen zur Verwendung von Redshift Spectrum:

- Richtlinien für den Bucket-Zugriff
- Cluster-IAM-Rolle
- Protokollieren und Prüfen des Amazon-S3-Zugriffs
- Zugang zu AWS Glue oder Amazon Athena

Richtlinien für den Bucket-Zugriff

Sie können den Zugriff auf Daten in Ihren Amazon-S3-Buckets mit einer Richtlinie steuern, die dem Bucket angefügt ist, aber auch über eine IAM-Rolle, die dem Cluster angefügt ist.

Redshift Spectrum auf bereitgestellten Clustern kann nicht auf Daten zugreifen, die in Amazon-S3-Buckets gespeichert sind, wenn diese eine Bucket-Richtlinie verwenden, die den Zugriff auf bestimmte VPC-Endpunkte beschränkt. Verwenden Sie stattdessen eine Bucket-Richtlinie, die den Zugriff nur auf bestimmte Prinzipale beschränkt, z. B. auf ein bestimmtes AWS Konto oder bestimmte Benutzer.

Verwenden Sie für die IAM-Rolle, die Zugriff auf den Bucket erhält, eine Vertrauensstellung, die die Annahme der Rolle nur durch den Amazon-Redshift-Service-Prinzipal erlaubt. Wenn die Rolle Ihrem Cluster angefügt ist, kann sie nur im Kontext von Amazon Redshift verwendet und nicht außerhalb des Clusters freigegeben werden. Weitere Informationen finden Sie unter Einschränken des Zugriffs auf IAM-Rollen. Es kann auch eine Service-Kontrollrichtlinie (SCP) verwendet werden, um die Rolle weiter einzuschränken. Weitere Informationen finden Sie unter Verhindern, dass IAM-Benutzer und -Rollen bestimmte Änderungen vornehmen, mit Ausnahme für eine angegebene Administratorrolle im AWS Organizations -Benutzerhandbuch.

Um Redshift Spectrum zu verwenden, dürfen keine IAM-Richtlinien vorhanden sein, die die Verwendung vorsignierter URLs blockieren.

Die folgende Beispiel-Bucket-Richtlinie erlaubt den Zugriff auf den angegebenen Bucket nur aus Datenverkehr, der von Redshift Spectrum stammt, das einem AWS Konto `123456789012` gehört.

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

```
}
```

Cluster-IAM-Rolle

Die Ihrem Cluster angefügte Rolle sollte über eine Vertrauensstellung verfügen, die die Annahme der Rolle nur dem Amazon-Redshift-Service erlaubt, wie nachfolgend gezeigt.

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

Sie können der Cluster-Rolle eine Richtlinie hinzufügen, die den COPY- und UNLOAD-Zugriff auf einen bestimmten Bucket COPY verhindert. Die folgende Richtlinie gestattet Datenverkehr zu dem angegebenen Bucket nur von 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"}}
    }]
}
```

Weitere Informationen finden Sie unter IAM-Richtlinien für Redshift Spectrum im Datenbankentwicklerhandbuch zu Amazon Redshift.

Protokollieren und Prüfen des Amazon-S3-Zugriffs

Ein Vorteil der Verwendung von Enhanced VPC Routing für Amazon Redshift ist, dass der gesamte COPY- und UNLOAD-Datenverkehr in den VPC-Flow-Protokollen protokolliert wird. Von Redshift

Spectrum stammender Datenverkehr zu Amazon S3 wird nicht durch Ihre VPC geleitet und wird daher auch nicht in den VPC-Flow-Protokollen aufgezeichnet. Wenn Redshift Spectrum auf Daten in Amazon S3 zugreift, führt es diese Vorgänge im Kontext des AWS Kontos und der jeweiligen Rollenrechte aus. Sie können den Amazon-S3-Zugriff mithilfe von Serverzugriffsprotokollierung in AWS CloudTrail und Amazon S3 protokollieren und prüfen.

Stellen Sie sicher, dass die S3-IP-Bereiche zu Ihrer Zulassungsliste hinzugefügt werden. Weitere Informationen zu den erforderlichen S3-IP-Bereichen finden Sie unter Netzwerkisolierung.

AWS CloudTrail Protokolle

Um den gesamten Zugriff auf Objekte in Amazon S3, einschließlich des Redshift Spectrum-Zugriffs, nachzuverfolgen, aktivieren CloudTrail Sie die Protokollierung für Amazon S3 S3-Objekte.

Sie können CloudTrail damit Kontoaktivitäten in Ihrer gesamten AWS Infrastruktur anzeigen, suchen, herunterladen, archivieren, analysieren und darauf reagieren. Weitere Informationen finden Sie unter Erste Schritte mit CloudTrail.

Verfolgt standardmäßig nur CloudTrail Aktionen auf Bucket-Ebene. Um Aktionen auf Objektebene (z. B. `GetObject`) zu verfolgen, aktivieren Sie Daten- und Verwaltungsereignisse für jeden protokollierten Bucket.

Amazon-S3-Server-Zugriffsprotokollierung

Die Server-Zugriffsprotokollierung bietet detaillierte Aufzeichnungen über die Anforderungen, die an einen Bucket gestellt wurden. Die Zugriffsprotokollinformationen können für Sicherheits- und Zugriffsüberprüfungen nützlich sein. Weitere Informationen finden Sie unter So aktivieren Sie die Server-Zugriffsprotokollierung im Benutzerhandbuch zu Amazon Simple Storage Service.

Weitere Informationen finden Sie im AWS Sicherheits-Blogbeitrag How to Use Bucket Policies and Apply Defense-in-Depth to Help Help Your Amazon S3 S3-Daten.

Zugang zu AWS Glue oder Amazon Athena

Redshift Spectrum greift auf Ihren Datenkatalog in AWS Glue oder Athena zu. Eine weitere Option ist die Verwendung eines speziellen Hive-Metastores für Ihren Datenkatalog.

Um den Zugriff auf AWS Glue oder Athena zu aktivieren, konfigurieren Sie Ihre VPC mit einem Internet-Gateway oder NAT-Gateway. Konfigurieren Sie Ihre VPC-Sicherheitsgruppen so, dass ausgehender Datenverkehr zu den öffentlichen Endpunkten für AWS Glue und Athena zugelassen wird. Alternativ können Sie einen VPC-Schnittstellen-Endpunkt konfigurieren, für den AWS Glue

Zugriff auf Ihren AWS Glue Data Catalog. Wenn Sie einen VPC-Schnittstellenendpunkt verwenden, AWS Glue erfolgt die Kommunikation zwischen Ihrer VPC und innerhalb des AWS Netzwerks. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts.

Sie können in Ihrer VPC die folgenden Pfade konfigurieren:

- Internet-Gateway — Um eine Verbindung zu AWS Diensten außerhalb Ihrer VPC herzustellen, können Sie ein Internet-Gateway an Ihr VPC-Subnetz anschließen, wie im Amazon VPC-Benutzerhandbuch beschrieben. Zur Verwendung eines Internet-Gateways muss Ihr Cluster eine öffentliche IP-Adresse haben, damit andere Services mit dem Cluster kommunizieren können.
- NAT-Gateway — Um eine Verbindung zu einem Amazon S3 S3-Bucket in einer anderen AWS Region oder zu einem anderen Service innerhalb des AWS Netzwerks herzustellen, konfigurieren Sie ein Network Address Translation (NAT) -Gateway, wie im Amazon VPC-Benutzerhandbuch beschrieben. Sie können mit dieser Konfiguration auch auf eine Host-Instance außerhalb des AWS -Netzwerks zugreifen.

Weitere Informationen finden Sie unter Enhanced VPC Routing in Amazon Redshift.

Überwachen der Amazon-Redshift-Cluster-Leistung

Amazon Redshift stellt Leistungsmetriken und Daten bereit, mit denen Sie den Zustand und die Leistung Ihrer Cluster und Datenbanken überwachen können. In diesem Abschnitt werden die Arten von Daten behandelt, mit denen Sie in Amazon Redshift arbeiten können, insbesondere in der Amazon-Redshift-Konsole.

Themen

- Übersicht
- Überwachung von Amazon Redshift mithilfe von Metriken CloudWatch
- Arbeiten mit Leistungsdaten in der Amazon-Redshift-Konsole

Übersicht

Die Leistungsdaten, die Sie in der Amazon-Redshift-Konsole verwenden können, fallen in zwei Kategorien:

- CloudWatch Amazon-Metriken — Mit CloudWatch Amazon-Metriken können Sie physische Aspekte Ihres Clusters überwachen, z. B. CPU-Auslastung, Latenz und Durchsatz. Metrikdaten werden direkt in der Amazon-Redshift-Konsole angezeigt. Sie können es sich auch in der CloudWatch Konsole ansehen. Alternativ können Sie es auf jede andere Art und Weise nutzen, wie Sie mit Metriken arbeiten, z. B. mit dem AWS CLI oder einem der AWS SDKs.
- Daten zur Abfrage-/Ladeleistung: Diese Leistungsdaten helfen Ihnen bei der Überwachung der Datenbankaktivität und -leistung. Diese Daten werden in der Amazon Redshift Redshift-Konsole aggregiert, sodass Sie das, was Sie in den CloudWatch Metriken sehen, auf einfache Weise mit bestimmten Datenbankabfrage- und Ladeereignissen korrelieren können. Sie können auch Ihre Eigenen benutzerdefinierten Leistungsabfragen erstellen und direkt auf der Datenbank ausführen. Abfrage- und Ladeleistungsdaten werden nur in der Amazon-Redshift-Konsole angezeigt. Sie werden nicht als Metriken veröffentlicht. CloudWatch

Leistungsdaten sind in die Amazon-Redshift-Konsole integriert, was das Arbeiten damit aus mehreren Gründen komfortabler macht:

- Mit einem Cluster verbundene Leistungsdaten werden im Kontext präsentiert, wenn Sie einen Cluster anzeigen und Sie diese Daten brauchen können, um Entscheidungen zu dem Cluster zu treffen, etwa über eine Größenanpassung.
- Einige Leistungskennzahlen werden in der Amazon Redshift Redshift-Konsole in besser skalierten Einheiten angezeigt als CloudWatch Beispielsweise wird in GB/s (im Vergleich zu Bytes/s in CloudWatch) angezeigt, was für den typischen Speicherplatz eines Knotens eine relevantere Einheit ist. `WriteThroughput`
- Sie können die Leistungsdaten für die Knoten eines Clusters problemlos gemeinsam in einer Grafik darstellen. Auf diese Weise können Sie die Leistung aller Knoten eines Clusters problemlos überwachen. Sie können die Leistungsdaten auch für jeden einzelnen Knoten anzeigen.

Amazon Redshift stellt Leistungsdaten (sowohl CloudWatch Metriken als auch Abfrage- und Ladedaten) ohne zusätzliche Kosten bereit. Leistungsdaten werden im Minutentakt aufgezeichnet. Sie können in der Amazon-Redshift-Konsole auf die historischen Werte der Leistungsdaten zugreifen. Ausführliche Informationen zur Verwendung des Zugriffs CloudWatch auf die Amazon Redshift Redshift-Leistungsdaten, die als CloudWatch Metriken bereitgestellt werden, finden Sie unter Was ist CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

Überwachung von Amazon Redshift mithilfe von Metriken CloudWatch

Mithilfe von CloudWatch Metriken für Amazon Redshift können Sie Informationen über den Zustand und die Leistung Ihres Clusters abrufen und Informationen auf Knotenebene einsehen. Bei der Arbeit mit diesen Metriken sollten Sie beachten, dass zu jeder Metrik eine oder mehrere Dimensionen gehören. Diese Dimensionen stellen Ihnen Informationen dazu bereit, worauf die Metrik angewendet werden kann, d. h. zum Geltungsumfang der Metrik. Amazon Redshift umfasst die folgenden beiden Dimensionen:

- Metriken mit einer `NodeID`-Dimension bieten Leistungsdaten für die Knoten eines Clusters. Diese Gruppe von Metriken umfasst Leader- und die Datenverarbeitungsknoten. Beispiele für diese Metriken sind etwa `CPUUtilization`, `ReadIOPS`, `WriteIOPS`.
- Metriken nur mit einer `ClusterIdentifier`-Dimension bieten Leistungsdaten für Cluster. Beispiele für diese Metriken sind etwa `HealthStatus` und `MaintenanceMode`.

> **Note**
>
> In einigen Fällen repräsentieren clusterspezifische Metriken eine Aggregierung des Knotenverhaltens. Interpretieren Sie diese Metrikwerte in diesen Fällen mit Vorsicht, da das Verhalten des Leader-Knotens mit dem des Datenverarbeitungsknotens aggregiert ist.

Allgemeine Informationen zu CloudWatch Metriken und Dimensionen finden Sie unter CloudWatch Konzepte im CloudWatch Amazon-Benutzerhandbuch.

Eine weitere Beschreibung der CloudWatch Metriken für Amazon Redshift finden Sie in den folgenden Abschnitten.

Themen

- Amazon-Redshift-Metriken
- Dimensionen für Amazon Redshift-Metriken
- Abfrage- und Ladeleistungsdaten von Amazon Redshift

Amazon-Redshift-Metriken

Der `AWS/Redshift`-Namespace enthält die folgenden Metriken. Sofern nicht anders angegeben, werden Metriken in 1-Minuten-Intervallen erfasst.

Title

Metrik	Beschreibung
`CommitQueueLength`	Die Anzahl der Transaktionen, die zu einem bestimmten Zeitpunkt darauf warten, einen Commit durchzuführen. Einheiten: Anzahl Maße: `ClusterIdentifier`
`ConcurrencyScaling ActiveClusters`	Die Anzahl der Nebenläufigkeitsskalierungs-Cluster, die zu einem gegebenen Zeitpunkt aktiv Abfragen verarbeiten. Einheiten: Anzahl

Metrik	Beschreibung
	Maße: `ClusterIdentifier`
`ConcurrencyScaling Seconds`	Die von Nebenläufigkeitsskalierungs-Clustern, die aktiv Abfragen verarbeiten, genutzten Sekunden. Einheiten: Anzahl Maße: `ClusterIdentifier`
`CPUUtilization`	Prozentsatz der CPU-Auslastung. Für Cluster stellt diese Metrik eine Aggregierung der CPU-Auslastungswerte aller Knoten (Leader- und Datenverarbeitungsknoten) dar. Einheiten: Prozent Maße: `ClusterIdentifier` , `NodeID` Maße: `ClusterIdentifier`
`DatabaseConnections`	Die Anzahl der Datenbankverbindungen zu einem Cluster. Einheiten: Anzahl Maße: `ClusterIdentifier`

Metrik	Beschreibung
`HealthStatus`	Zeigt den Status des Clusters an. Der Cluster stellt jede Minute eine Verbindung zu seiner Datenbank her und führt eine einfache Abfrage aus. Kann dieser Vorgang erfolgreich ausgeführt werden, wird der Cluster als fehlerfrei eingestuft. Andernfalls ist der Cluster fehlerhaft. Ein fehlerhafter Status kann auftreten, wenn die Auslastung der Cluster-Datenbank sehr hoch ist, oder falls ein Konfigurationsproblem mit einer Datenbank auf dem Cluster vorliegt. **Note** In Amazon wird diese Metrik als 1 oder 0 gemeldet CloudWatch, wohingegen diese Metrik in der Amazon Redshift Redshift-Konsole der Einfachheit `UNHEALTHY` halber mit den Worten `HEALTHY` oder angezeigt wird. Wenn diese Metrik in der Amazon-Redshift-Konsole angezeigt wird, werden Sampling-Durchschnittswerte ignoriert und es wird nur `HEALTHY` oder `UNHEALTHY` angezeigt. Bei Amazon CloudWatch können aufgrund eines Stichprobenproblems andere Werte als 1 und 0 auftreten. Jeder Wert unter 1 für `HealthStatus` wird als 0 (`UNHEALTHY`) berichtet. Einheiten: Anzahl (1/0) (`HEALTHY`/`UNHEALTHY` in der Amazon-Redshift-Konsole) Maße: `ClusterIdentifier`

Metrik	Beschreibung
`MaintenanceMode`	Gibt an, ob sich der Cluster im Wartungsmodus befindet. **Note** In Amazon wird diese Metrik als 1 oder 0 gemeldet CloudWatch, wohingegen diese Metrik in der Amazon Redshift Redshift-Konsole der Einfachheit `OFF` halber mit den Worten `ON` oder angezeigt wird. Wenn diese Metrik in der Amazon-Redshift-Konsole angezeigt wird, werden Sampling-Durchschnittswerte ignoriert und es wird nur `ON` oder `OFF` angezeigt. Bei Amazon CloudWatch können aufgrund von Stichprobenproblemen andere Werte als 1 und 0 auftreten. Jeder Wert größer als 0 für `MaintenanceMode` wird als 1 (`ON`) berichtet. Einheiten: Anzahl (1/0) (`ON`/`OFF` in der Amazon-Redshift-Konsole). Maße: `ClusterIdentifier`
`MaxConfiguredConcurrencyScalingClusters`	Maximale Anzahl der Nebenläufigkeitsskalierungs-Cluster; von der Parametergruppe konfiguriert. Weitere Informationen finden Sie unter Amazon-Redshift-Parametergruppen. Einheiten: Anzahl Maße: `ClusterIdentifier`
`NetworkReceiveThroughput`	Die Rate, mit der der Knoten bzw. der Cluster Daten empfängt. Einheiten: Byte/Sekunde (MB/s in der Amazon-Redshift-Konsole) Maße: `ClusterIdentifier` , `NodeID` Maße: `ClusterIdentifier`

Metrik	Beschreibung
NetworkTransmitThroughput	Die Rate, mit der der Knoten bzw. der Cluster Daten schreibt. Einheiten: Byte/Sekunde (MB/s in der Amazon-Redshift-Konsole) Maße: ClusterIdentifier , NodeID Maße: ClusterIdentifier
PercentageDiskSpaceUsed	Der prozentuale Anteil des verwendeten Speicherplatzes. Einheiten: Prozent Maße: ClusterIdentifier Maße: ClusterIdentifier , NodeID
QueriesCompletedPerSecond	Durchschnittliche Anzahl der ausgeführten Abfragen pro Sekunde. Wird in 5-Minuten-Intervallen gemeldet. Diese Metrik wird auf Clustern mit einem Knoten nicht unterstützt. Einheiten: Anzahl/Sekunde Maße: ClusterIdentifier , latency Maße: ClusterIdentifier , wlmid
QueryDuration	Die durchschnittliche Zeit, die es dauert, bis eine Abfrage ausgeführt wurde. Wird in 5-Minuten-Intervallen gemeldet. Diese Metrik wird auf Clustern mit einem Knoten nicht unterstützt. Einheiten: Mikrosekunden Dimensionen: ClusterIdentifier , NodeID, latency Maße: ClusterIdentifier , latency Dimensionen: ClusterIdentifier , NodeID, wlmid

Metrik	Beschreibung
QueryRuntimeBreakdown	Die Gesamtzeit; die Abfragen in der Abfragestufe verbracht haben. Wird in 5-Minuten-Intervallen gemeldet. Einheiten: Millisekunden Abmessungen: ClusterIdentifier, NodeID, Stage Abmessungen: ClusterIdentifier, Bühne
ReadIOPS	Durchschnittliche Anzahl der Lesevorgänge pro Sekunde. Einheiten: Anzahl/Sekunde Maße: `ClusterIdentifier` , `NodeID` Maße: `ClusterIdentifier`
ReadLatency	Die durchschnittliche Dauer für I/O-Lesevorgänge. Einheiten: Sekunden Maße: `ClusterIdentifier` , `NodeID` Maße: `ClusterIdentifier`
ReadThroughput	Die durchschnittliche Anzahl Byte, die pro Sekunde vom Datenträger gelesen werden. Einheiten: Byte (GB/s in der Amazon-Redshift-Konsole) Maße: `ClusterIdentifier` , `NodeID` Maße: `ClusterIdentifier`
RedshiftManagedStorageTotalCapacity	Gesamte verwaltete Speicherkapazität Einheiten: Megabyte Maße: `ClusterIdentifier`

Metrik	Beschreibung
`TotalTableCount`	Die Anzahl der zu einem bestimmten Zeitpunkt geöffneten Benutzertabellen. Diese Summe enthält keine Amazon-Redshift-Spectrum-Tabellen. Einheiten: Anzahl Maße: `ClusterIdentifier`
`WLMQueueLength`	Die Anzahl der Abfragen, die auf die Aufnahme, in eine Workload-Management-Warteschlange (WLM-Queue) aufgenommen zu werden, warten. Einheiten: Anzahl Maße: `ClusterIdentifier` , `service class` Maße: `ClusterIdentifier` , `QueueName`
`WLMQueueWaitTime`	Für das Warten in einer WLM-Warteschlange (Workload Management) aufgewendete Gesamtzeit. Wird in 5-Minuten-Intervallen gemeldet. Einheiten: Millisekunden Maße: `ClusterIdentifier` , `QueryPriority` Maße: `ClusterIdentifier` , `wlmid` Maße: `ClusterIdentifier` , `QueueName`

Metrik	Beschreibung
`WLMQueriesCompletedPerSecond`	Die durchschnittliche Anzahl der ausgeführten Abfragen pro Sekunde für eine Workload Management (WLM)-Warteschlange. Wird in 5-Minuten-Intervallen gemeldet. Diese Metrik wird auf Clustern mit einem Knoten nicht unterstützt. Einheiten: Anzahl/Sekunde Maße: `ClusterIdentifier` , `wlmid` Maße: `ClusterIdentifier` , `QueueName`
`WLMQueryDuration`	Die durchschnittliche Zeitdauer zum Abschließen einer Abfrage für eine Workload Management (WLM)-Warteschlange. Wird in 5-Minuten-Intervallen gemeldet. Diese Metrik wird auf Clustern mit einem Knoten nicht unterstützt. Einheiten: Mikrosekunden Maße: `ClusterIdentifier` , `wlmid` Maße: `ClusterIdentifier` , `QueueName`
`WLMRunningQueries`	Die Anzahl der Abfragen, die vom Haupt-Cluster und vom Nebenläufigkeitsskalierungs-Cluster pro WLM-Warteschlange ausgeführt werden. Einheiten: Anzahl Maße: `ClusterIdentifier` , `wlmid` Maße: `ClusterIdentifier` , `QueueName`
`WriteIOPS`	Durchschnittliche Anzahl der Schreibvorgänge pro Sekunde. Einheiten: Anzahl/Sekunde Maße: `ClusterIdentifier` , `NodeID` Maße: `ClusterIdentifier`

Metrik	Beschreibung
`WriteLatency`	Die durchschnittliche Dauer für I/O-Schreibvorgänge. Einheiten: Sekunden Maße: `ClusterIdentifier` , `NodeID` Maße: `ClusterIdentifier`
`WriteThroughput`	Die durchschnittliche Anzahl von Bytes, die pro Sekunde auf den Datenträger geschrieben werden. Einheiten: Byte (GB/s in der Amazon-Redshift-Konsole) Maße: `ClusterIdentifier` , `NodeID` Maße: `ClusterIdentifier`
`SchemaQuota`	Das konfigurierte Kontingent für ein Schema. Einheiten: Megabyte Dimensionen: `ClusterIdentifier` , `Database`, `Schema` Periodisch/Push: `Periodic` Häufigkeit: `5 minutes` Stopp-Kriterien: Schema gelöscht oder Kontingent entfernt
`NumExceededSchemaQuotas`	Die Anzahl der Schemata mit überschrittenen Kontingenten. Einheiten: Anzahl Maße: `ClusterIdentifier` Periodisch/Push: `Periodic` Häufigkeit: `5 minutes` Stopp-Kriterium: k. A.

Metrik	Beschreibung
`StorageUsed`	Der Datenträger oder Speicherplatz, der von einem Schema genutzt wird. Einheiten: Megabyte Dimensionen: `ClusterIdentifier` , `Database`, `Schema` Periodisch/Push: `Periodic` Häufigkeit: `5 minutes` Stopp-Kriterien: Schema gelöscht oder Kontingent entfernt
`PercentageQuotaUsed`	Der Prozentsatz des genutzten Datenträgers oder Speicherplatzes im Verhältnis zum konfigurierten Schemakontingent. Einheiten: Prozent Dimensionen: `ClusterIdentifier` , `Database`, `Schema` Periodisch/Push: `Periodic` Häufigkeit: `5 minutes` Stopp-Kriterien: Schema gelöscht oder Kontingent entfernt

Metrik	Beschreibung
`UsageLimitAvailable`	Gibt je nach Folgendes UsageLimitAvailable zurück: FeatureType • Wenn ja`CONCURRENCY_SCALING`, FeatureType wird die Gesamtzeit UsageLimitAvailable zurückgegeben, die für die Parallelitätsskalierung in 1-Minuten-Schritten genutzt werden kann. • Wenn ja`CROSS_REGION_DATASHARING`, FeatureType wird die Gesamtmenge der Daten UsageLimitAvailable zurückgegeben, die in Schritten von 1 TB gescannt werden können. • Wenn ja`SPECTRUM`, FeatureType wird die Gesamtmenge der Daten UsageLimitAvailable zurückgegeben, die in Schritten von 1 TB gescannt werden können. Einheiten: Minuten oder TB Dimensionen: `ClusterIdentifier`, `FeatureType`, `UsageLimitId`

Metrik	Beschreibung
`UsageLimitConsumed`	Gibt je nach FeatureType Folgendes UsageLimitConsumed zurück: • Wenn ja`CONCURRENCY_SCALING` , FeatureType wird die Gesamtzeit, die für die Parallelitätsskalierung verwendet wurde, in Schritten von 1 Minute UsageLimitAvailable zurückgegeben. • Wenn ja`CROSS_REGION_DATASHARING` , FeatureType wird die Gesamtmenge der gescannten Daten in Schritten von 1 TB UsageLimitAvailable zurückgegeben. • Wenn ja`SPECTRUM`, FeatureType wird die Gesamtmenge der gescannten Daten in Schritten von 1 TB UsageLimitAvailable zurückgegeben. Einheiten: Minuten oder TB Dimensionen: `ClusterIdentifier` , `FeatureType` , `UsageLimitId`

Dimensionen für Amazon Redshift-Metriken

Amazon-Redshift-Daten können nach einer der in der folgenden Tabelle aufgeführten Dimensionen gefiltert werden.

Dimension	Beschreibung
`latency`	Die möglichen Werte lauten wie folgt: • kurz – unter 10 Sekunden • mittel – zwischen 10 Sekunden und 10 Minuten • lang – über 10 Minuten
`NodeID`	Filtert angeforderte Daten, die für die Knoten eines Clusters spezifisch sind. `NodeID` ist entweder „Leader“, „Shared“ oder

Dimension	Beschreibung
	„Compute-N“, wobei N gleich 0, 1 ... entsprechend der Anzahl der Knoten im Cluster ist. "Shared" bedeutet, dass das Cluster nur über einen Knoten verfügt, d. h., dass der Führungs- und der Datenverarbeitungsknoten kombiniert sind. Für Leader- und Datenverarbeitungsknoten werden Metriken nur für `CPUUtilization` , `NetworkTransmitThroughput` und `ReadIOPS` berichtet. Andere Metriken, die die `NodeId`-Dimension verwenden, werden nur für Datenverarbeitungs knoten gemeldet.
`ClusterIdentifier`	Filtert angeforderte Daten, die für den Cluster spezifisch sind. Cluster-spezifische Metriken beinhalten `HealthStatus` , `MaintenanceMode` und `DatabaseConnections` . Allgemeine Metriken für diese Dimension (z. B. `ReadIOPS`), die auch Knotenmetriken sind, stellen den Gesamtwert der Knotenmetrikdaten dar. Berücksichtigen Sie bei der Interpret ation dieser Metriken den Umstand, dass sie das Gesamtver halten der Führungs- und Datenverarbeitungsknoten darstellen.
`service class`	Die ID für eine `WLM`-Service-Klasse.

Dimension	Beschreibung
`stage`	Die Ausführungsstufen einer Abfrage. Die möglichen Werte lauten wie folgt: • QueryPlanning: Zeit, die für das Parsen und Optimieren von SQL-Anweisungen aufgewendet wurde. • QueryWaiting: Wartezeit in der WLM-Warteschlange. • QueryExecutingRead: Zeit, die für die Ausführung von Leseabfragen aufgewendet wurde. • QueryExecutingInsert: Zeit, die für die Ausführung von Insert-Abfragen aufgewendet wurde. • QueryExecutingDelete: Zeit, die für die Ausführung von Löschabfragen aufgewendet wurde. • QueryExecutingUpdate: Zeitaufwand für die Ausführung von Aktualisierungsabfragen. • QueryExecutingCtas: Zeit, die für die Ausführung von Abfragen zum Erstellen von Tabellen als Abfragen aufgewend et wurde. • QueryExecutingUnload: Zeit, die für die Ausführung von Entladeabfragen aufgewendet wurde. • QueryExecutingCopy: Zeitaufwand für die Ausführung von Kopierabfragen. • QueryCommit: Zeit, die für das Festschreiben aufgewendet wurde.
`wlmid`	Der Bezeichner für eine Workload Management-Warteschlange.
`QueryPriority`	Die Priorität der Abfrage. Mögliche Werte sind `CRITICAL`, `HIGHEST`, `HIGH`, `NORMAL`, `LOW` und `LOWEST`.
`QueueName`	Der Name der Workload Management-Warteschlange.
`FeatureType`	Das Feature, das durch eine Nutzungsbeschränkung eingeschr änkt ist. Mögliche Werte sind `CONCURRENCY_SCALING` , `CROSS_REGION_DATASHARING` und `SPECTRUM`.

Dimension	Beschreibung
`UsageLimitId`	Der Bezeichner für ein Nutzungslimit.

Abfrage- und Ladeleistungsdaten von Amazon Redshift

Zusätzlich zu den CloudWatch Metriken stellt Amazon Redshift Daten zur Abfrage- und Ladeleistung bereit. Abfrage- und Lade-Leistungsdaten helfen Ihnen beim Verständnis des Verhältnis zwischen der Datenbankleistung und den Cluster-Metriken. Zum Beispiel: Wenn Sie erkennen, dass die CPU-Nutzung eines Clusters einen Spitzenwert zeigt, finden Sie diesen Wert auf dem CPU-Graph des Clusters und können die Abfragen identifizieren, die zu diesem Zeitpunkt ausgeführt wurden. Wenn Sie andererseits eine bestimmte Abfrage untersuchen, finden Sie die Metrikdaten (etwa die CPU-Nutzung) in ihrem Kontext angezeigt, so dass Sie die Auswirkungen der Abfrage auf die Cluster-Metriken verstehen können-

Abfrage- und Ladeleistungsdaten werden nicht als CloudWatch Metriken veröffentlicht und können nur in der Amazon Redshift Redshift-Konsole angezeigt werden. Abfrage- und Ladeleistungsdaten werden aus der Abfrage mit den Systemtabellen Ihrer Datenbank generiert (weitere Informationen finden Sie unter Systemtabellenreferenz im Amazon-Redshift-Entwicklerhandbuch). Sie können auch Ihre eigenen benutzerdefinierten Leistungsabfragen generieren, wir empfehlen jedoch, mit den in der Konsole präsentierten Abfrage- und Lade-Leistungsdaten zu beginnen. Weitere Informationen dazu, wie Sie die Leistung Ihrer Datenbank selbst messen und überwachen können, finden Sie unter Verwalten der Leistung im Amazon-Redshift-Entwicklerhandbuch.

Die folgende Tabelle beschreibt die verschiedenen Aspekte der Abfrage- und Ladedaten, auf die Sie in der Amazon-Redshift-Konsole zugreifen können.

Abfrage-/Ladedaten	Beschreibung
Abfragezu sammenfassung	Eine Liste der Abfragen in einem angegebenen Zeitraum. Die Liste kann nach Werten wie Abfrage-ID, Abfragelaufzeit und Status sortiert werden. Zeigen Sie diese Daten auf der Registerkarte Query monitoring (Abfrageü berwachung) der Cluster-Detailseite an.
Abfragedetails	Bietet Details zu einer bestimmten Abfrage, darunter: • Abfrageeigenschaften, wie etwa Abfrage-ID, Typ, Cluster, auf dem die Abfrage ausgeführt wurde und Laufzeit.

Abfrage-/Ladedaten	Beschreibung
	• Details wie Status der Abfrage und Zahl der Fehler. • Die ausgeführte SQL-Anweisung. • Falls verfügbar, ein Erläuterungsplan. • Cluster-Leistungsdaten während der Abfrageausführung (weitere Informationen finden Sie unter Anzeigen der Abfrageverlaufsdaten).
Lade-Zusammenfassung	Listet alle Ladevorgänge in dem angegebenen Zeitraum auf. Die Liste kann nach Werten wie Abfrage-ID, Abfragelaufzeit und Status sortiert werden. Zeigen Sie diese Daten auf der Registerkarte Query monitoring (Abfrageüberwachung) der Cluster-Detailseite an.
Lade-Details	Bietet Details zu einer bestimmten Ladeoperation, darunter: • Lade-Eigenschaften, wie etwa Abfrage-ID, Typ, Cluster, auf dem die Abfrage ausgeführt wurde und Laufzeit. • Details wie Status des Ladevorgangs und Zahl der Fehler. • Die ausgeführte SQL-Anweisung. • Eine Liste der geladenen Dateien. • Cluster-Leistungsdaten während des Ladevorgangs (weitere Informationen finden Sie unter Anzeigen der Abfrageverlaufsdaten).

Arbeiten mit Leistungsdaten in der Amazon-Redshift-Konsole

In diesem Abschnitt erfahren Sie, wie Sie Leistungsdaten in der Amazon-Redshift-Konsole anzeigen können, einschließlich Informationen zur Cluster- und Abfrageleistung. Dazu können Sie direkt in der Amazon-Redshift-Konsole Alarme zu Clustermetriken erstellen.

Wenn Sie Leistungsdaten in der Amazon-Redshift-Konsole anzeigen, tun Sie dies für einzelne Cluster. Die Leistungsdatengraphen für einen Cluster ermöglichen Ihnen den Zugriff auf Daten zur Beantwortung der häufigsten Fragen zur Leistung. Einige Leistungsdaten (siehe Überwachung von Amazon Redshift mithilfe von Metriken CloudWatch) können Sie auch verwenden, CloudWatch um Ihre Metrikdiagramme weiter anzupassen. Sie können beispielsweise längere Zeiten auswählen oder Metriken über Cluster hinweg kombinieren. Weitere Informationen zur Arbeit mit der CloudWatch Konsole finden Sie unter Arbeiten mit Leistungskennzahlen in der CloudWatch Konsole.

Im folgenden Video erfahren Sie, wie Sie Abfragen überwachen, isolieren und optimieren, indem Sie die Abfrageüberwachungsfunktionen in der Amazon-Redshift-Konsole verwenden: Query Monitoring with Amazon Redshift.

Themen

- Anzeigen von Cluster-Leistungsdaten
- Anzeigen der Abfrageverlaufsdaten
- Anzeigen von Datenbankleistungsdaten
- Anzeigen der Parallelität des Workloads und der Parallelitätsskalierungsdaten
- Anzeigen von Abfragen und Ladevorgänge
- Anzeigen von Cluster-Metriken während der Ausführung von Lade-Operationen
- Analysieren der Workload-Leistung
- Verwalten von Alarmen
- Arbeiten mit Leistungskennzahlen in der CloudWatch Konsole

Anzeigen von Cluster-Leistungsdaten

Mithilfe von Cluster-Metriken in Amazon Redshift können Sie die folgenden gängigen Leistungsaufgaben durchführen:

- Feststellung, ob die Clustermetriken in einem bestimmten Zeitraum abnorm sind und, falls dies der Fall ist, Identifizierung der Abfragen, die dafür verantwortlich sind.
- Prüfung, ob sich frühere oder aktuelle Abfragen auf die Clusterleistung auswirken. Wenn Sie eine problematische Abfrage identifizieren, können Sie Einzelheiten dazu anzeigen, einschließlich der Clusterleistung während der Ausführung der Abfrage. Diese Informationen können Ihnen dabei helfen, herauszufinden, warum die Abfrage langsam durchgeführt wurde, und was Sie tun können, um ihre Leistung zu verbessern.

So zeigen Sie Leistungsdaten an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Namen eines Clusters aus der Liste aus, um die Details zu dem Cluster aufzurufen. Die Details des Clusters werden angezeigt, u. a. einschließlich der Registerkarten Cluster performance (Cluster-Leistung),

Query monitoring (Abfrageüberwachung), Databases (Datenbanken), Datashares, Schedules (Zeitpläne), Maintenance (Wartung) und Properties (Eigenschaften).

3. Wählen Sie die Registerkarte Cluster performance (Cluster-Leistung) für Leistungsinformationen, einschließlich der folgenden, aus:

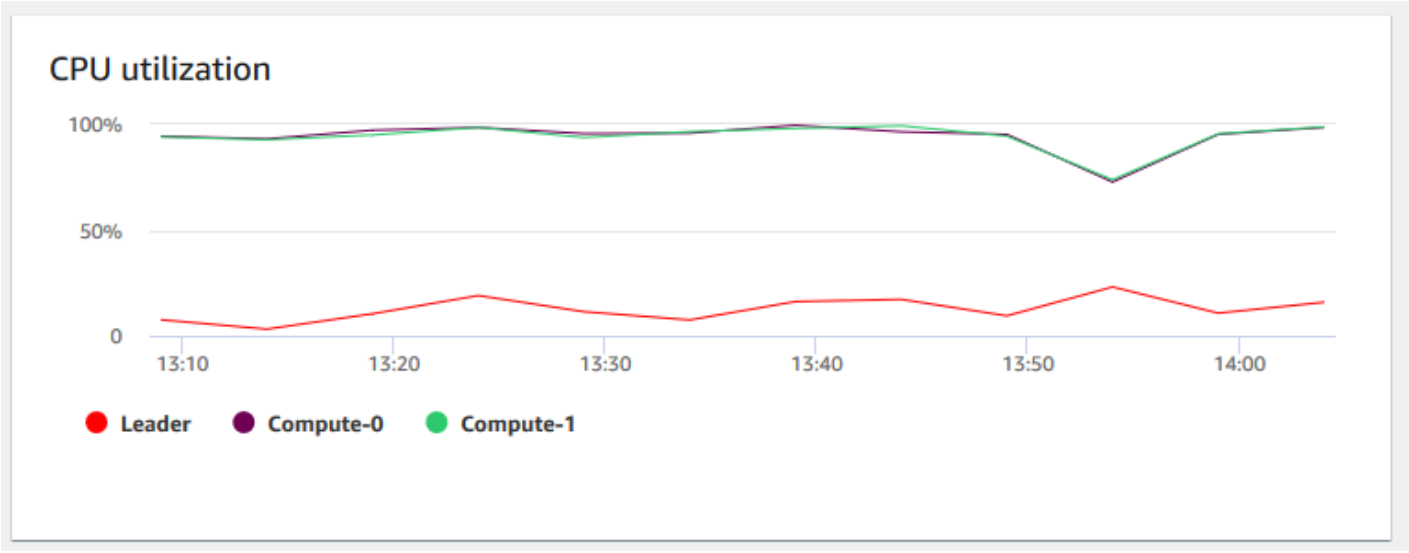
   - CPU-Nutzung
   - Percentage disk space used (Prozentualer Festplattenspeicherverbrauch)
   - Datenbankverbindungen
   - Gesundheitsstatus
   - Query duration (Abfragedauer)
   - Query throughput (Abfrage Durchsatz)
   - Concurrency scaling activity (Parallelitätsskalierungsaktivität)

   Viele weitere Metriken sind verfügbar. Um die verfügbaren Metriken anzuzeigen und die angezeigten auszuwählen, wählen Sie das Preferences (Präferenzen)-Symbol aus.

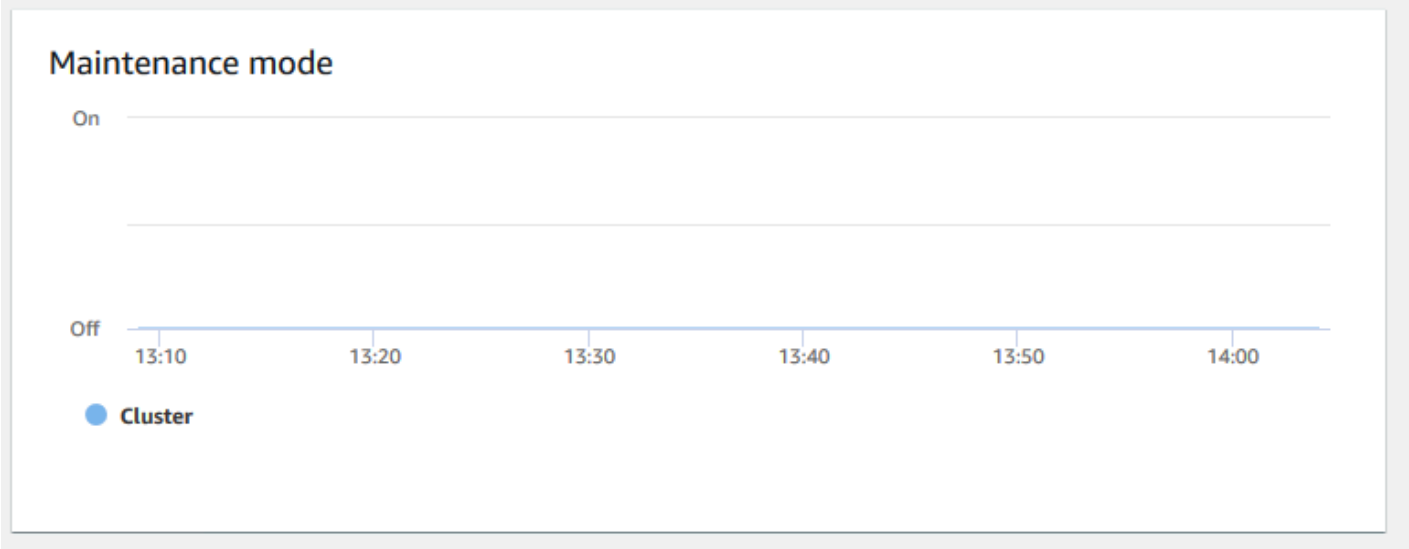
Diagramme der Clusterleistung

Im Folgenden finden Sie einige Beispiele für Diagramme, die in der neuen Amazon-Redshift-Konsole angezeigt werden.

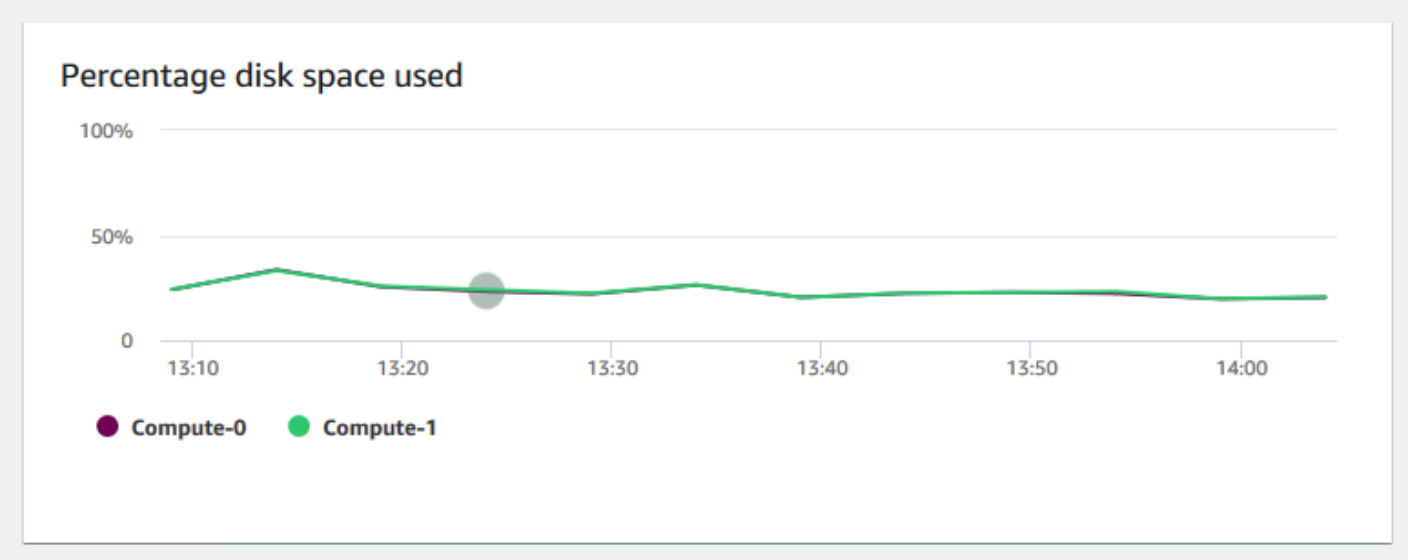
- CPU utilization (CPU-Auslastung) – zeigt den Prozentsatz der CPU-Auslastung für alle Knoten (Führungs- und Rechenknoten) an. Um einen Zeitpunkt zu ermitteln, zu dem die Clusterauslastung am niedrigsten ist, bevor die Clustermigration oder andere ressourcenaufwändige Vorgänge geplant wird, überwachen Sie dieses Diagramm, um die CPU-Auslastung pro einzelnem Knoten oder für alle Knoten anzuzeigen.



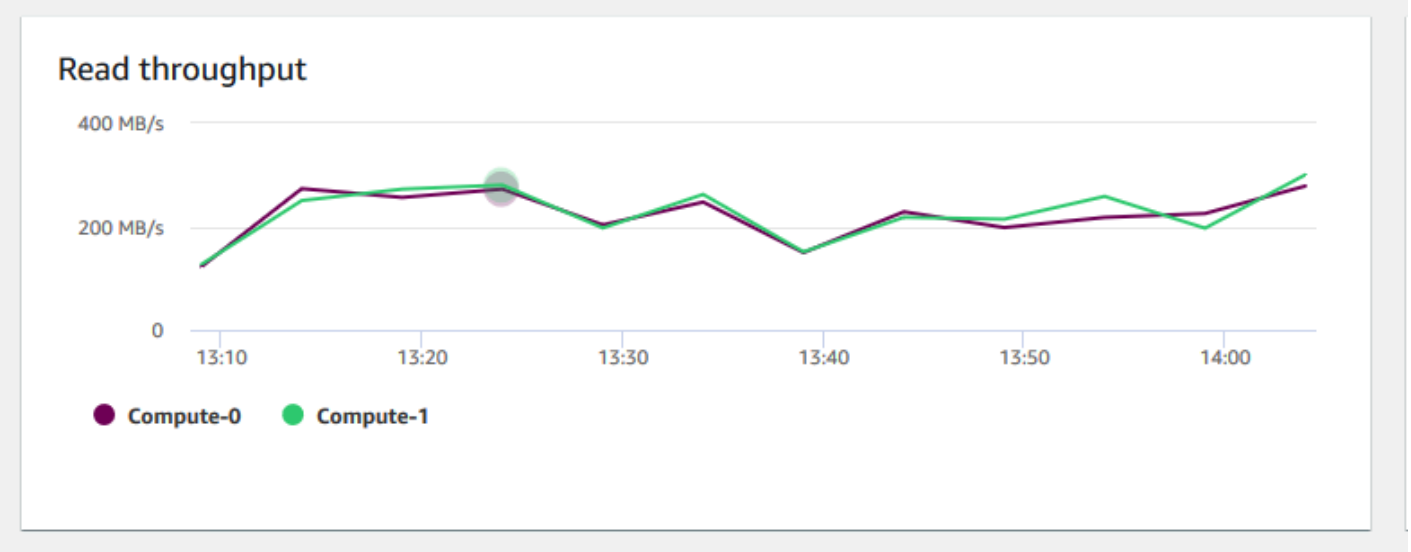
- Maintenance mode (Wartungsmodus) – zeigt mithilfe der Indikatoren `On` und `Off` an, ob sich der Cluster zu einem bestimmten Zeitpunkt im Wartungsmodus befindet. Sie können den Zeitpunkt sehen, zu dem der Cluster gewartet wird. Sie können diese Zeit dann mit Operationen korrelieren, die mit dem Cluster durchgeführt werden, um seine zukünftigen Ausfallzeiten für wiederkehrende Ereignisse abzuschätzen.



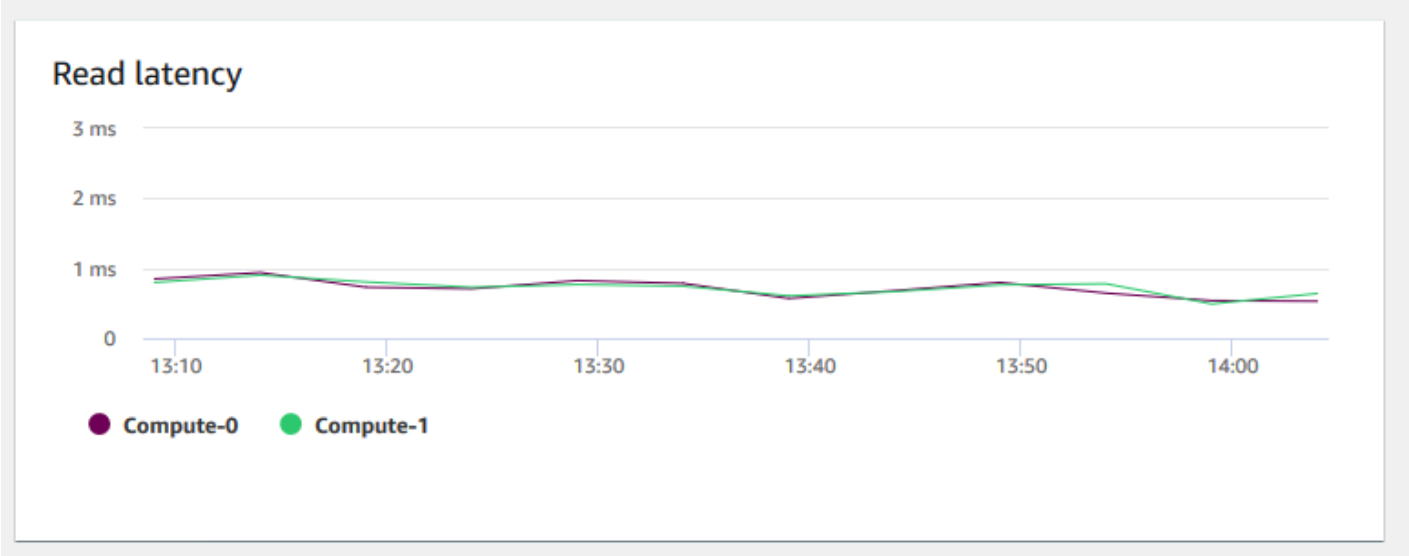
- Percentage disk space used (Prozentualer Speicherplatzverbrauch) – zeigt den Anteil des verwendeten Speicherplatzes pro Rechenknoten (nicht für den Cluster als Ganzes) an. Sie können dieses Diagramm untersuchen, um die Datenträgerauslastung zu überwachen. Wartungsvorgänge wie VACUUM und COPY verwenden temporären Zwischenspeicher für ihre Sortiervorgänge. Eine Spitze in der Datenträgernutzung ist daher zu erwarten.



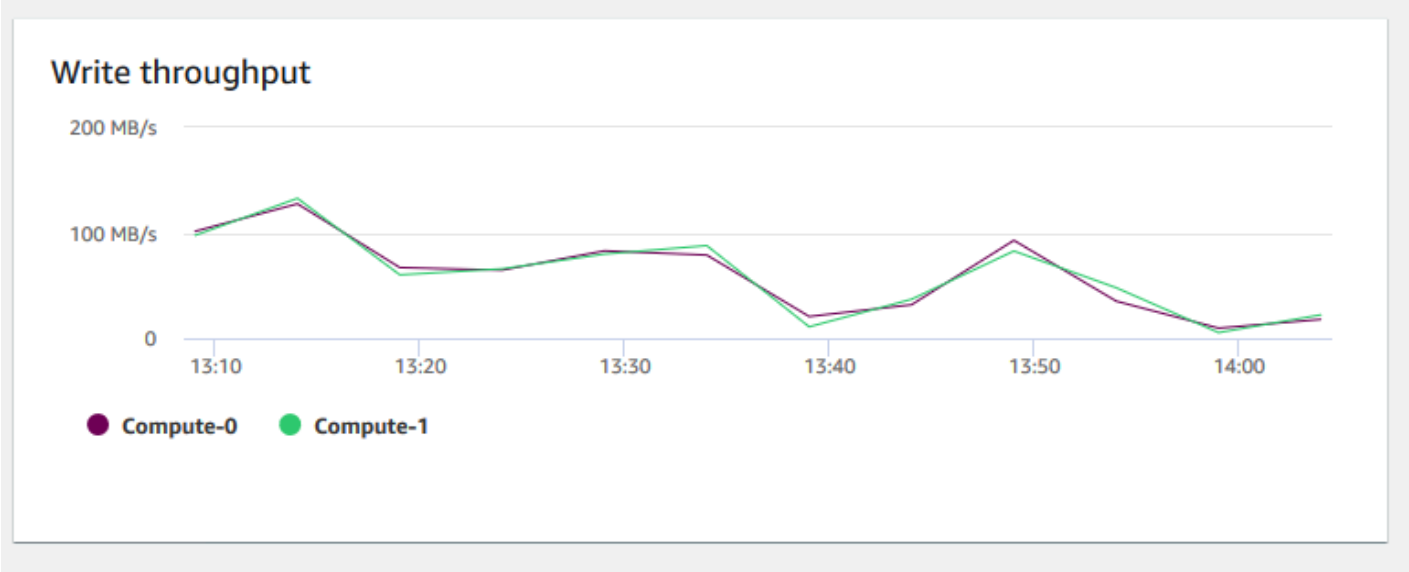
- Read throughput (Lesedurchsatz) – zeigt die durchschnittliche Zahl der Megabyte an, die pro Sekunde vom Datenträger gelesen werden. Sie können dieses Diagramm auswerten, um den entsprechenden physischen Aspekt des Clusters zu überwachen. Dieser Durchsatz beinhaltet nicht den Netzwerkdatenverkehr zwischen den Instances im Cluster und dessen Volume.



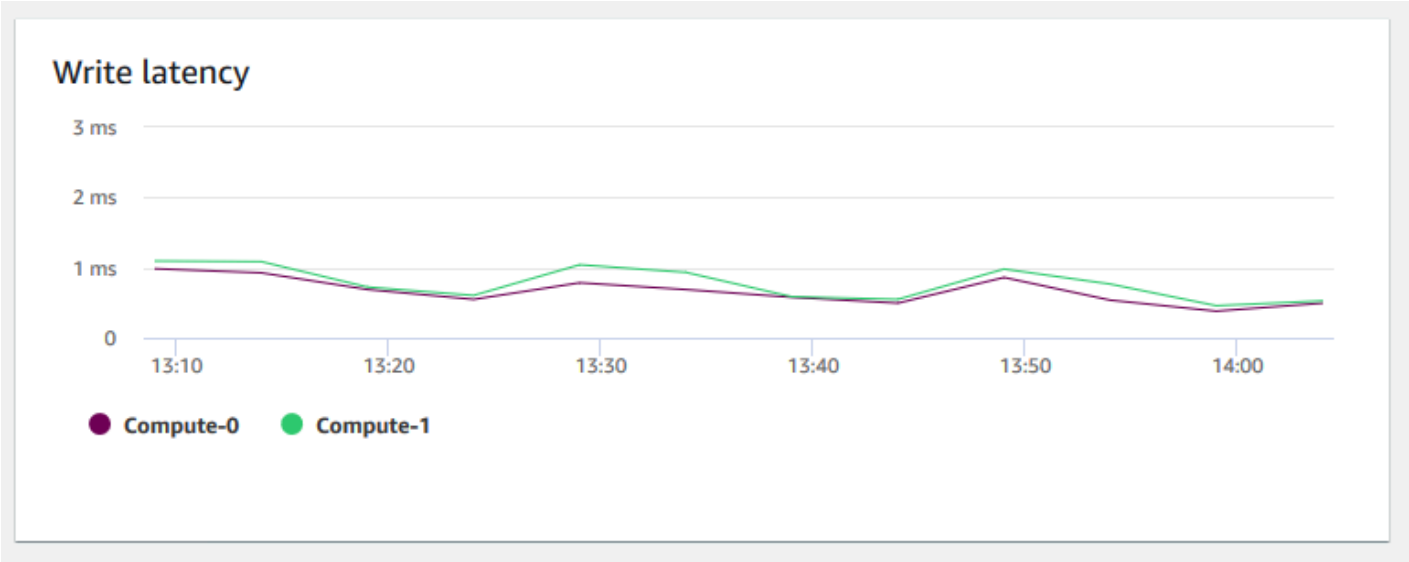
- Read latency (Leselatenz) – zeigt die durchschnittliche Zeit an, die für I/O-Lesevorgänge vom Datenträger benötigt wird (in Millisekunden). Sie können die Reaktionszeiten für die zurückzugebenden Daten anzeigen. Wenn die Latenz hoch ist, bedeutet dies, dass der Absender mehr Zeit im Leerlauf verbringt (keine neuen Pakete sendet), was Geschwindigkeit des Durchsatzanstiegs verringert.



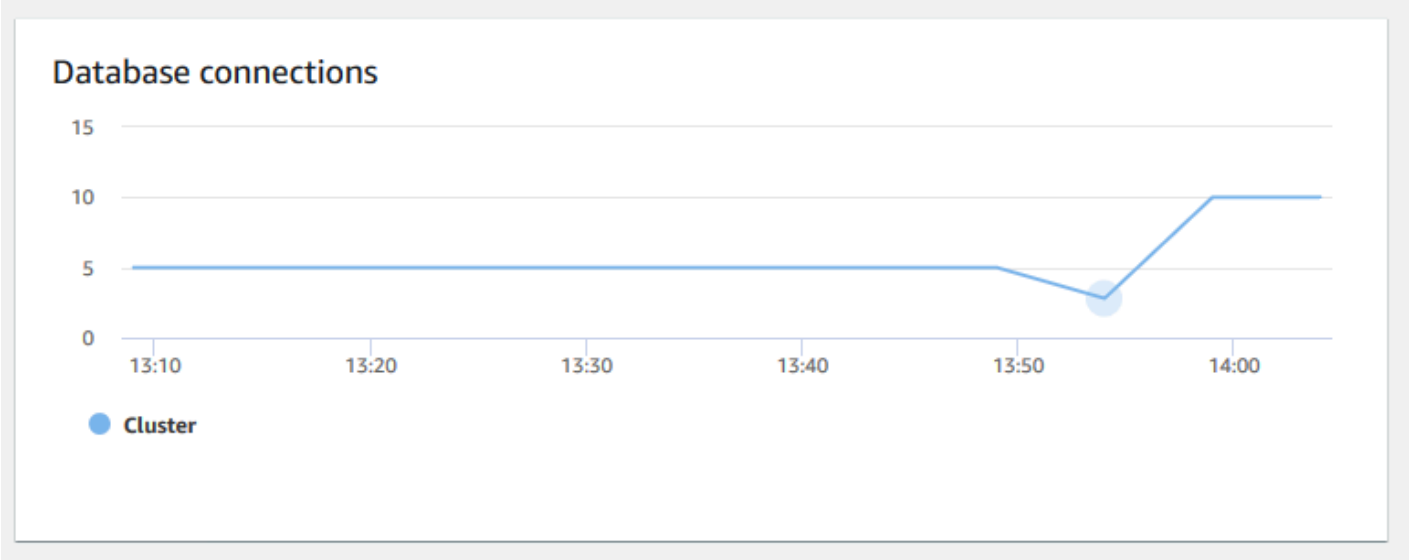
- Write throughput (Schreibdurchsatz) – zeigt die durchschnittliche Zahl der Megabyte an, die pro Sekunde auf den Datenträger geschrieben werden. Sie können diese Metrik auswerten, um den entsprechenden physischen Aspekt des Clusters zu überwachen. Dieser Durchsatz beinhaltet nicht den Netzwerkdatenverkehr zwischen den Instances im Cluster und dessen Volume.



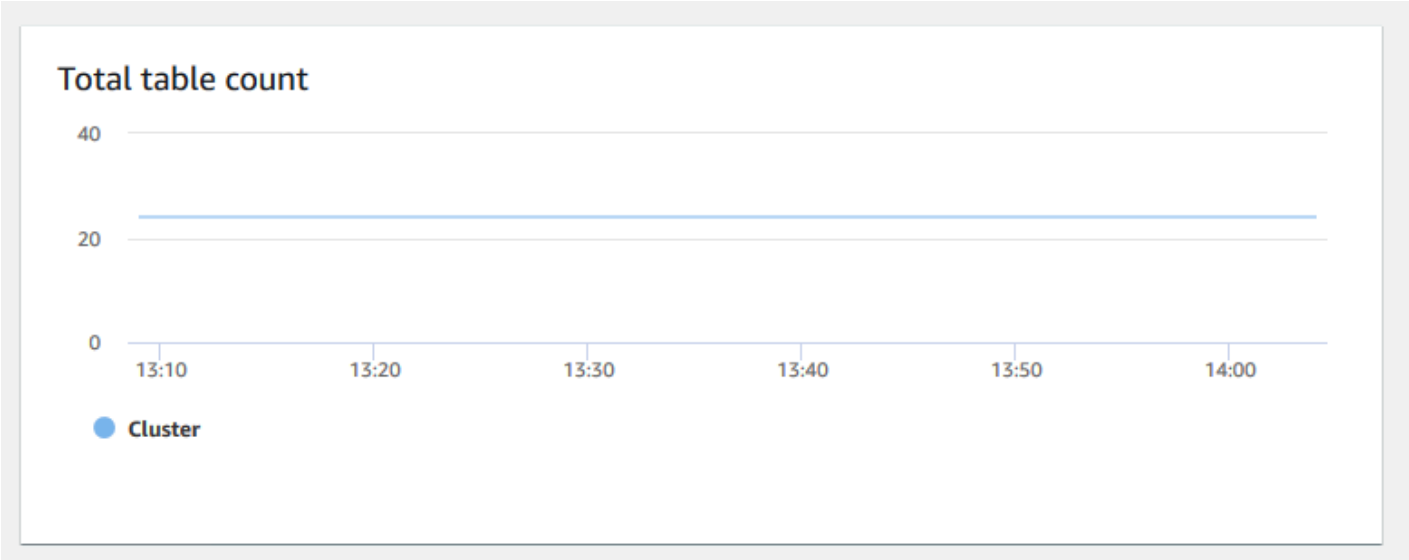
- Write latency (Schreib-Latenz) – zeigt die durchschnittliche Zeit in Millisekunden an, die für I/O-Schreibvorgänge auf dem Datenträger benötigt wird. Sie können die Zeit für die Rückgabe der Schreibbestätigung auswerten. Wenn die Latenz hoch ist, bedeutet dies, dass der Absender mehr Zeit im Leerlauf verbringt (keine neuen Pakete sendet), was Geschwindigkeit des Durchsatzanstiegs verringert.



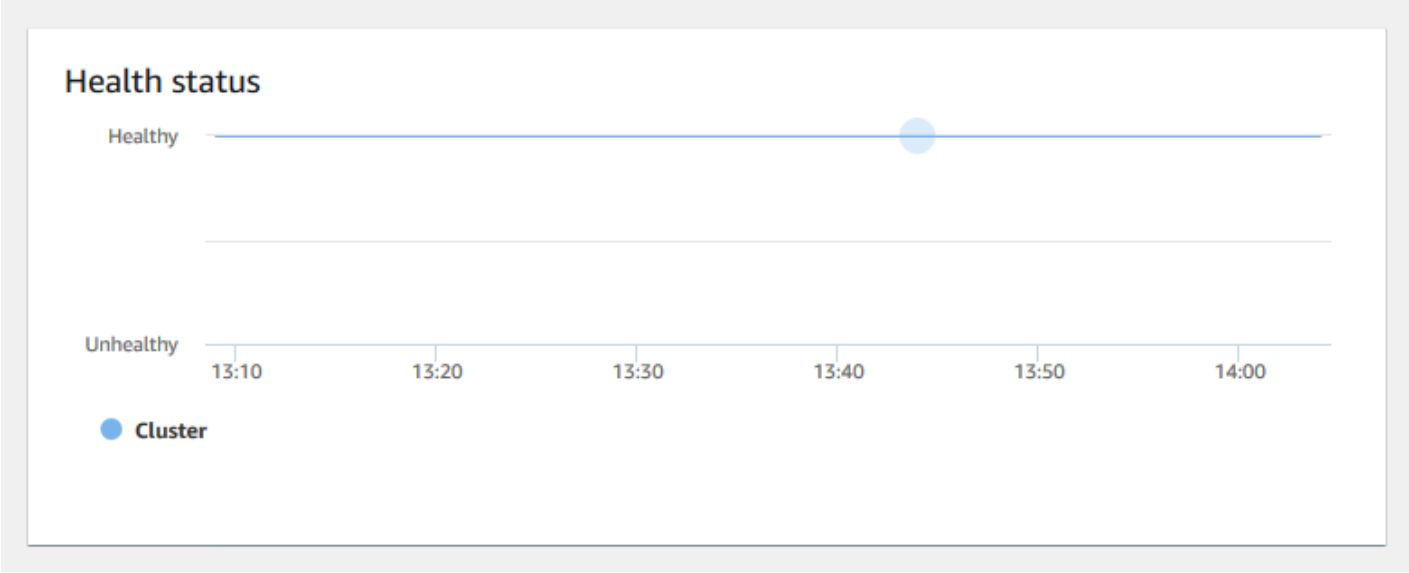
- Database connections (Datenbankverbindungen) – zeigt die Anzahl der Datenbankverbindungen zu einem Cluster an. Sie können dieses Diagramm verwenden, um zu sehen, wie viele Verbindungen mit der Datenbank hergestellt werden, und um einen Zeitpunkt zu ermitteln, zu dem die Clusterauslastung am niedrigsten ist.



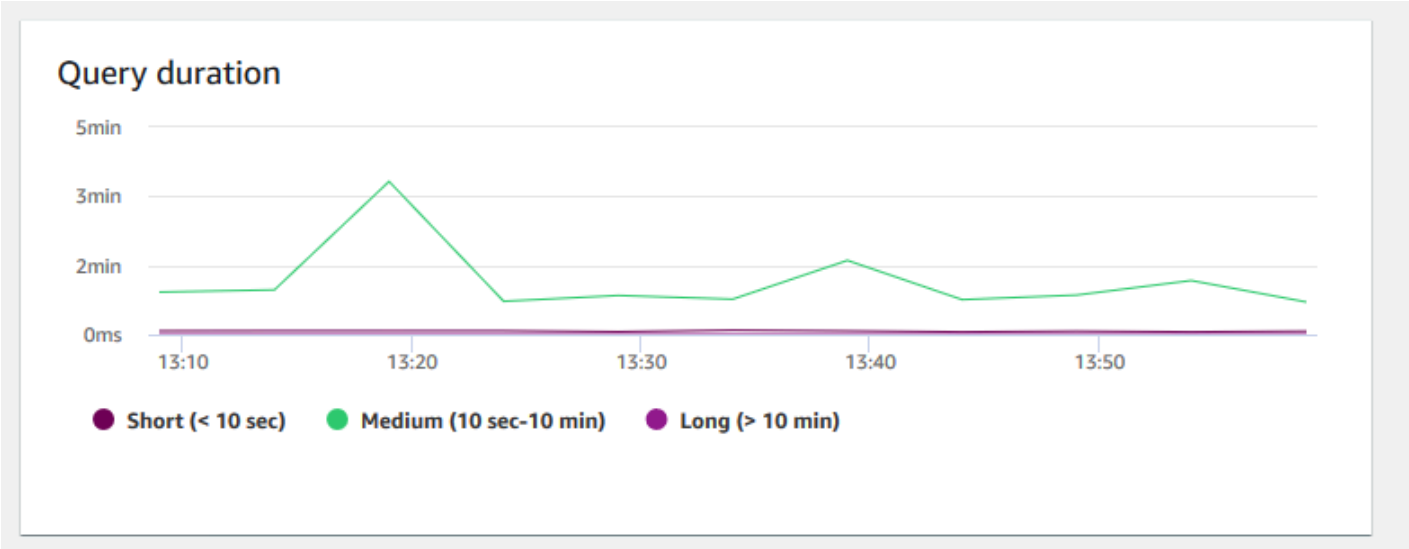
- Total table count (Gesamtanzahl der Tabellen) – zeigt die Anzahl der Benutzertabellen an, die zu einem bestimmten Zeitpunkt innerhalb eines Clusters geöffnet sind. Sie können die Clusterleistung überwachen, wenn die Anzahl geöffneter Tabellen hoch ist.



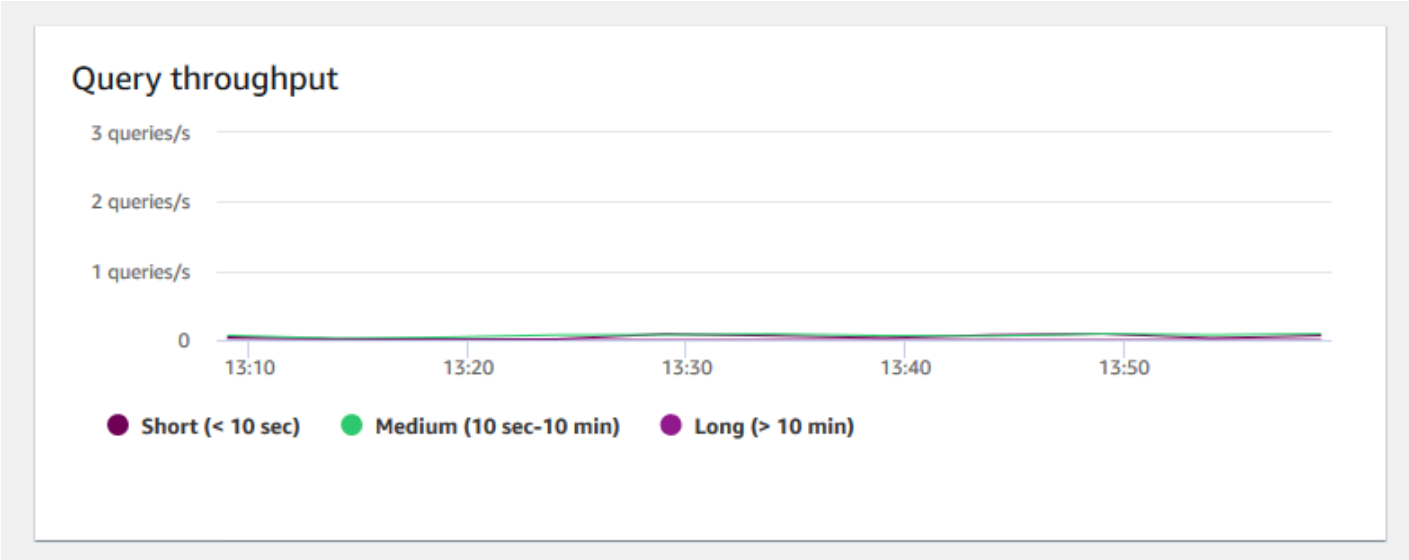
- Health status (Integritätsstatus) – zeigt den Zustand des Clusters als `Healthy` oder `Unhealthy` an. Wenn der Cluster eine Verbindung zu seiner Datenbank herstellen kann und eine einfache Abfrage erfolgreich ausführt, gilt der Cluster als fehlerfrei. Andernfalls ist der Cluster fehlerhaft. Ein fehlerhafter Status kann auftreten, wenn die Auslastung der Cluster-Datenbank sehr hoch ist, oder falls ein Konfigurationsproblem mit einer Datenbank auf dem Cluster vorliegt.



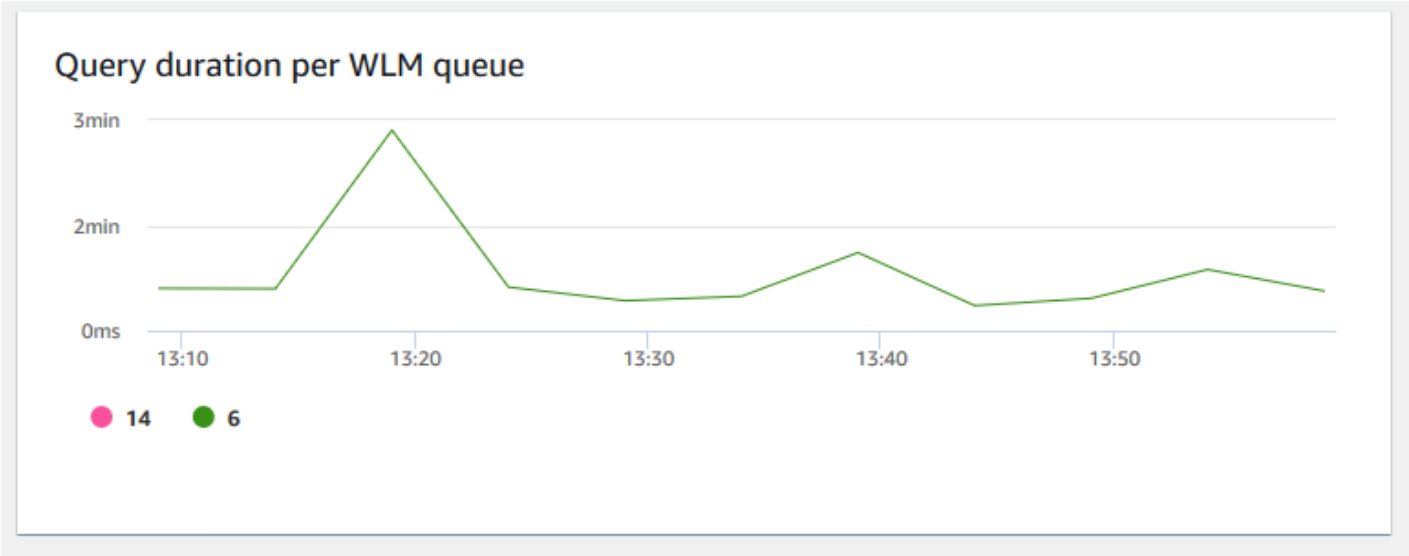
- Query duration (Abfragedauer) – zeigt die durchschnittliche Zeit für das Abschließen einer Abfrage in Mikrosekunden an. Sie können die Daten in diesem Diagramm vergleichen, um die I/O-Leistung innerhalb des Clusters zu messen und bei Bedarf die zeitaufwendigsten Abfragen zu optimieren.



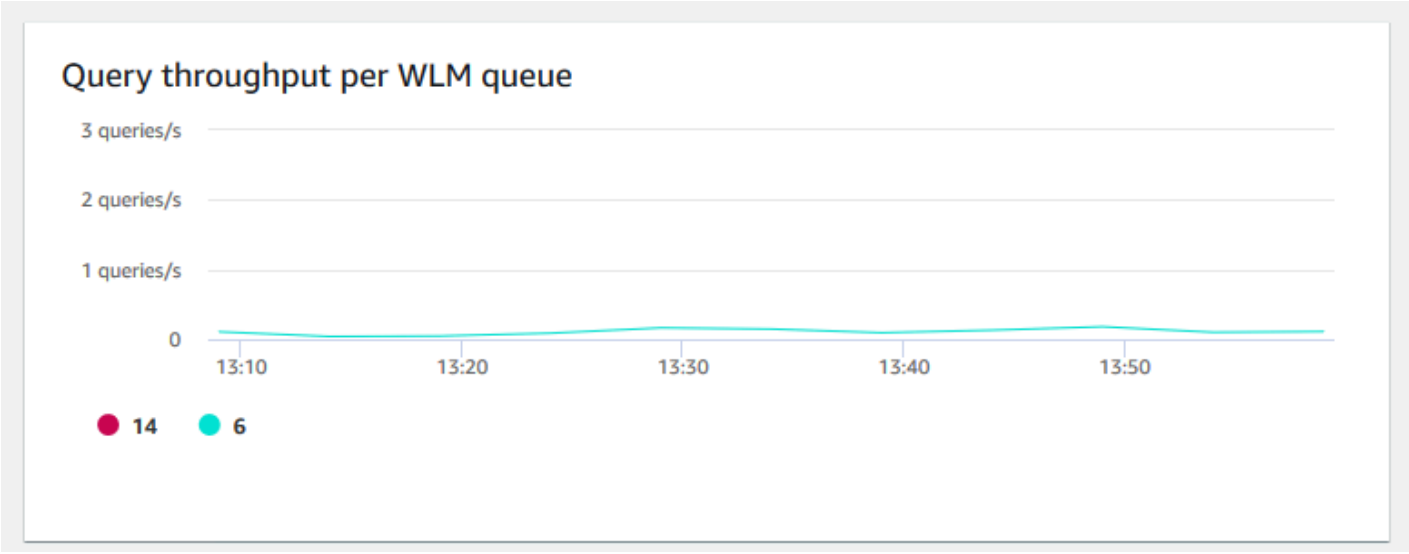
- Query throughput (Abfragedurchsatz) – zeigt die durchschnittliche Anzahl abgeschlossener Abfragen pro Sekunde an. Sie können Daten in diesem Diagramm analysieren, um die Datenbankleistung zu messen und die Fähigkeit des Systems zu charakterisieren, ein Mehrbenutzer-Workload auf ausgewogene Weise zu unterstützen.



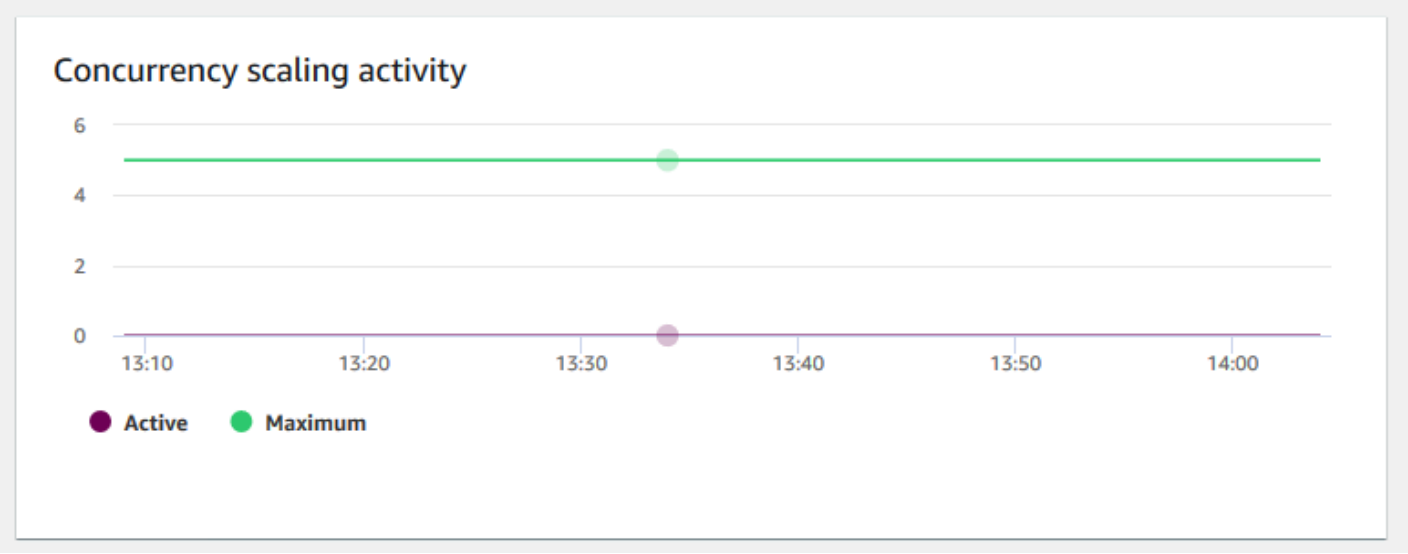
- Query duration per WLM queue (Abfragedauer pro WLM-Warteschlange) – zeigt die durchschnittliche Zeit für das Abschließen einer Abfrage in Mikrosekunden an. Sie können die Daten in diesem Diagramm vergleichen, um die I/O-Leistung pro WLM-Warteschlange zu messen und bei Bedarf die zeitaufwendigsten Abfragen zu optimieren.



- Query throughput per WLM queue (Abfragedurchsatz pro WLM-Warteschlange) – zeigt die durchschnittliche Anzahl abgeschlossener Abfragen pro Sekunde an. Sie können Daten in diesem Diagramm analysieren, um die Datenbankleistung pro WLM-Warteschlange zu messen.



- Concurrency scaling activity (Nebenläufigkeitsskalierungsaktivität) – zeigt die Anzahl der aktiven Nebenläufigkeitsskalierungs-Cluster an. Bei aktivierter Nebenläufigkeitsskalierung fügt Amazon Redshift automatisch zusätzliche Cluster-Kapazität hinzu, wenn diese benötigt wird, um eine gestiegene Zahl von gleichzeitigen Leseabfragen zu verarbeiten.



Anzeigen der Abfrageverlaufsdaten

Sie können Abfrageverlaufsmetriken in Amazon Redshift verwenden, um Folgendes zu tun:

- Isolieren und Diagnostizieren von Abfrageleistungsproblemen.
- Vergleichen Sie Abfragelaufzeitmetriken und Cluster-Leistungsmetriken auf derselben Zeitachse, um zu sehen, wie die beiden zusammenhängen könnten. Auf diese Weise können Sie Abfragen mit geringer Leistung identifizieren, Engpassabfragen finden und feststellen, ob Sie für Ihren Workload die Größe Ihres Clusters anpassen müssen.
- Zeigen Sie die Details einer bestimmten Abfrage an, indem Sie sie auf der Zeitachse auswählen. Wenn die Query ID (Abfrage-ID) und andere Eigenschaften in einer Zeile unterhalb des Diagramms angezeigt werden, können Sie die Abfrage auswählen, um Abfragedetails anzuzeigen. Zu den Details gehören zum Beispiel die SQL-Anweisung der Abfrage, Ausführungsdetails und der Abfrageplan. Weitere Informationen finden Sie unter Anzeigen von Abfragedetails.
- Stellen Sie fest, ob Ihre Ladeaufgaben erfolgreich abgeschlossen wurden, und erfüllen Sie Ihre Service Level Agreements (SLAs).

So zeigen Sie Abfrageverlaufsdaten an

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster-Namen aus der Liste aus, um die Details zu dem Cluster aufzurufen. Die Details des Clusters werden angezeigt, u. a.

einschließlich der Registerkarten Cluster performance (Cluster-Leistung), Query monitoring (Abfrageüberwachung), Databases (Datenbanken), Datashares, Schedules (Zeitpläne), Maintenance (Wartung) und Properties (Eigenschaften).

3. Wählen Sie die Registerkarte Query monitoring (Abfrageüberwachung) für Metriken zu Ihren Abfragen aus.
4. Wählen Sie im Abschnitt Query monitoring (Abfrageüberwachung) die Registerkarte Query history (Abfrageverlauf) aus.

   Mithilfe der Steuerelemente im Fenster können Sie zwischen Query list (Abfrageliste) und Cluster metrics (Cluster-Metriken) wechseln.

   Wenn Sie Query list (Abfrageliste) auswählen, enthält die Registerkarte die folgenden Diagramme:

   - Query runtime (Abfragelaufzeit) – die Abfrageaktivität auf einer Zeitachse. Mit diesem Diagramm können Sie anzeigen, welche Abfragen im selben Zeitrahmen ausgeführt werden. Wählen Sie eine Abfrage aus, um weitere Details zur Abfrageausführung anzuzeigen. Die X-Achse zeigt den ausgewählten Zeitraum an. Sie können die als Diagramm dargestellten Abfragen nach „ausgeführt“, „abgeschlossen“, „geladen“ usw. filtern. Jeder Balken stellt eine Abfrage dar, und die Länge des Balkens stellt seine Laufzeit vom Anfang des Balkens bis zum Ende dar. Die Abfragen können SQL-Datenmanipulationsanweisungen (z. B. SELECT, INSERT, DELETE) und Ladevorgänge (z. B. COPY) enthalten. Standardmäßig werden die 100 am längsten ausgeführten Abfragen für den ausgewählten Zeitraum angezeigt.
   - Queries and loads (Abfragen und Ladevorgänge) – eine Liste der Abfragen und Ladevorgänge, die auf dem Cluster ausgeführt wurden. Das Fenster enthält die Option Terminate query (Abfrage beenden), wenn gerade eine Abfrage ausgeführt wird.

   Wenn Sie Cluster metrics (Cluster-Metriken) auswählen, enthält die Registerkarte die folgenden Diagramme:

   - Query runtime (Abfragelaufzeit) – die Abfrageaktivität auf einer Zeitachse. Mit diesem Diagramm können Sie anzeigen, welche Abfragen im selben Zeitrahmen ausgeführt werden. Wählen Sie eine Abfrage aus, um weitere Details zur Abfrageausführung anzuzeigen.
   - CPU utilization (CPU-Auslastung) – die CPU-Auslastung des Clusters nach Führungsknoten und Durchschnitt der Rechenknoten.

- Storage capacity used (Verwendete Speicherkapazität) – der prozentuale Anteil der genutzten Speicherkapazität.
- Active database connections (Aktive Datenbankverbindungen) – die Anzahl aktiver Datenbankverbindungen mit dem Cluster.

Berücksichtigen Sie Folgendes, wenn Sie mit den Abfrageverlaufsdiagrammen arbeiten:

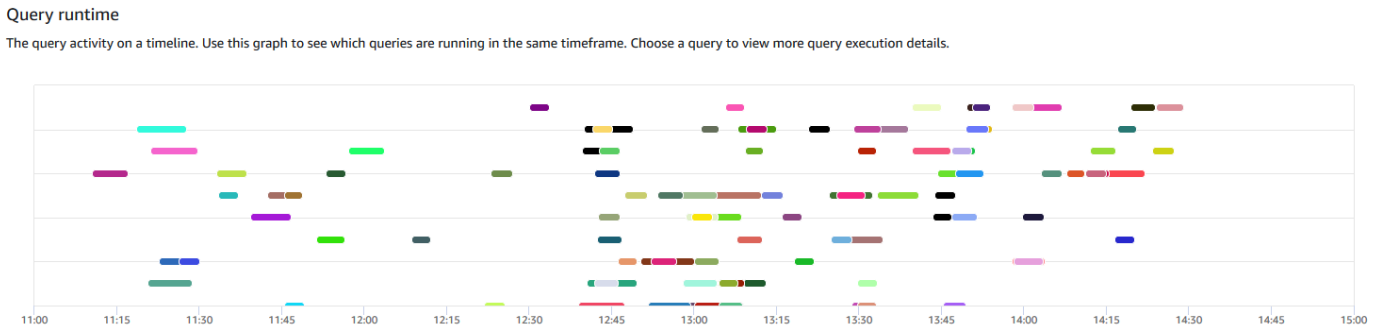
- Wählen Sie im Diagramm Query runtime (Abfrage-Laufzeit) einen Balken aus, der eine bestimmte Abfrage darstellt, um Details zu dieser Abfrage anzuzeigen. Sie können auch eine Abfrage-ID für Queries and loads (Abfragen und Ladevorgänge) auswählen, um deren Details anzuzeigen.
- Sie können wischen, um einen Abschnitt des Diagramms Query runtime (Abfragelaufzeit) auszuwählen und so die Ansicht zu vergrößern, damit ein bestimmter Zeitraum angezeigt wird.
- Damit alle Daten vom ausgewählten Filter berücksichtigt werden, blättern Sie im Diagramm Query runtime (Abfragelaufzeit) durch alle Seiten, die in der Liste „ Queries and loads (Abfragen und Ladevorgänge) aufgeführt sind.
- Sie können die Spalten und die Anzahl der Zeilen, die in der Liste Queries and loads (Abfragen und Ladevorgänge) angezeigt werden, über das Zahnradsymbol für Einstellungen ändern.
- Die Liste Queries and loads (Abfragen und Ladevorgänge) kann auch angezeigt werden, indem Sie über das linke Queries (Abfragen)-Symbol des Navigators zu Queries and loads (Abfragen und Ladevorgänge) navigieren. Weitere Informationen finden Sie unter Anzeigen von Abfragen und Ladevorgänge.

Diagramme des Abfrageverlaufs

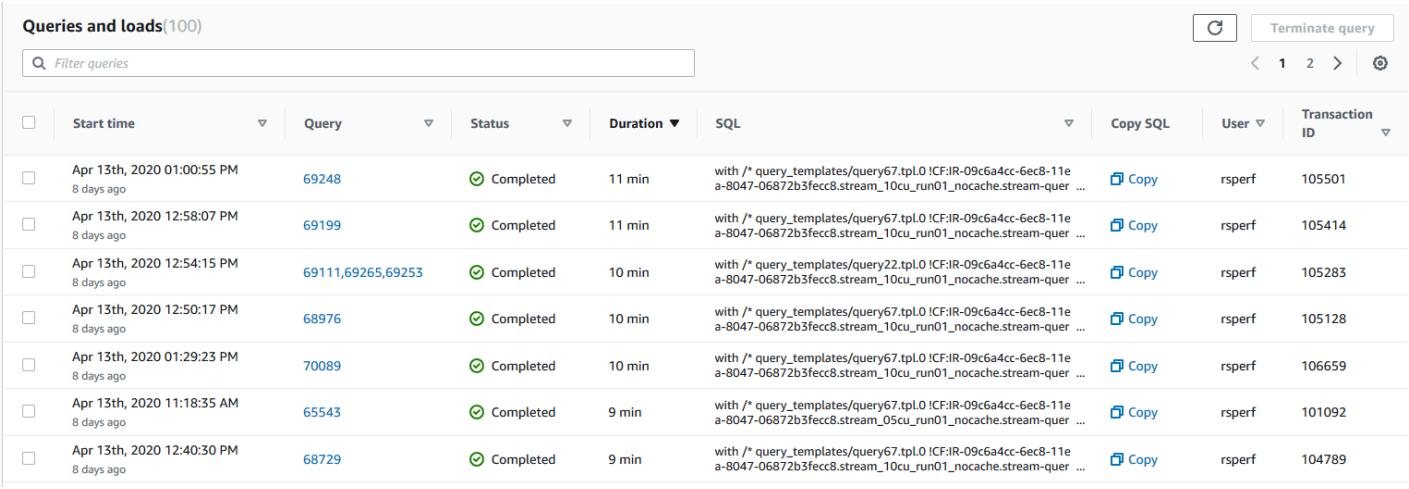
Im Folgenden finden Sie einige Beispiele für Diagramme, die in der neuen Amazon-Redshift-Konsole angezeigt werden.

> **Note**
>
> Die Diagramme in der Amazon-Redshift-Konsole enthalten nur Daten für die letzten 100 000 Abfragen.

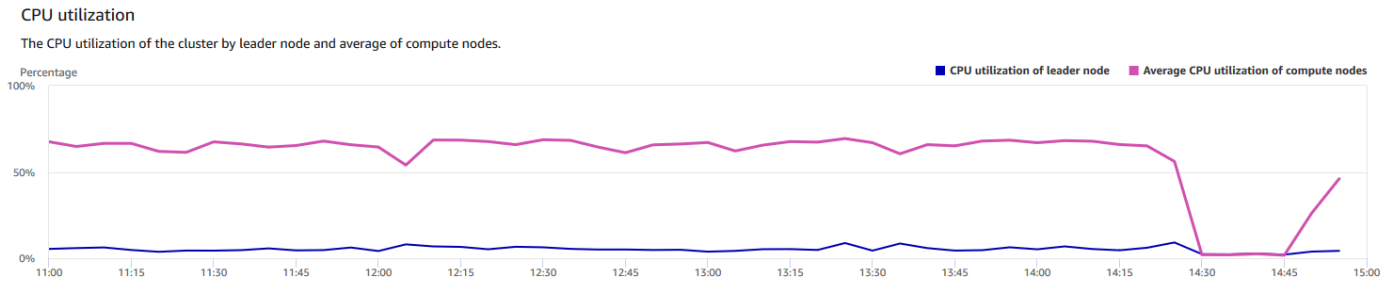
- Query runtime (Abfrage-Laufzeit)



- Queries and loads (Abfragen und Ladevorgänge)



- CPU-Nutzung



- Verwendete Speicherkapazität

- Active database connections (Aktive Datenbankverbindungen)

Anzeigen von Datenbankleistungsdaten

Sie können mit den Datenbankleistungsmetriken in Amazon Redshift Folgendes tun:

- Analysieren Sie die von Abfragen benötigte Zeit anhand von Verarbeitungsschritten. Sie können nach ungewöhnlichen Tendenzen suchen, die in der Menge der in einer Phase verbrachten Zeit auftreten.
- Sie können die Anzahl der Abfragen, die Dauer und den Durchsatz von Abfragen nach Zeitbereichen (kurz, mittel, lang) analysieren.
- Sie können nach Trends in der Menge der Abfragewartezeit nach Abfragepriorität (Niedrigste, Niedrig, Normal, Hoch, Höchste, Kritische) suchen.
- Sie können nach Trends in der Abfragedauer, dem Durchsatz oder der Wartezeit nach WLM-Warteschlange suchen.

So zeigen Sie Datenbankleistungsdaten an

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster-Namen aus der Liste aus, um die Details zu dem Cluster aufzurufen. Die Details des Clusters werden angezeigt, einschließlich der Registerkarten Cluster performance (Cluster-Leistung), Query monitoring (Abfrageüberwachung), Databases (Datenbanken), Datashares, Schedules (Zeitpläne), Maintenance (Wartung) und Properties (Eigenschaften).
3. Wählen Sie die Registerkarte Query monitoring (Abfrageüberwachung) für Metriken zu Ihren Abfragen aus.

4. Wählen Sie im Abschnitt Query monitoring (Abfrageüberwachung) die Registerkarte Database performance (Datenbankleistung) aus.

   Mithilfe der Steuerelemente im Fenster können Sie zwischen Cluster metrics (Cluster-Metriken) und WLM queue metrics (WLM-Warteschlangenmetriken) wechseln.

   Wenn Sie Cluster metrics (Cluster-Metriken) auswählen, enthält die Registerkarte die folgenden Diagramme:

   - Workload execution breakdown (Aufschlüsselung der Workload-Ausführung) – die Zeit, die für die Abfrageverarbeitungsphasen benötigt wird.
   - Queries by duration range (Abfragen nach Zeitdauerbereich) – die Anzahl kurzer, mittlerer und langer Abfragen.
   - Query throughput (Abfragedurchsatz) – die durchschnittliche Anzahl der pro Sekunde abgeschlossenen Abfragen.
   - Query duration (Abfragedauer) – die durchschnittliche Zeit zur Ausführung einer Abfrage.
   - Average queue wait time by priority (Durchschnittliche Warteschlangenwartezeit nach Priorität) – die Zeit, die Abfragen insgesamt mit Warten in der WLM-Warteschlange verbracht haben (nach Abfragepriorität).

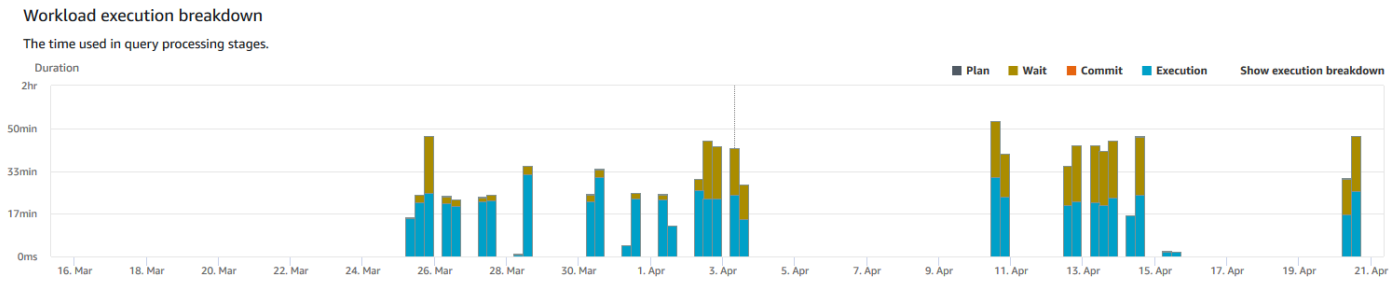
   Wenn Sie WLM queue metrics (WLM-Warteschlangenmetriken) auswählen, enthält die Registerkarte die folgenden Diagramme:

   - Query duration by queue (Abfragedauer nach Warteschlange) – die durchschnittliche Abfragedauer nach WLM-Warteschlange.
   - Query throughput by queue (Abfragedurchsatz nach Warteschlange) – die durchschnittliche Anzahl von Abfragen, die pro Sekunde abgeschlossen wurden, nach WLM-Warteschlange.
   - Query wait time by queue (Wartezeit für Abfragen nach Warteschlange) – die durchschnittliche Zeit, die Abfragen mit Warten verbracht haben, nach WLM-Warteschlange.

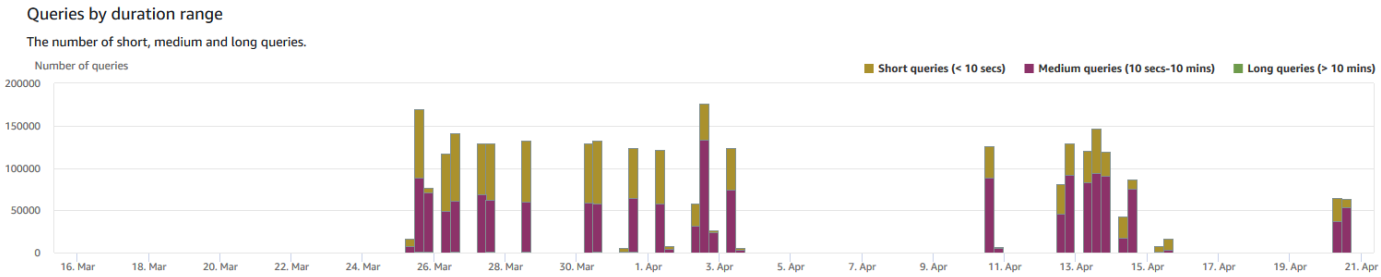
Diagramme der Datenbankleistung

Im Folgenden finden Sie einige Beispiele für Diagramme, die in der neuen Amazon-Redshift-Konsole angezeigt werden.

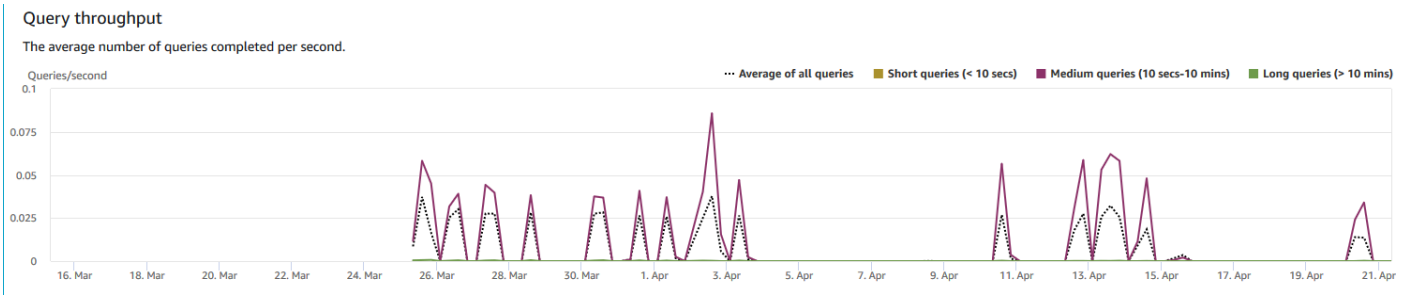
- Workload Execution Breakdown (Aufgliederung der Workload-Ausführung)



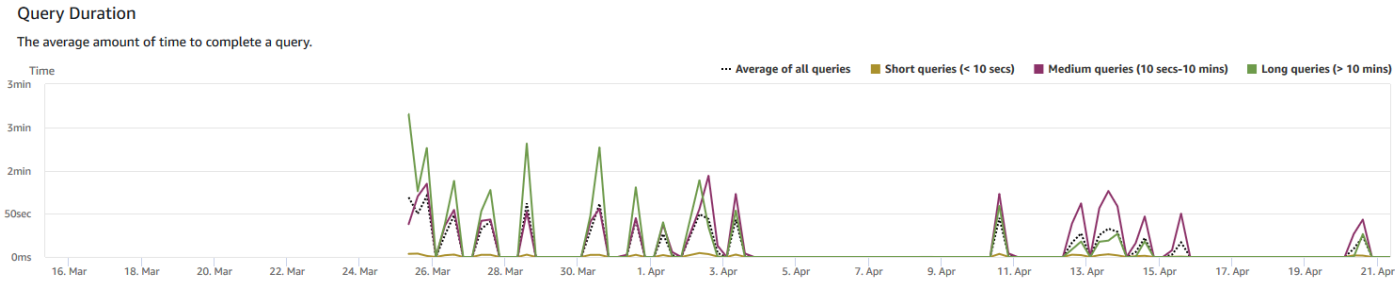
- Queries by duration range (Abfragen nach Dauerbereich)



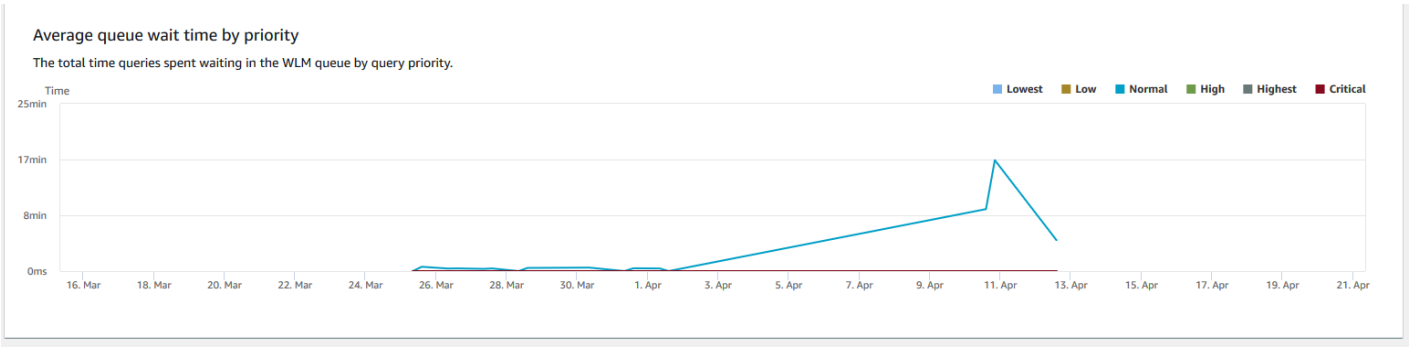
- Query throughput (Abfrage Durchsatz)



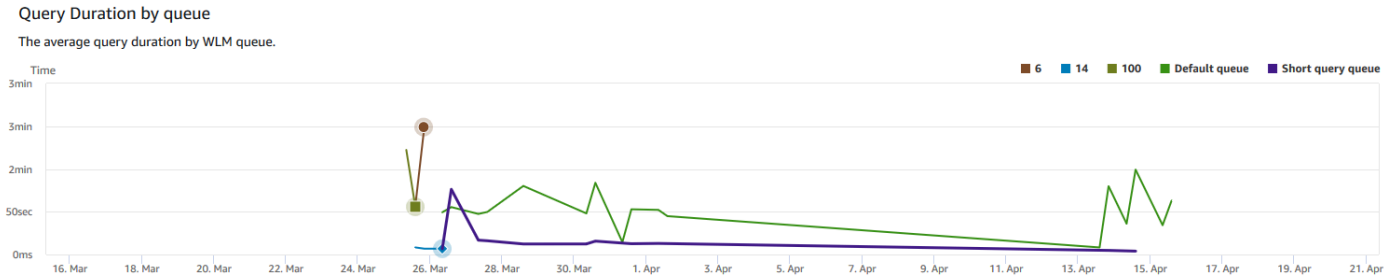
- Query duration (Abfragedauer)



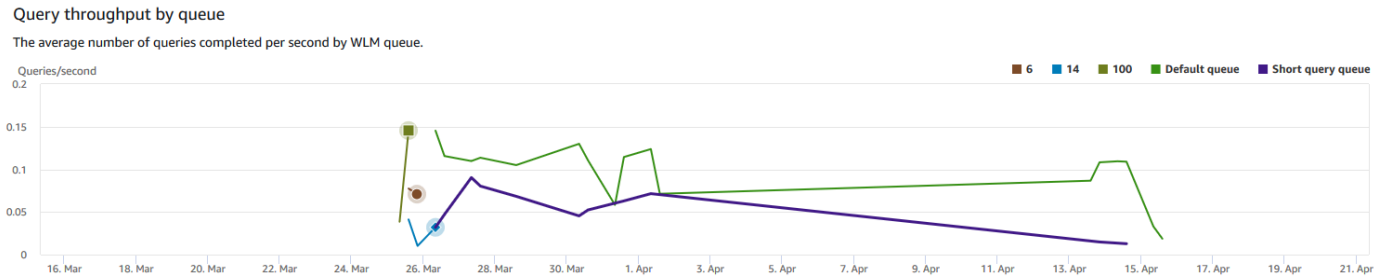
- Average queue wait time by priority (Durchschnittliche Wartezeit der Warteschlange nach Priorität)



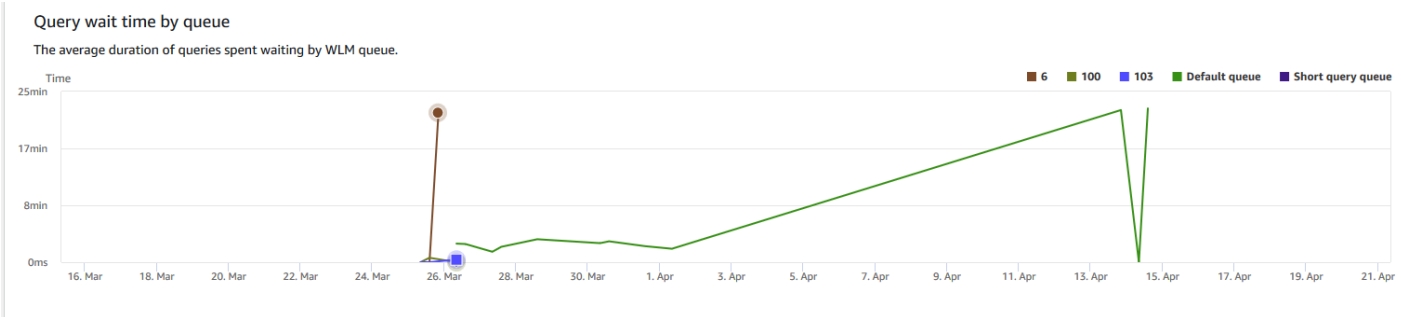
- Query duration by queue (Abfragedauer nach Warteschlange)



- Query throughput by queue (Abfragedurchsatz nach Warteschlange)



- Query wait time by queue (Wartezeit für die Abfrage nach Warteschlange)



Anzeigen der Parallelität des Workloads und der Parallelitätsskalierungsdaten

Mit Nebenläufigkeitsskalierungsmetriken in Amazon Redshift können Sie Folgendes tun:

- Analysieren Sie, ob Sie die Anzahl von Abfragen in der Warteschlange reduzieren können, indem Sie die Parallelität skalieren. Sie können nach WLM-Warteschlange oder für alle WLM-Warteschlangen vergleichen.
- Anzeigen von Nebenläufigkeitsskalierungsaktivitäten in Nebenläufigkeitsskalierungs-Clustern. So können Sie feststellen, ob die Nebenläufigkeitsskalierung durch `max_concurrency_scaling_clusters` begrenzt wird. Wenn dies zutrifft, können Sie `max_concurrency_scaling_clusters` im DB-Parameter erhöhen.
- Anzeigen der Gesamtnutzung der Nebenläufigkeitsskalierung für alle Nebenläufigkeitsskalierungs-Cluster zusammen.

So zeigen Sie die Parallelitäts-Skalierungsdaten an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster-Namen aus der Liste aus, um die Details zu dem Cluster aufzurufen. Die Details des Clusters werden angezeigt, u. a. einschließlich der Registerkarten Cluster performance (Cluster-Leistung), Query monitoring (Abfrageüberwachung), Databases (Datenbanken), Datashares, Schedules (Zeitpläne), Maintenance (Wartung) und Properties (Eigenschaften).
3. Wählen Sie die Registerkarte Query monitoring (Abfrageüberwachung) für Metriken zu Ihren Abfragen aus.
4. Wählen Sie im Abschnitt Query monitoring (Abfrageüberwachung) die Registerkarte Workload Concurrency (Workload-Parallelität) aus.

   Die Registerkarte enthält folgende Diagramme:

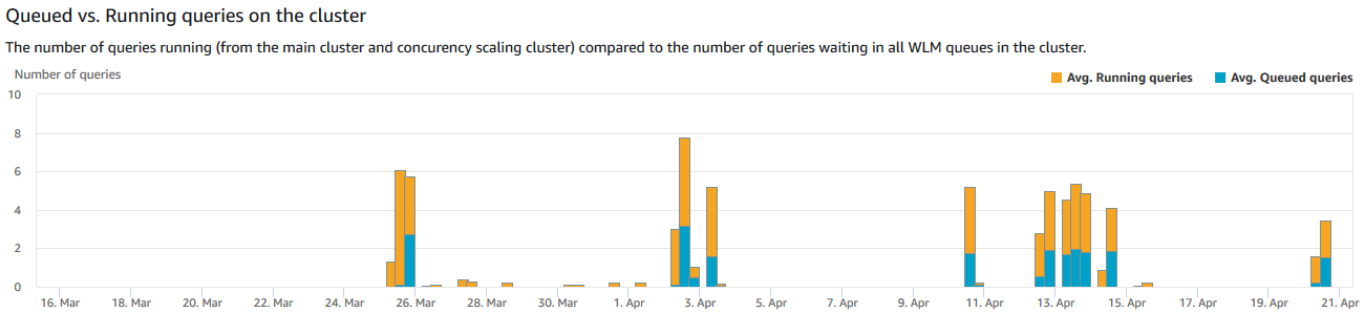
   - Queued vs. Running queries on the cluster (Abfragen in der Warteschlange vs. ausgeführte Abfragen auf dem Cluster) – die Anzahl der ausgeführten Abfragen (Haupt-Cluster und Nebenläufigkeitsskalierungs-Cluster) im Vergleich zur Anzahl der Abfragen, die in allen WLM-Warteschlangen im Cluster warten.

- Queued vs. Running queries per queue (Abfragen in der Warteschlange vs. ausgeführte Abfragen pro Warteschlange) – die Anzahl der ausgeführten Abfragen (Haupt-Cluster und Nebenläufigkeitsskalierungs-Cluster) im Vergleich zur Anzahl der Abfragen, die in jeder WLM-Warteschlange warten.
- Concurrency scaling activity (Nebenläufigkeitsskalierungsaktivität) – die Anzahl der Nebenläufigkeitsskalierungs-Cluster, die Abfragen aktiv verarbeiten.
- Concurrency scaling usage (Nutzung der Nebenläufigkeitsskalierung) – die Nutzung von Nebenläufigkeitsskalierungs-Clustern mit aktiver Abfrageverarbeitungsaktivität.

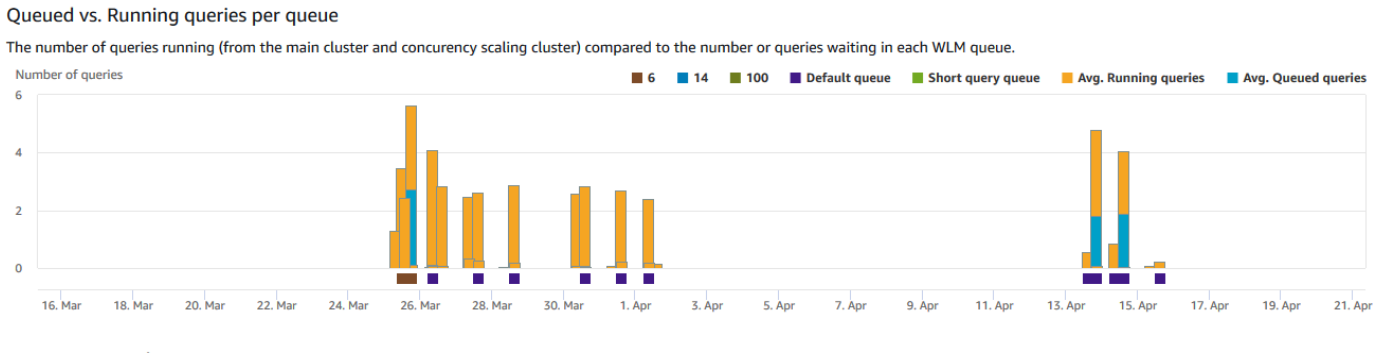
Diagramme der Parallelität des Workloads

Im Folgenden finden Sie einige Beispiele für Diagramme, die in der neuen Amazon-Redshift-Konsole angezeigt werden. Um ähnliche Diagramme in Amazon zu erstellen CloudWatch, können Sie die Parallelitätsskalierung und die CloudWatch WLM-Metriken verwenden. Weitere Informationen zu CloudWatch Metriken für Amazon Redshift finden Sie unterÜberwachung von Amazon Redshift mithilfe von Metriken CloudWatch .

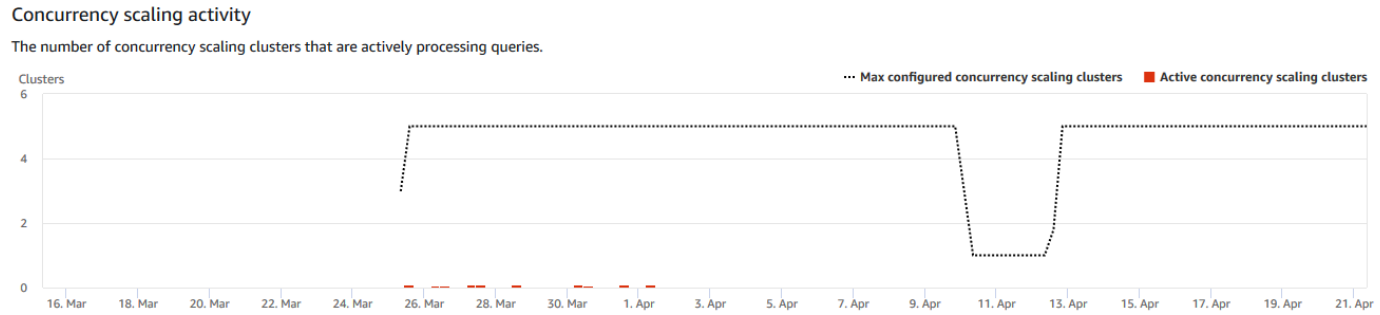
- Queued vs. Running queries on the cluster (Abfragen in der Warteschlange vs. ausgeführte Abfragen auf dem Cluster)



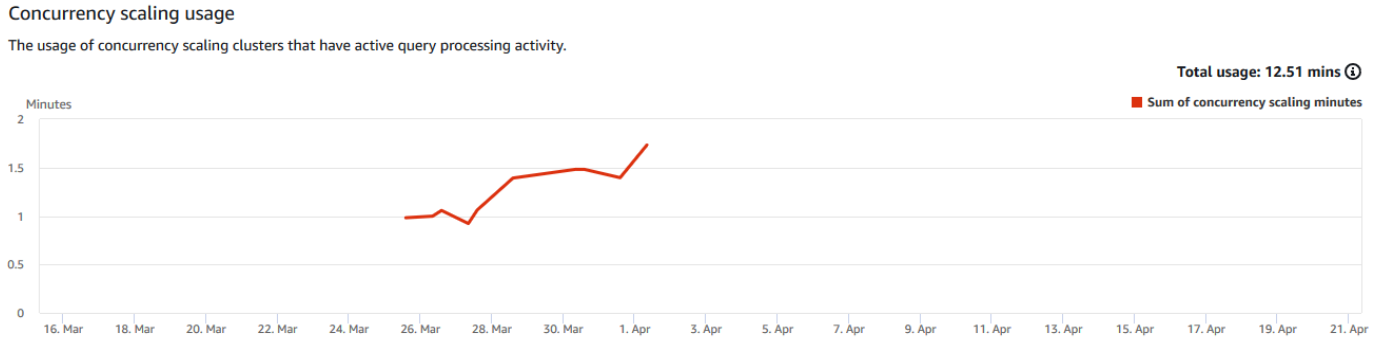
- Queued vs. Running queries per queue (Abfragen in der Warteschlange vs. ausgeführte Abfragen pro Warteschlange)



- Concurrency scaling activity (Parallelitätsskalierungsaktivität)



- Concurrency scaling usage (Nutzung der Parallelitätsskalierung)



Anzeigen von Abfragen und Ladevorgänge

Die Amazon-Redshift-Konsole bietet Informationen zu Abfragen und Ladevorgängen, die in der Datenbank ausgeführt werden. Sie können mithilfe dieser Informationen Abfragen identifizieren und reparieren, deren Verarbeitung lange Zeit in Anspruch nimmt, und die Engpässe verursachen, durch die andere Abfragen nicht effizient verarbeitet werden können. Sie können die Abfrageinformationen in der Amazon-Redshift-Konsole verwenden, um die Abfrageverarbeitung zu überwachen.

So zeigen Sie Abfrage-Leistungsdaten an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Queries and loads (Abfragen und Ladevorgänge) aus, um die Liste der Abfragen für Ihr Konto anzuzeigen.

   Standardmäßig zeigt die Liste Abfragen für alle Ihre Cluster der letzten 24 Stunden an. Sie können den Bereich des angezeigten Datums in der Konsole ändern.

   > **Important**
   >
   > Die Liste Queries and loads (Abfragen und Laden) zeigt die am längsten laufenden Abfragen im System an (bis zu 100 Abfragen).

Beenden einer laufenden Abfrage

Sie können außerdem die Seite Queries (Abfragen) verwenden, um eine gerade ausgeführt Abfrage zu beenden.

> **Note**
>
> Die Möglichkeit zum Beenden von Abfragen und Ladevorgängen in der Amazon-Redshift-Konsole unterliegt spezifischen Berechtigungen. Wenn Sie möchten, dass Benutzer Abfragen und Ladevorgänge beenden können, stellen Sie sicher, dass Sie die `redshift:CancelQuerySession` Aktion zu Ihrer AWS Identity and Access Management (IAM-) Richtlinie hinzufügen. Diese Anforderung gilt unabhängig davon, ob Sie die AWS verwaltete Amazon Redshift Redshift-Read-Only-Richtlinie auswählen oder eine benutzerdefinierte Richtlinie in IAM erstellen. Benutzer mit der Richtlinie Amazon Redshift Full Access (Amazon Redshift kompletter Zugriff) besitzen bereits die notwendige Berechtigung zum Beenden von Abfragen und Ladevorgängen. Weitere Informationen zu Aktionen in IAM-Richtlinien für Amazon Redshift finden Sie unter Verwalten des Zugriffs auf Ressourcen.

So beenden Sie eine laufende Abfrage:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Queries and loads (Abfragen und Ladevorgänge) aus, um die Liste der Abfragen für Ihr Konto anzuzeigen.
3. Wählen Sie die laufende Abfrage aus, die Sie in der Liste beenden möchten. Wählen Sie dann Terminate query (Abfrage beenden) aus.

Anzeigen von Abfragedetails

Sie können Abfragedetails in der Amazon-Redshift-Konsole analysieren. Mit einem Abfrage-ID können Sie Details einer Abfrage anzeigen. Zu den Details gehören z. B. der Abschlussstatus, die Dauer und die SQL-Anweisung der Abfrage sowie, ob es sich um eine Benutzerabfrage oder eine von Amazon Redshift umgeschriebene Abfrage handelt. Eine Benutzerabfrage ist eine Abfrage, die entweder von einem SQL-Client oder von einem Business-Intelligence-Tool an Amazon Redshift gesendet wird. Amazon Redshift schreibt die Abfrage möglicherweise neu, um sie zu optimieren, was zu mehreren neu geschriebenen Abfragen führen kann. Der Prozess wird zwar von Amazon Redshift ausgeführt, dennoch sehen Sie umgeschriebene Abfragen zusammen mit der Benutzerabfrage auf der Abfragedetailseite.

So zeigen Sie eine Abfrage an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Queries and loads (Abfragen und Ladevorgänge) aus, um die Liste der Abfragen für Ihr Konto anzuzeigen. Möglicherweise müssen Sie die Einstellungen auf dieser Seite ändern, um Ihre Anfrage zu finden.
3. Wählen Sie den Identifikator Query (Abfrage) in der Liste aus, um Query details (Abfragedetails) anzuzeigen.

   Die Seite Query details (Abfragedetails) enthält Query details (Abfragedetails)- und Query plan (Abfrageplan)-Registerkarten mit Metriken über die Abfrage.

   Zu den Metriken gehören Details zu einer Abfrage wie Startzeit, Abfrage-ID, Status und Dauer. Zu den weiteren Details gehört, ob eine Abfrage auf einem Haupt-Cluster oder einem

Nebenläufigkeitsskalierungs-Cluster ausgeführt wurde und ob es sich um eine übergeordnete oder um eine umgeschriebene Abfrage handelt.

Analyse der Abfrageausführung

So analysieren Sie eine Abfrage:

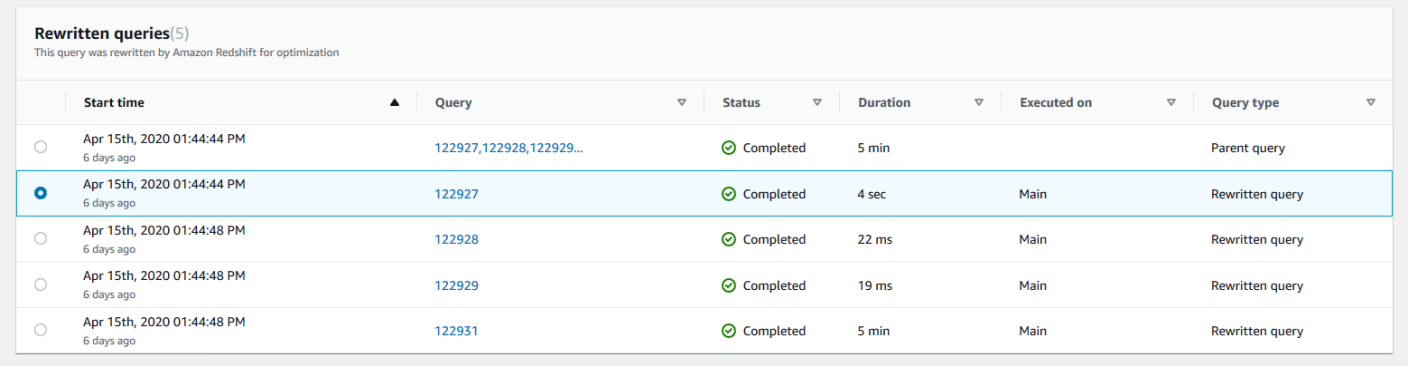
1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Queries and loads (Abfragen und Ladevorgänge) aus, um die Liste der Abfragen für Ihr Konto anzuzeigen. Möglicherweise müssen Sie die Einstellungen auf dieser Seite ändern, um Ihre Anfrage zu finden.
3. Wählen Sie den Identifikator Query (Abfrage) in der Liste aus, um Query details (Abfragedetails) anzuzeigen.

   Die Seite Query details (Abfragedetails) enthält Query details (Abfragedetails)- und Query plan (Abfrageplan)-Registerkarten mit Metriken über die Abfrage.

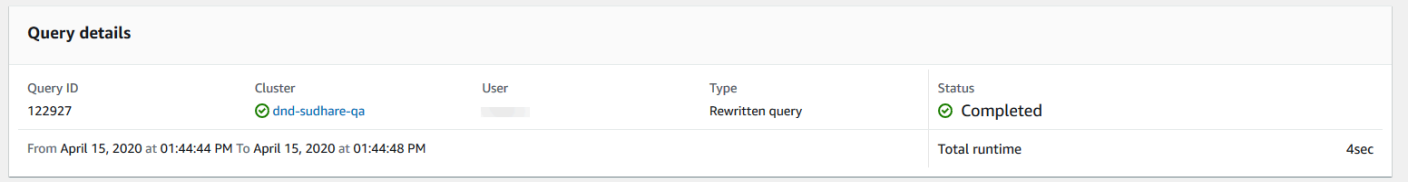
   > **Note**
   >
   > Sie können auch von einer Cluster details (Cluster-Details)-Seite und der Registerkarte Query history (Abfrageverlauf), wenn Sie einen Drilldown für eine Abfrage in einem Query runtime (Abfragelaufzeit)-Diagramm durchführen, zur Seite Query details (Abfragedetails) navigieren.

Die Seite Query details (Abfragedetails) enthält die folgenden Abschnitte:

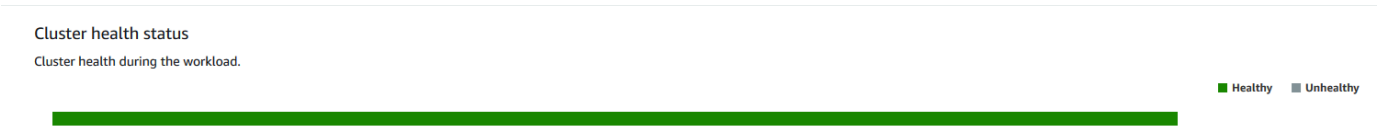
- Eine Liste der Rewritten queries (neu geschriebenen Abfragen), wie im folgenden Screenshot dargestellt.



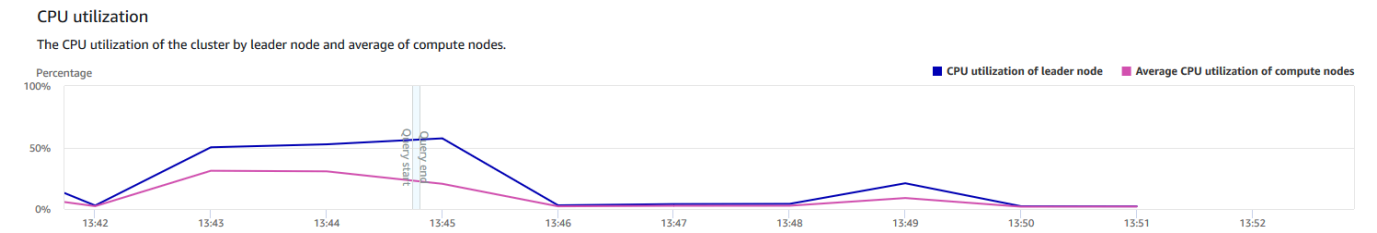
- Ein Abschnitt Query details (Abfragedetails), wie im folgenden Screenshot dargestellt.



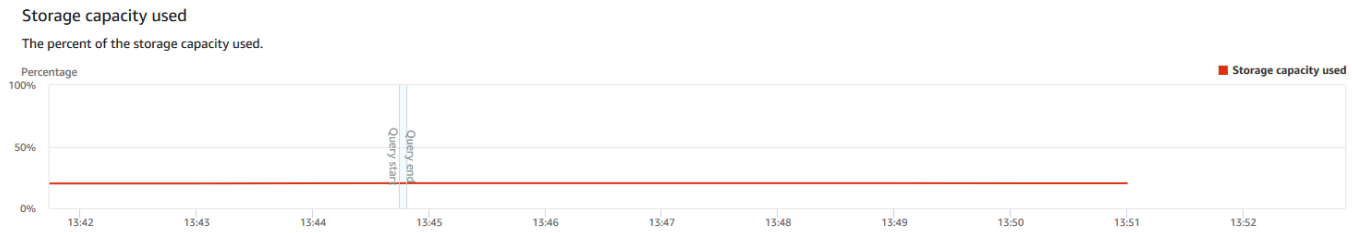
- Eine Registerkarte Query details (Abfragedetails), die die ausgeführte SQL und die Execution details (Ausführungsdetails) über die Ausführung enthält.
- Eine Registerkarte Query plan (Abfrageplan), die die Schritte des Query plan (Abfrageplans) und andere Informationen über den Abfrageplan enthält. Diese Tabelle enthält auch Diagramme zum Cluster, wenn die Abfrage ausgeführt wurde.
  - Cluster health status (Cluster-Integritätsstatus)



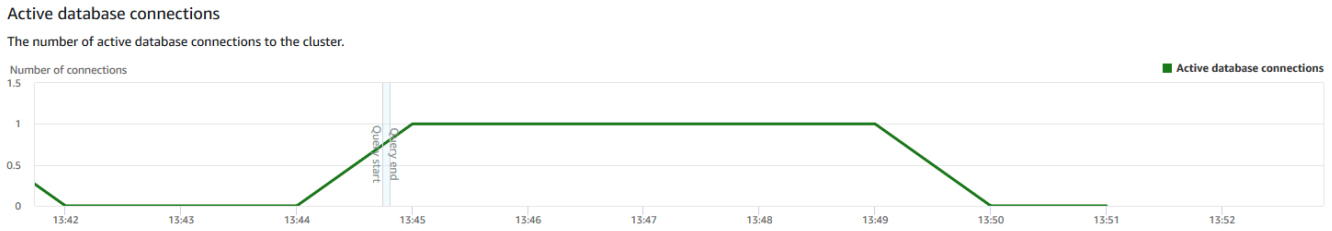
  - CPU-Nutzung



  - Verwendete Speicherkapazität



- Active database connections (Aktive Datenbankverbindungen)



Anzeigen der Cluster-Leistung während der Ausführung von Abfragen

So zeigen Sie die Cluster-Leistung während der Ausführung von Abfragen an

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster-Namen aus der Liste aus, um die Details zu dem Cluster aufzurufen. Die Details des Clusters werden angezeigt, u. a. einschließlich der Registerkarten Cluster performance (Cluster-Leistung), Query monitoring (Abfrageüberwachung), Databases (Datenbanken), Datashares, Schedules (Zeitpläne), Maintenance (Wartung) und Properties (Eigenschaften).
3. Wählen Sie die Registerkarte Query monitoring (Abfrageüberwachung) aus, um weitere Details anzuzeigen.

   Weitere Informationen finden Sie unter Anzeigen der Abfrageverlaufsdaten.

Anzeigen von Cluster-Metriken während der Ausführung von Lade-Operationen

Wenn Sie die Cluster-Leistung während der Ladevorgänge anzeigen, können Sie Abfragen identifizieren, die Ressourcen verbrauchen, und Maßnahmen ergreifen, um deren Auswirkungen

zu mindern. Sie können einen Ladevorgang beenden, wenn Sie nicht wünschen, dass er bis zum Abschluss ausgeführt wird.

> **Note**
>
> Die Möglichkeit zum Beenden von Abfragen und Ladevorgängen in der Amazon-Redshift-Konsole unterliegt spezifischen Berechtigungen. Wenn Sie möchten, dass Benutzer Abfragen und Ladevorgänge beenden können, stellen Sie sicher, dass Sie die `redshift:CancelQuerySession` Aktion zu Ihrer AWS Identity and Access Management (IAM-) Richtlinie hinzufügen. Diese Anforderung gilt unabhängig davon, ob Sie die von Amazon Redshift Read Only AWS verwaltete Richtlinie auswählen oder eine benutzerdefinierte Richtlinie in IAM erstellen. Benutzer mit der Richtlinie Amazon Redshift Full Access (Amazon Redshift kompletter Zugriff) besitzen bereits die notwendige Berechtigung zum Beenden von Abfragen und Ladevorgängen. Weitere Informationen zu Aktionen in IAM-Richtlinien für Amazon Redshift finden Sie unter Verwalten des Zugriffs auf Ressourcen.

So zeigen Sie die Cluster-Leistung während des Ladevorgangs an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster-Namen aus der Liste aus, um die Details zu dem Cluster aufzurufen. Die Details des Clusters werden angezeigt, u. a. einschließlich der Registerkarten Cluster performance (Cluster-Leistung), Query monitoring (Abfrageüberwachung), Databases (Datenbanken), Datashares, Schedules (Zeitpläne), Maintenance (Wartung) und Properties (Eigenschaften).
3. Wählen Sie die Registerkarte Query monitoring (Abfrageüberwachung) aus, um weitere Details anzuzeigen.
4. Wählen Sie im Abschnitt Queries and loads (Abfragen und Laden) Loads (Laden) aus, um die Ladevorgänge eines Clusters anzuzeigen. Wenn eine Abfrage ausgeführt wird, können Sie diese beenden, indem Sie Terminate query (Abfrage beenden) auswählen.

Analysieren der Workload-Leistung

Eine detaillierte Ansicht der Performance Ihrer Workload finden Sie in der Workload Execution Breakdown-Tabelle (Aufgliederung der Workload-Ausführung) auf der Konsole. Wir erstellen

das Diagramm mit Daten, die von der QueryRuntimeBreakdown Metrik bereitgestellt werden. Anhand dieses Diagramms erkennen Sie, wie viel Zeit Ihre Abfragen in den verschiedenen Bearbeitungsphasen verbringen, wie z. B. Warten und Planen.

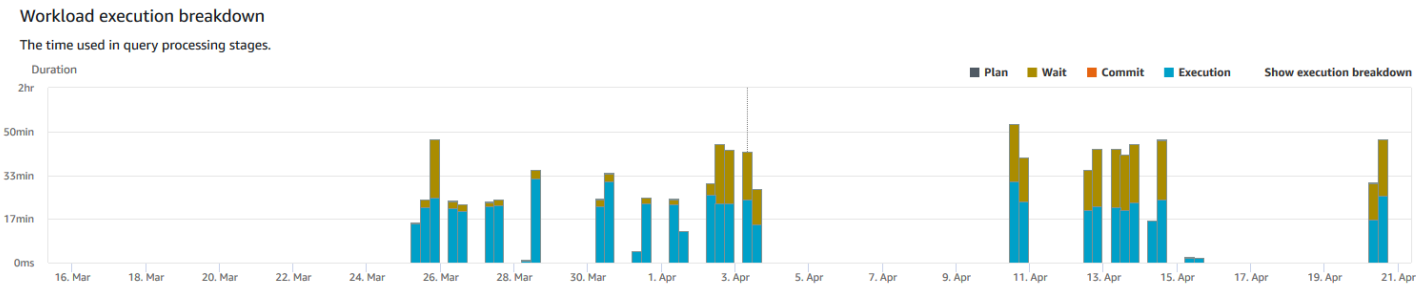
> **Note**
>
> Die Workload Execution Breakdown-Tabelle wird bei Einzelknoten-Clustern nicht angezeigt.

In der folgenden Metriken-Liste beschreibt die verschiedenen Bearbeitungsphasen:

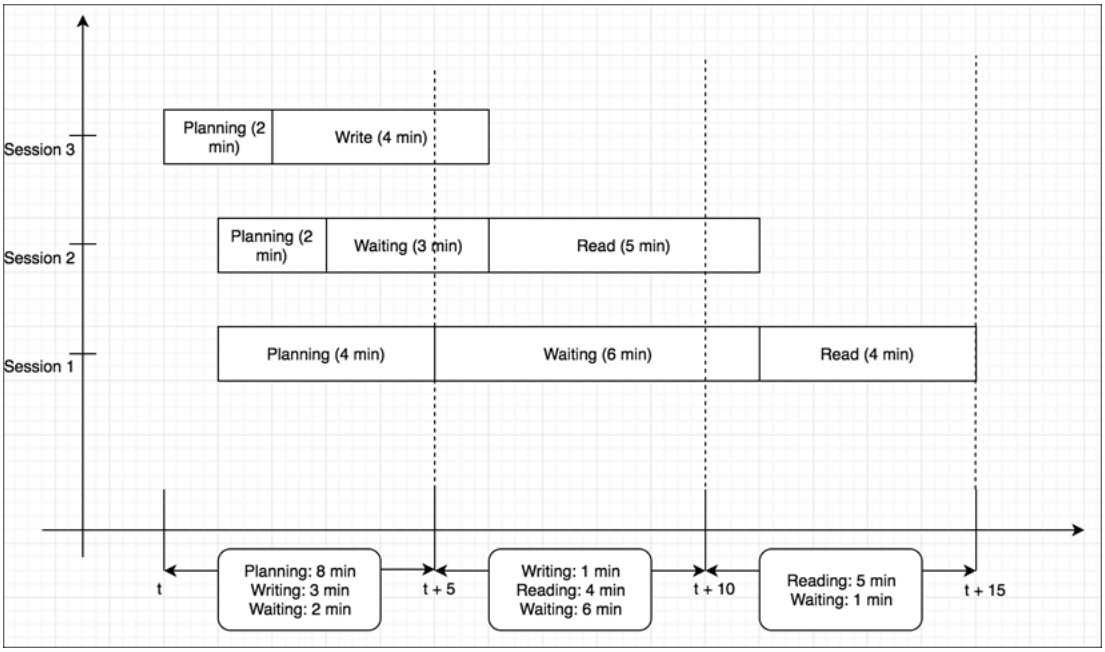
- `QueryPlanning`: Für die Analyse und Optimierung der SQL-Anweisungen aufgewendete Zeit.
- `QueryWaiting`: Für das Warten in einer WLM-Warteschlange (Workload Management) aufgewendete Zeit.
- `QueryExecutingRead`: Für die Ausführung von Leseabfragen aufgewendete Zeit.
- `QueryExecutingInsert`: Für die Ausführung von Einfügungsabfragen aufgewendete Zeit.
- `QueryExecutingDelete`: Für die Ausführung von Löschabfragen aufgewendete Zeit.
- `QueryExecutingUpdate`: Für die Ausführung von Aktualisierungsabfragen aufgewendete Zeit.
- `QueryExecutingCtas`: Für die Ausführung von CREATE TABLE AS-Abfragen aufgewendete Zeit.
- `QueryExecutingUnload`: Für die Ausführung von Entladeabfragen aufgewendete Zeit.
- `QueryExecutingCopy`: Für die Ausführung von Kopierabfragen aufgewendete Zeit.

Beispiel: Das folgende Diagramm in der Amazon-Redshift-Konsole zeigt die Dauer, die Abfragen in den Phasen Planen, Warten, Lesen und Schreiben verbracht haben. Sie können die Erkenntnisse aus diesem Diagramm zur weiteren Analyse mit anderen Metriken kombinieren. In einigen Fällen zeigt Ihr Diagramm möglicherweise, dass Abfragen mit kurzer Dauer (wie von der `QueryDuration`-Metrik gemessen) lange Zeit in der Wartephase verbringen, In diesen Fällen können Sie die WLM-Gleichzeitigkeitsrate für eine bestimmte Warteschlange erhöhen, um den Durchsatz zu erhöhen.

Im Folgenden finden Sie ein Beispiel für die Ausführung des Aufschlüsselungsdiagramms für die Workload-Ausführung. Im Diagramm gibt der Y-Achsenwert die durchschnittliche Dauer jeder Stufe zur angegebenen Zeit an. Dies wird als gestapeltes Balkendiagramm angezeigt.



Das folgende Diagramm zeigt, wie Amazon Redshift die Abfrageverarbeitung für gleichzeitige Sitzungen aggregiert.



So zeigen Sie die Cluster-Workload-Aufschlüsselungstabelle an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Clusters (Cluster) und dann den Cluster-Namen aus der Liste aus, um die Details zu dem Cluster aufzurufen. Die Details des Clusters werden angezeigt, u. a. einschließlich der Registerkarten Cluster performance (Cluster-Leistung), Query monitoring (Abfrageüberwachung), Databases (Datenbanken), Datashares, Schedules (Zeitpläne), Maintenance (Wartung) und Properties (Eigenschaften).
3. Wählen Sie die Registerkarte Query monitoring (Abfrageüberwachung) für Metriken zu Ihren Abfragen aus.

4. Wählen Sie im Abschnitt Query monitoring (Abfrageüberwachung) die Option Database performance (Datenbankleistung) und dann Cluster metrics (Clustermetriken) aus.

   Die folgenden Metriken werden für den gewählten Zeitbereich als gestapeltes Balkendiagramm dargestellt:

   - Plan Zeit
   - Wait (Warten) Zeit
   - Commit-Zeit
   - Uhrzeit der Ausführung

Verwalten von Alarmen

Alarme, die Sie in der Amazon Redshift Redshift-Konsole erstellen, sind CloudWatch Alarme. Diese sind nützlich, da Sie Ihnen dabei helfen, proaktive Entscheidungen zu Ihrem Cluster oder Ihrer Serverless-Instance zu treffen. Sie können einen oder mehrere Alarme für all der in Überwachung von Amazon Redshift mithilfe von Metriken CloudWatch aufgeführten Metriken einrichten. Die Einrichtung eines Alarms für hohe `CPUUtilization`-Werte auf einem Cluster-Knoten hilft beispielsweise dabei zu erkennen, wann der Knoten überlastet ist. Ein Alarm bei hohem `DataStorage` würde den Speicherplatz überwachen, den Ihr Serverless-Namespace für Ihre Daten verwendet.

Über Actions (Aktionen) können Sie Alarme ändern oder löschen. Sie können auch einen Chime- oder Slack-Alarm erstellen, um eine Warnung von an Slack oder Amazon Chime CloudWatch zu senden, indem Sie eine Slack- oder Amazon Chime Chime-Webhook-URL angeben.

Dieser Abschnitt erläutert die Erstellung eines Alarms mit der Amazon-Redshift-Konsole. Sie können einen Alarm mithilfe der CloudWatch Konsole oder auf jede andere Art und Weise, wie Sie mit Metriken arbeiten, erstellen, z. B. mit dem oder einem SDK. AWS CLI AWS

So erstellen Sie einen CloudWatch Alarm mit der Amazon Redshift Redshift-Konsole

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.

   Wenn Sie Amazon Redshift Serverless verwenden, wählen Sie Go to Serverless (Serverless aufrufen) oben rechts im Dashboard aus.
2. Wählen Sie im Navigationsmenü Alarms (Alarme) und dann Create alarm (Alarm erstellen) aus.

3. Geben Sie auf der Seite „Alarm erstellen“ die Eigenschaften ein, um einen CloudWatch Alarm zu erstellen.
4. Wählen Sie Alarm erstellen aus.

Arbeiten mit Leistungskennzahlen in der CloudWatch Konsole

Beachten Sie bei der Arbeit mit Amazon Redshift Redshift-Metriken in der CloudWatch Konsole einige Dinge:

- Abfrage- und Ladeleistungsdaten sind nur in der Amazon-Redshift-Konsole verfügbar.
- Einige Metriken in der CloudWatch haben andere Einheiten als die, die in der Amazon Redshift Redshift-Konsole verwendet werden. Beispielsweise `WriteThroughput` wird sie in GB/s (im Vergleich zu Bytes/s in CloudWatch) angezeigt, was für den typischen Speicherplatz eines Knotens eine relevantere Einheit ist.

Beachten Sie bei der Arbeit mit Amazon Redshift Redshift-Metriken in der CloudWatch Konsole, in Befehlszeilentools oder einem Amazon SDK die folgenden Konzepte:

1. Geben Sie zunächst die Metrikdimension an, mit der Sie arbeiten möchten. Eine Dimension ist ein Name-Wert-Paar, mit dem Sie eine Metrik eindeutig identifizieren. Die Dimensionen für Amazon Redshift sind `ClusterIdentifier` und `NodeID`. In der CloudWatch Konsole stehen die `Redshift Node` Ansichten `Redshift Cluster` und zur einfachen Auswahl cluster- und knotenspezifischer Dimensionen zur Verfügung. Weitere Informationen zu Dimensionen finden Sie unter Dimensionen im CloudWatch Entwicklerhandbuch.
2. Geben Sie dann den Metriknamen an, z. B. `ReadIOPS`.

In der folgenden Tabelle finden Sie eine Zusammenfassung der Arten der verfügbaren Amazon-Redshift-Metrikdimensionen. Je nach Metrik sind die Daten entweder in 1-Minuten- oder 5-Minuten-Intervallen kostenlos verfügbar. Weitere Informationen finden Sie unter Amazon-Redshift-Metriken.

CloudWatch Namespace	Dimension	Beschreibung
`AWS/Redshift`	`NodeID`	Filtert angeforderte Daten, die für die Knoten eines Clusters spezifisch sind. `NodeID` ist entweder „Leader“, „Shared“ oder „Compute-N“, wobei N gleich 0, 1 ...

CloudWatch Namespace	Dimension	Beschreibung
		entsprechend der Anzahl der Knoten im Cluster ist. "Shared" bedeutet, dass das Cluster nur über einen Knoten verfügt, d. h., dass der Führungs- und der Datenverarbeitungsknoten kombiniert sind.
	`ClusterIdentifier`	Filtert angeforderte Daten, die für den Cluster spezifisch sind. Cluster-spezifische Metriken beinhalten `HealthStatus` , `MaintenanceMode` und `DatabaseConnections` . Allgemeine Metriken für diese Dimension (z. B. `ReadIOPS`), die auch Knotenmetriken sind, stellen den Gesamtwert der Knotenmetrikdaten dar. Berücksichtigen Sie bei der Interpretation dieser Metriken den Umstand, dass sie das Gesamtverhalten der Führungs- und Datenverarbeitungsknoten darstellen.

Das Arbeiten mit Gateway- und Volume-Metriken gleicht dem Arbeiten mit anderen Service-Metriken. Viele der häufigsten Aufgaben werden in der CloudWatch Dokumentation beschrieben, darunter die folgenden:

- Anzeigen der verfügbaren Metriken
- Abrufen von Statistiken für eine Metrik
- Erstellen von CloudWatch-Alarmen

Amazon-Redshift-Ereignisse

Themen

- Übersicht über Cluster-Ereignisse
- Arbeiten mit Amazon Simple Notification Service
- Abonnieren von Cluster-Ereignisbenachrichtigungen von Amazon Redshift
- Anzeigen von Cluster-Ereignissen unter Verwendung der Konsole
- Cluster-Ereignisse mithilfe der Amazon Redshift-API AWS CLI und der Amazon Redshift Redshift-API anzeigen
- Verwalten von Cluster-Ereignisbenachrichtigungen
- Ereignisbenachrichtigungen zu Amazon Redshift
- Ereignisbenachrichtigungen von Amazon Redshift Serverless mit Amazon EventBridge
- Ereignisbenachrichtigungen zur Null-ETL-Integration mit Amazon EventBridge

Übersicht über Cluster-Ereignisse

Amazon Redshift verfolgt Cluster-Ereignisse und speichert Informationen über sie für einen Zeitraum von mehreren Wochen in Ihrem AWS Konto. Amazon Redshift meldet bei jedem Ereignis Informationen wie Datum und Uhrzeit, zu denen das Ereignis auftrat, eine Beschreibung, die Ereignisquelle (z. B. ein Cluster, eine Parametergruppe oder ein Snapshot) und die Quell-ID.

Amazon Redshift informiert Sie bei bestimmten Ereignissen vorab. Diese Ereignisse haben die Ereigniskategorie `pending`. Wir informieren Sie beispielsweise vorab, wenn für einen der Knoten in Ihrem Cluster ein Hardwareupdate erforderlich ist. Sie können Ereignisse der Kategorie „pending“ wie andere Amazon Redshift-Ereignisse abonnieren. Weitere Informationen finden Sie unter Abonnieren von Cluster-Ereignisbenachrichtigungen von Amazon Redshift.

Sie können die Amazon Redshift Management Console, die Amazon Redshift API oder die AWS SDKs verwenden, um Ereignisinformationen abzurufen. Sie können eine Liste aller Ereignisse abrufen oder Filter – etwa zur Ereignisdauer oder zum Beginn- und Enddatum - verwenden, um Ereignisinformationen nur für einen bestimmten Zeitraum zu erhalten.

Sie können auch Ereignisse abrufen, die von einem bestimmten Quelltyp erstellt wurden, etwa Cluster-Ereignisse oder Parametergruppen-Ereignisse. Die Spalte Source (Quelle) zeigt den Ressourcennamen und den Ressourcentyp, der eine bestimmte Aktion auslöst.

Sie können Abonnements für Amazon-Redshift-Ereignisbenachrichtigungen erstellen, die eine Gruppe von Ereignisfiltern angeben. Wenn ein Ereignis auftritt, das den Filterkriterien entspricht, nutzt Amazon Redshift Amazon Simple Notification Service, um Sie aktiv über das Auftreten des Ereignisses zu informieren.

Eine Liste der Amazon-Redshift-Ereignisse nach Quellentyp und Kategorie finden Sie unter the section called “Amazon-Redshift-Ereigniskategorien und -Ereignismeldungen”.

Arbeiten mit Amazon Simple Notification Service

Amazon Redshift verwendet den Amazon Simple Notification Service (Amazon SNS) für Benachrichtigungen zu Amazon-Redshift-Ereignissen. Sie aktivieren die Benachrichtigungen, indem Sie ein Amazon-Redshift-Ereignisabonnement erstellen. Geben Sie im Amazon-Redshift-Abonnement einen Satz von Filtern für Amazon-Redshift-Ereignisse und ein Amazon-SNS-Thema an. Wenn ein Ereignis eintritt, das den Filterkriterien entspricht, veröffentlicht Amazon Redshift eine Benachrichtigungsmeldung zum Amazon-SNS-Thema. Amazon SNS übermittelt die Nachricht dann an alle Amazon-SNS-Verbraucher, die über ein Amazon-SNS-Abonnement für das Thema verfügen. Die an die Amazon SNS-Verbraucher gesendeten Nachrichten können in jeder Form erfolgen, die von Amazon SNS für eine AWS Region unterstützt wird, z. B. als E-Mail, Textnachricht oder Anruf an einen HTTP-Endpunkt. Beispielsweise unterstützen alle Regionen E-Mail-Benachrichtigungen, SMS-Benachrichtigungen können jedoch nur in der Region USA Ost (Nord-Virginia) erstellt werden.

> **Note**
>
> Derzeit können Sie nur ein Ereignisabonnement für ein Amazon-SNS-Standardthema erstellen (nicht für ein Amazon-SNS-FIFO-Thema). Weitere Informationen finden Sie unter Amazon-SNS-Ereignisquellen im Entwicklerhandbuch zu Amazon Simple Notification Service.

Wenn Sie ein Abonnement für Ereignisbenachrichtigungen erstellen, geben Sie einen oder mehrere Ereignisfilter an. Amazon Redshift sendet Benachrichtigungen über das Abonnement immer dann, wenn ein Ereignis auftritt, das allen Filterkriterien entspricht. Zu den Filterkriterien gehören Quelltyp (wie etwa Cluster oder Snapshot), Quell-ID (etwa der Name eines Clusters oder Snapshots), Ereigniskategorie (etwa Überwachung oder Sicherheit) sowie der Schweregrad des Ereignisses (wie etwa INFO oder FEHLER).

Sie können die Benachrichtigung ganz einfach deaktivieren, ohne ein Abonnement zu löschen, indem Sie das Optionsfeld Aktiviert No im AWS Management Console oder indem Sie den `Enabled` Parameter auf `false` Verwenden der Amazon Redshift Redshift-CLI oder -API setzen.

Die Fakturierung für Amazon-Redshift-Ereignisbenachrichtigungen erfolgt über Amazon Simple Notification Service (Amazon SNS). Wenn Sie Ereignisbenachrichtigungen verwenden, fallen Amazon-SNS-Gebühren an. Weitere Informationen zur Amazon-SNS-Fakturierung finden Sie unter Amazon Simple Notification Service Pricing (Amazon Simple Notification Service – Preise).

Sie können auch mit der Managementkonsole stattgefundene Amazon-Redshift-Ereignisse anzeigen. Weitere Informationen finden Sie unter Amazon-Redshift-Ereignisse.

Abonnieren von Cluster-Ereignisbenachrichtigungen von Amazon Redshift

Sie können ein Abonnement für Amazon-Redshift-Ereignisbenachrichtigungen erstellen, um benachrichtigt zu werden, wenn ein Ereignis für einen bestimmten Cluster, Snapshot, eine Sicherheitsgruppe oder eine Parametergruppe eintritt. Am einfachsten lässt sich ein Abonnement mit der Amazon-SNS-Konsole erstellen. Weitere Informationen zum Erstellen und Abonnieren eines Amazon-SNS-Themas finden Sie unter Getting started with Amazon SNS (Erste Schritte mit Amazon SNS).

Sie können ein Abonnement für Amazon-Redshift-Ereignisbenachrichtigungen erstellen, um benachrichtigt zu werden, wenn ein Ereignis für einen bestimmten Cluster, Snapshot, eine Sicherheitsgruppe oder eine Parametergruppe eintritt. Am einfachsten lässt sich ein Abonnement mit der erstellen AWS Management Console. Wenn Sie Abonnements für Ereignisbenachrichtigungen mithilfe der CLI oder API erstellen möchten, müssen Sie ein Amazon Simple Notification Service-Thema erstellen und dieses Thema über die Amazon SNS-Konsole oder Amazon SNS-API abonnieren. Sie müssen sich auch den Amazon-Ressourcennamen (ARN) des Themas notieren, da dieser beim Übermitteln von CLI-Befehlen oder API-Aktionen verwendet wird. Weitere Informationen zum Erstellen und Abonnieren eines Amazon-SNS-Themas finden Sie unter Getting started with Amazon SNS (Erste Schritte mit Amazon SNS).

Ein Amazon-Redshift-Ereignisabonnement kann diese Ereigniskriterien angeben:

- Quelltyp, die Werte sind Cluster, Snapshot, Parametergruppen und Sicherheitsgruppen.
- Quell-ID einer Ressource, wie etwa `my-cluster-1` oder `my-snapshot-20130823`. Die ID muss für eine Ressource in derselben AWS Region wie das Event-Abonnement gelten.

- Ereigniskategorie, die Werte sind Konfiguration, Management, Überwachung, Sicherheit und ausstehend
- Schweregrad des Ereignisses, die Werte sind INFO oder FEHLER.

Die Ereigniskriterien können unabhängig voneinander angegeben werden, Sie müssen jedoch einen Quelltyp angeben, bevor Sie Quell-IDs in der Konsole angeben können. Zum Beispiel: Sie können eine Ereigniskategorie angeben, ohne dass Sie einen Quelltyp, eine Quell-ID oder einen Schweregrad angeben. Sie können zwar Quell-IDs für Ressourcen angeben, die nicht dem angegebenen Quelltyp entsprechen, für Ereignisse von solchen Ressourcen werden jedoch keine Benachrichtigungen gesendet. Zum Beispiel: Wenn Sie den Quelltyp Cluster und die ID einer Sicherheitsgruppe angeben, entspricht keines der von dieser Sicherheitsgruppe gemeldeten Ereignisse den Filterkriterien für den Quelltyp, weshalb für solche Ereignisse keine Benachrichtigungen gesendet werden.

Amazon Redshift sendet eine Benachrichtigung für jedes Ereignis, das allen in einem Abonnement angegebenen Kriterien entspricht. Einige Beispiele für die ausgegebenen Ereignissätze:

- Das Abonnement gibt den Quelltyp Cluster, die Quell-ID my-cluster-1, die Kategorie Überwachung und den Schweregrad FEHLER an. Das Abonnement sendet Benachrichtigungen nur für Überwachungsereignisse mit dem Schweregrad FEHLER von my-cluster-1.
- Das Abonnement gibt den Quelltyp Cluster, die Kategorie Konfiguration und den Schweregrad INFO an. Das Abonnement sendet Benachrichtigungen für Konfigurationsereignisse mit dem Schweregrad INFO von jedem Amazon Redshift Redshift-Cluster im AWS Konto.
- Das Abonnement gibt die Kategorie Konfiguration und den Schweregrad INFO an. Das Abonnement sendet Benachrichtigungen über Konfigurationsereignisse mit dem Schweregrad INFO von jeder Amazon Redshift Redshift-Ressource im AWS Konto.
- >Das Abonnement gibt den Schweregrad FEHLER an. Das Abonnement sendet Benachrichtigungen für alle Ereignisse mit dem Schweregrad FEHLER von allen Amazon Redshift Redshift-Ressourcen im AWS Konto.

Wenn Sie ein Objekt löschen oder umbenennen, dessen Name als Quell-ID in einem bestehenden Abonnement auftritt, bleibt das Abonnement aktiv, es kann jedoch keine Ereignisse von dem betreffenden Objekt weiterleiten. Wenn Sie später ein neues Objekt mit dem selben Namen, der in der Quell-ID des Abonnements genannt ist, erstellen, beginnt das Abonnement, Benachrichtigungen zu Ereignissen von dem neuen Objekt zu senden.

Amazon Redshift veröffentlicht Ereignisbenachrichtigungen zu einem Amazon-SNS-Thema, das durch seinen Amazon-Ressourcennamen (ARN) identifiziert wird. Wenn Sie ein Ereignisabonnement mit der Amazon-Redshift-Konsole erstellen, können Sie ein vorhandenes Amazon-SNS-Thema angeben oder die Erstellung des Themas durch die Konsole anfordern, wenn diese das Abonnement einrichtet. Alle Amazon-Redshift-Ereignisbenachrichtigungen, die an das Amazon-SNS-Thema gesendet werden, werden an alle Amazon-SNS-Konsumenten übermittelt, die dieses Thema abonniert haben. Sie können über die Amazon-SNS-Konsole Änderungen für das Amazon-SNS-Thema ausführen, wie das Hinzufügen oder Entfernen von Konsumentenabonnements für das Thema. Weitere Informationen zum Erstellen und Abonnieren von Amazon-SNS-Themen erhalten Sie unter Erste Schritte mit Amazon Simple Notification Service.

In den folgenden Abschnitten werden alle Kategorien und Ereignisse aufgeführt, zu denen Sie Benachrichtigungen erhalten können. Zudem finden Sie Informationen zum Abonnieren und Verwenden der Amazon-Redshift-Ereignisabonnements.

Anzeigen von Cluster-Ereignissen unter Verwendung der Konsole

So zeigen Sie Ereignisse an:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Events (Ereignisse) aus.

Cluster-Ereignisse mithilfe der Amazon Redshift-API AWS CLI und der Amazon Redshift Redshift-API anzeigen

Sie können zum Anzeigen von Ereignissen die folgende Amazon-Redshift-CLI-Operation verwenden.

- describe-events

Amazon Redshift stellt die folgende API zur Anzeige von Ereignissen bereit.

- DescribeEvents

Verwalten von Cluster-Ereignisbenachrichtigungen

Sie können ein Abonnement für Ereignisbenachrichtigungen mit Amazon Simple Notification Service (Amazon SNS) erstellen, um eine Benachrichtigung zu erhalten, wenn für einen Amazon-Redshift-Cluster, einen Snapshot, eine Sicherheitsgruppe oder eine Parametergruppe ein Ereignis eintritt. Diese Benachrichtigungen werden an ein SNS-Thema gesendet, das seinerseits Meldungen an alle SNS-Nutzer übermittelt, die dieses Thema abonniert haben. Die SNS-Nachrichten an die Verbraucher können in jedem von Amazon SNS für eine AWS Region unterstützten Benachrichtigungsformular erfolgen, z. B. in einer E-Mail, einer Textnachricht oder einem Anruf an einen HTTP-Endpunkt. Zum Beispiel: Alle Regionen unterstützen E-Mail-Benachrichtigungen, SMS-Benachrichtigungen können jedoch nur in USA Ost (Nord-Virginia) erstellt werden. Weitere Informationen finden Sie unter Ereignisbenachrichtigungen zu Amazon Redshift.

Verwalten von Cluster-Ereignisbenachrichtigungen mit der Amazon-Redshift-Konsole

Erstellen eines Ereignisbenachrichtigungsabonnements

So erstellen Sie ein Ereignisabonnement:

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Events (Ereignisse) aus.
3. Wählen Sie die Registerkarte Event subsription (Ereignisabonnement und dann Create event subsription (Ereignisabonnement erstellen) aus.
4. Geben Sie die Eigenschaften Ihres Ereignisabonnements ein (z. B. Name, Quelltyp, Kategorie und Schweregrad). Sie können außerdem Amazon-SNS-Themen aktivieren, um über Ereignisse informiert zu werden.
5. Wählen Sie Create event subscriptions (Ereignisabonnements erstellen) aus, um Ihr Abonnement zu erstellen.

Verwaltung von Cluster-Ereignisbenachrichtigungen mithilfe der AWS CLI und der Amazon Redshift Redshift-API

Sie können zur Verwaltung von Cluster-Ereignisbenachrichtigungen die folgenden Amazon-Redshift-CLI-Operationen verwenden.

- create-event-subscription
- delete-event-subscription
- describe-event-categories
- describe-event-subscriptions
- describe-events
- modify-event-subscription

Sie können zur Verwaltung von Ereignisbenachrichtigungen die folgenden Amazon-Redshift-API-Aktionen verwenden.

- CreateEventSubscription
- DeleteEventSubscription
- DescribeEventCategories
- DescribeEventSubscriptions
- DescribeEvents
- ModifyEventSubscription

Weitere Informationen zu Amazon-Redshift-Ereignisbenachrichtigungen finden Sie unter Ereignisbenachrichtigungen zu Amazon Redshift.

Ereignisbenachrichtigungen zu Amazon Redshift

Amazon-Redshift-Ereigniskategorien und -Ereignismeldungen

Dieser Abschnitt zeigt die Ereignis-IDs und -Kategorien für jeden Amazon-Redshift-Quelltyp.

Die folgende Tabelle zeigt den Ereignistyp sowie eine Liste der Ereignisse für den Fall, dass der Quelltyp „Cluster“ ist.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Konfiguration	REDSHIFT-EREIGNIS-1000	INFO	Die Parametergruppe [Name der Parametergruppe] wurde um [Uhrzeit] aktualisiert. Wenn Sie nur dynamische Parameter geändert haben, werden die zugehörigen Cluster jetzt geändert. Wenn Sie auch statische Parameter geändert haben, werden alle Aktualisierungen, auch die der dynamischen Parameter, installiert, wenn Sie die zugehörigen Cluster neu starten.
Konfiguration	REDSHIFT-EREIGNIS-1001	INFO	Ihr Amazon-Redshift-Cluster [Clustername] wurde zur Verwendung der Parametergruppe [Name der Parametergruppe] um [Uhrzeit] modifiziert.
Konfiguration	REDSHIFT-EREIGNIS-1500	ERROR	Der Amazon VPC [VPC-Name] existiert nicht. Ihre Konfigurationsänderungen für den Cluster [Clustername] wurden nicht angewendet. Korrigieren Sie das Problem in der AWS Management Console .
Konfiguration	REDSHIFT-EREIGNIS-1501	ERROR	Die Kunden-Subnetze [Subnetzname], die Sie für Amazon VPC [VPC-Name] angegeben haben, existieren nicht oder sind ungültig. Ihre Konfigurationsänderungen für den Cluster [Clustername] wurden nicht angewendet. Korrigieren Sie das Problem in der AWS Management Console .
Konfiguration	REDSHIFT-EREIGNIS-1502	ERROR	Subnetze in der Subnetzgruppe [Subnetzgruppenname] haben keine verfügbaren IP-

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
			Adressen. Cluster [Clustername] konnte nicht erstellt werden.
Konfiguration	REDSHIFT-EREIGNIS-1503	ERROR	Der Amazon VPC [VPC-Name] hat kein verbundenes Internet-Gateway. Ihre Konfigurationsänderungen für den Cluster [Clustername] wurden nicht angewendet. Bitte besuchen Sie die AWS Management Console , um das Problem zu beheben.
Konfiguration	REDSHIFT-EREIGNIS-1504	ERROR	Das HSM für den Cluster [Clustername] ist nicht erreichbar.
Konfiguration	REDSHIFT-EREIGNIS-1505	ERROR	Das HSM für den Cluster [Clustername] kann nicht registriert werden. Versuchen Sie es mit einer anderen Konfiguration.
Konfiguration	REDSHIFT-EREIGNIS-1506	ERROR	Amazon Redshift hat den Grenzwert für die Elastic Network-Schnittstelle Ihres Kontos überschritten. Löschen Sie bis zu [maximale Anzahl von Elastic Network Interfaces] Elastic Network Interfaces oder fordern Sie mit EC2 eine Erhöhung des Limits für die Anzahl der Netzwerkschnittstellen pro AWS Region an.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Konfiguration	REDSHIFT-EREIGNIS-1509	ERROR	Der Amazon-Redshift-Cluster [Clustername] kann nicht erstellt werden, da das VPC-Endpunkt-Limit Ihres Kontos erreicht wurde. Löschen Sie nicht verwendete VPC-Endpunkte oder fordern Sie eine Erhöhung des Grenzwerts für VPC-Endpunkte an. Weitere Informationen finden Sie unter VPC-Endpunkte im Amazon-VPC-Benutzerhandbuch.
Konfiguration	REDSHIFT-EVENT-1510	ERROR	Wir haben festgestellt, dass der Versuch, Beispieldaten auf Ihren Amazon-Redshift-Cluster [Clustername] zu laden, nicht erfolgreich war. Um Beispieldaten zu laden, konfigurieren Sie zuerst Ihre VPC so, dass sie Zugriff auf Amazon-S3-Buckets hat, erstellen Sie dann einen neuen Cluster und laden Sie Beispieldaten. Weitere Informationen finden Sie unter Erweitertes VPC-Routing im Amazon-Redshift-Verwaltungsleitfaden.
Konfiguration	REDSHIFT-EVENT-1511	ERROR	Der Amazon-Redshift-Cluster [Clustername] kann nicht erstellt werden, da Sie das Limit Ihres Kontos für elastische IP-Adressen überschritten haben. Löschen Sie ungenutzte elastische IP-Adressen oder fordern Sie eine Limiterhöhung mit Amazon EC2 an.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-2000	INFO	Ihr Amazon-Redshift-Cluster: [Clustername] wurde erstellt und steht zur Verwendung bereit.
Verwaltung	REDSHIFT-EREIGNIS-2001	INFO	Ihr Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] gelöscht. Es [wurde ein / wurde kein] abschließender Snapshot gespeichert.
Verwaltung	REDSHIFT-EREIGNIS-2002	INFO	Die VPC-Sicherheitsgruppen für den Cluster [Clustername] wurden um [Uhrzeit in UTC] aktualisiert.
Verwaltung	REDSHIFT-EREIGNIS-2003	INFO	Die Wartung an Ihrem Cluster [Clustername] hat um [Uhrzeit in UTC] begonnen.
Verwaltung	REDSHIFT-EREIGNIS-2004	INFO	Die Wartung an Ihrem Cluster [Clustername] wurde um [Uhrzeit in UTC] abgeschlossen.
Verwaltung	REDSHIFT-EREIGNIS-2006	INFO	Elastische Größenanpassung für Cluster [Clustername] wurde um [Uhrzeit in UTC] begonnen. Der Cluster befindet sich im schreibgeschützten Modus.
Verwaltung	REDSHIFT-EREIGNIS-2007	INFO	Eine Anfrage zur Größenänderung für den Cluster [Clustername] wurde bestätigt.
Verwaltung	REDSHIFT-EREIGNIS-2008	INFO	Ihre Wiederherstellungsoperation zur Erstellung eines neuen Amazon-Redshift-Cluster-[Clustername] Snapshot [Snapshot-Name] wurde um [Uhrzeit] gestartet. Wechseln Sie zur , um den Fortschritt der Wiederherstellung zu überwachen AWS Management Console.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-2013	INFO	Ihr Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] umbenannt.
Verwaltung	REDSHIFT-EREIGNIS-2014	INFO	Eine Anfrage zur Tabellenwiederherstellung für den Amazon-Redshift-Cluster [Clustername] ist eingegangen.
Verwaltung	REDSHIFT-EREIGNIS-2015	INFO	Die Tabellenwiederherstellung für den Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] abgebrochen.
Verwaltung	REDSHIFT-EREIGNIS-2016	INFO	Der Austausch Ihres Amazon-Redshift-Clusters [Clustername] wurde um [Uhrzeit] begonnen.
Verwaltung	REDSHIFT-EREIGNIS-2017	INFO	Eine vom Kunden initiierte Wartung begann um [Uhrzeit] an Ihrem Amazon-Redshift-Cluster [Clustername]. Während der Wartung ist der Cluster möglicherweise nicht verfügbar.
Verwaltung	REDSHIFT-EREIGNIS-2018	INFO	Eine vom Kunden initiierte Wartung wurde um [Uhrzeit] an Ihrem Amazon-Redshift-Cluster [Clustername] abgeschlossen.
Verwaltung	REDSHIFT-EREIGNIS-2019	ERROR	Eine vom Kunden initiierte Wartung schlug um [Uhrzeit] an Ihrem Amazon-Redshift-Cluster [Clustername] fehl. Der Cluster wird in seinen ursprünglichen Zustand zurück versetzt.
Verwaltung	REDSHIFT-EREIGNIS-2020	INFO	Die Spur Ihres Amazon-Redshift-Clusters [Clustername] wurde von [Ursprüngliche Spur] in [Geänderte Spur] geändert.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-2021	ERROR	Die [Operation] des Amazon-Redshift-Clusters [Name des Clusters] war nicht erfolgreich, während Kapazitäten aus dem Kapazität spool abgerufen wurden. Zurzeit wird zwar am Abruf von Kapazitäten gearbeitet; Ihre Anfrage wurde zunächst jedoch abgebrochen. Löschen Sie dieses Cluster und wiederholen Sie den Vorgang zu einem späteren Zeitpunkt.
Verwaltung	REDSHIFT-EREIGNIS-2022	ERROR	Die [Operation] des Amazon-Redshift-Clusters [Name des Clusters] war nicht erfolgreich, während Kapazitäten aus dem Kapazität spool abgerufen wurden. Zurzeit wird zwar am Abruf von Kapazitäten gearbeitet; Ihre Anfrage wurde zunächst jedoch abgebrochen. In [alternative Availability Zones] sind Kapazitäten verfügbar. Löschen Sie diesen Cluster, und wiederholen Sie den Vorgang in einer alternativen Availability Zone.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-2023	ERROR	Auf Ihrem Amazon-Redshift-Einzelknoten-Cluster [Name des Clusters] wurde ein Hardware-Ausfall entdeckt. Dieser hat möglicherweise zu fehlgeschlagenen Abfragen oder zur Unterbrechung der Verfügbarkeit des Clusters geführt. Das Ersetzen des Clusters war nicht erfolgreich, während Kapazitäten aus dem Kapazitätspool abgerufen wurden. Sie müssen ein neues Cluster aus einem Snapshot wiederherstellen. Löschen Sie dieses Cluster, wählen Sie den letzten verfügbaren Snapshot aus und stellen Sie aus diesem Snapshot ein neues Cluster wieder her. Dieses Cluster wird automatisch auf fehlerfreier Hardware bereitgestellt.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-2024	ERROR	Auf Ihrem Amazon Redshift-Einzelknoten-Cluster [Name des Clusters] wurde ein Hardware-Ausfall entdeckt. Dieser hat möglicherweise zu fehlgeschlagenen Abfragen oder zur Unterbrechung der Verfügbarkeit des Clusters geführt. Das Ersetzen des Clusters war nicht erfolgreich, während Kapazitäten aus dem Kapazitätspool abgerufen wurden. In der Availability Zone [alternative Availability Zones] sind Kapazitäten verfügbar. Löschen Sie dieses Cluster, wählen Sie den letzten verfügbaren Snapshot aus und stellen Sie aus diesem Snapshot ein neues Cluster wieder her. Dieses Cluster wird automatisch auf fehlerfreier Hardware bereitgestellt.
Verwaltung	REDSHIFT-EREIGNIS-3011	INFO	Elastische Größenanpassung für Amazon-Redshift-Cluster '[Clustername]' wurde um [Uhrzeit] begonnen. Datenbankverbindungen bleiben während der Größenanpassung erhalten. Es kann jedoch vorkommen, dass bestimmte Abfragen und Verbindungen während dieses Vorgangs terminiert oder aufgrund einer Zeitüberschreitung abgebrochen werden.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-3012	INFO	Eine Anfrage zur elastischen Größenanpassung für den Cluster '[Clustername]' ist für Start um [Uhrzeit] eingegangen. Wir werden eine Ereignisbenachrichtigungen zusenden, wenn die Größenanpassung durchgeführt wird.
Ausstehend	REDSHIFT-EREIGNIS-2025	INFO	Ihre Datenbank für Ihren Cluster <Clustername> wird zwischen <Startzeit> und <Endzeit> aktualisiert. Ihr Cluster ist in dieser Zeit nicht verfügbar. Planen Sie diese Ausfallzeit ein.
Ausstehend	REDSHIFT-EREIGNIS-2026	INFO	Ihr Cluster <Clustername> wird zwischen <Startzeit> und <Endzeit> aktualisiert. Ihr Cluster ist in dieser Zeit nicht verfügbar. Planen Sie diese Ausfallzeit ein.
Überwachung	REDSHIFT-EREIGNIS-2050	INFO	Auf dem Amazon-Redshift-Cluster [Clustername] wurde ein Hardwarefehler entdeckt. Eine Austauschanfrage wurde um [Uhrzeit] initiiert.
Überwachung	REDSHIFT-EREIGNIS-3000	INFO	Ihr Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] neu gestartet.
Überwachung	REDSHIFT-EREIGNIS-3001	INFO	Ein Knoten auf Ihrem Amazon-Redshift-Cluster: [Clustername] wurde um [Uhrzeit] automatisch ausgetauscht, und Ihr Cluster funktioniert normal.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Überwachung	REDSHIFT-EREIGNIS-3002	INFO	Die Größenanpassung für Ihren Amazon-Redshift-Cluster [Clustername] ist abgeschlossen, und Ihr Cluster ist für Lese- und Schreibvorgänge verfügbar. Die Größenanpassung wurde um [Uhrzeit] initiiert und nahm [Stunden] Stunden in Anspruch.
Überwachung	REDSHIFT-EREIGNIS-3003	INFO	Der Amazon-Redshift-Cluster [Clustername] wurde erfolgreich vom Snapshot [Snapshot name] erstellt und steht zur Verwendung zur Verfügung.
Überwachung	REDSHIFT-EREIGNIS-3007	INFO	Ihr Amazon Redshift Redshift-Snapshot [Snapshot-Name] wurde erfolgreich von [AWS Quellregion] in [AWS Zielregion] zu [Uhrzeit] kopiert.
Überwachen	REDSHIFT-EREIGNIS-3008	INFO	Die Tabellenwiederherstellung für den Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] gestartet.
Überwachung	REDSHIFT-EREIGNIS-3009	INFO	Die Tabellenwiederherstellung für den Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] erfolgreich abgeschlossen.
Überwachung	REDSHIFT-EREIGNIS-3010	ERROR	Die Tabellenwiederherstellung für den Amazon-Redshift-Cluster [Clustername] ist um [Uhrzeit] fehlgeschlagen.
Überwachung	REDSHIFT-EREIGNIS-3013	ERROR	Die angeforderte elastische Größenanpassung für Amazon-Redshift-Cluster [Clustername] schlug um [Zeit] aufgrund von [Grund] fehl.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Überwachung	REDSHIFT-EREIGNIS-3014	INFO	Der Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] neu gestartet.
Überwachung	REDSHIFT-EREIGNIS-3500	ERROR	Die Größenanpassung für Ihren Amazon-Redshift-Cluster [Clustername] ist fehlgeschlagen. Die Größenanpassung wird in einigen Minuten erneut versucht.
Überwachung	REDSHIFT-EREIGNIS-3501	ERROR	Ihre Wiederherstellungsoperation zur Erstellung eines neuen Amazon-Redshift-Clusters [Clustername] von Snapshot [Snapshotname] ist um [Uhrzeit] fehlgeschlagen. Versuchen Sie den Vorgang erneut.
Überwachung	REDSHIFT-EREIGNIS-3504	ERROR	Der Amazon-S3-Bucket [Bucketname] ist für die Protokollierung des Clusters [Clustername] nicht gültig.
Überwachung	REDSHIFT-EREIGNIS-3505	ERROR	Der Amazon-S3-Bucket [Bucketname] verfügt nicht über die korrekten IAM-Richtlinien für den Cluster [Clustername].
Überwachung	REDSHIFT-EREIGNIS-3506	ERROR	Der Amazon-S3-Bucket [Bucketname] existiert nicht. Die Protokollierung für den Cluster [Clustername] kann nicht fortgesetzt werden.
Überwachung	REDSHIFT-EREIGNIS-3507	ERROR	Der Amazon-Redshift-Cluster [Clustername] kann nicht mit EIP [IP-Adresse] erstellt werden. Diese EIP wird bereits verwendet.
Überwachung	REDSHIFT-EREIGNIS-3508	ERROR	Der Amazon-Redshift-Cluster [Clustername] kann nicht mit EIP [IP-Adresse] erstellt werden. Die EIP kann nicht gefunden werden.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Überwachung	REDSHIFT-EREIGNIS-3509	ERROR	Für den Cluster [Clustername] ist die regionenübergreifende Snapshot-Kopie nicht aktiviert.
Überwachung	REDSHIFT-EREIGNIS-3510	ERROR	Der Start der Tabellenwiederherstellung für den Amazon-Redshift-Cluster [Clustername] ist um [Uhrzeit] fehlgeschlagen. Grund: [Grund].
Überwachung	REDSHIFT-EREIGNIS-3511	ERROR	Die Tabellenwiederherstellung für den Amazon-Redshift-Cluster [Clustername] ist um [Uhrzeit] fehlgeschlagen.
Überwachung	REDSHIFT-EREIGNIS-3512	ERROR	Der Amazon-Redshift-Cluster [Clustername] ist aufgrund eines Hardwareproblems ausgefallen. Der Cluster wird automatisch vom letzten Snapshot [Snapshotname] wiederhergestellt, der um [Uhrzeit] erstellt wurde.
Überwachung	REDSHIFT-EREIGNIS-3513	ERROR	Der Amazon-Redshift-Cluster [Clustername] ist aufgrund eines Hardwareproblems ausgefallen. Der Cluster wird automatisch vom letzten Snapshot [Snapshotname] wiederhergestellt, der um [Uhrzeit] erstellt wurde. Alle nach diesem Zeitpunkt vorgenommenen Änderungen an der Datenbank müssen erneut übermittelt werden.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Überwachung	REDSHIFT-EREIGNIS-3514	ERROR	Der Amazon-Redshift-Cluster [Clustername] ist aufgrund eines Hardwareproblems ausgefallen. Der Cluster wird in den Hardware-Fehlerstatus versetzt. Löschen Sie den Cluster, und stellen Sie ihn vom letzten Snapshot [Snapshotname] wieder her, der um [Uhrzeit] erstellt wurde.
Überwachung	REDSHIFT-EREIGNIS-3515	ERROR	Der Amazon-Redshift-Cluster [Clustername] ist aufgrund eines Hardwareproblems ausgefallen. Der Cluster wird in den Hardware-Fehlerstatus versetzt. Löschen Sie den Cluster, und stellen Sie ihn vom letzten Snapshot [Snapshotname] wieder her, der um [Uhrzeit] erstellt wurde. Alle nach diesem Zeitpunkt vorgenommenen Änderungen an der Datenbank müssen erneut übermittelt werden.
Überwachung	REDSHIFT-EREIGNIS-3516	ERROR	Der Amazon-Redshift-Cluster [Clustername] fiel aufgrund eines Hardwarefehlers aus, und es gab keine Backups für den Cluster. Der Cluster wird in den Hardware-Fehlerstatus versetzt und kann gelöscht werden.
Überwachung	REDSHIFT-EREIGNIS-3519	INFO	Der Neustart von Cluster [Clustername] begann um [Uhrzeit].
Überwachung	REDSHIFT-EREIGNIS-3520	INFO	Der Neustart von Cluster [Clustername] wurde um [Uhrzeit] abgeschlossen.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Überwachung	REDSHIFT-EREIGNIS-3521	INFO	Wir haben auf dem Cluster [Clustername] ein Konnektivitätsproblem erkannt. Um [Uhrzeit] wurde eine automatische Diagnoseprüfung initiiert.
Überwachung	REDSHIFT-EREIGNIS-3522	INFO	Die Wiederherstellungsaktion auf [Clustername] schlug um [Uhrzeit] fehl. Das Amazon-Redshift-Team arbeitet an einer Lösung.
Überwachung	REDSHIFT-EREIGNIS-3533	ERROR	Die Größenanpassung für das Cluster [Name des Clusters] wurde um [Uhrzeit] abgebrochen. Die Operation wurde aufgrund von [Grund] abgebrochen. [Maßnahme erforderlich].
Überwachung	REDSHIFT-EREIGNIS-3534	INFO	Die elastische Größenanpassung für Amazon-Redshift-Cluster '[Clustername]' wurde um [Uhrzeit] abgeschlossen. Der Cluster ist jetzt für Lese- und Schreiboperationen verfügbar, während wir die Daten übertragen. Möglicher weise dauern bestimmte Abfragen etwas länger, solange die Datenübertragung noch nicht abgeschlossen ist.
Überwachung	REDSHIFT-EREIGNIS-3537	INFO	Die Datenübertragung des Clusters [Clustername] wurde um [Uhrzeit in UTC] abgeschlossen.
Überwachung	REDSHIFT-EREIGNIS-3600	INFO	Die angeforderte Größenanpassungsoperation für das Amazon-Redshift-Cluster [Name des Clusters] wurde in der Vergangenheit abgebrochen. Das Rollback wurde um [Uhrzeit] abgeschlossen.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Ausstehend	REDSHIFT-EREIGNIS-3601	INFO	Ein Knoten in Ihrem Cluster <Clustername> wird zwischen <Startzeit> und <Endzeit> ersetzt. Diese Wartungsoperation kann nicht aufgeschoben werden. Planen Sie diese Ausfallzeit ein.
Ausstehend	REDSHIFT-EREIGNIS-3602	INFO	Ein Knoten in Ihrem Cluster <Clustername> wird geplant zwischen <Startzeit> und <Endzeit> ersetzt. Ihr Cluster ist in dieser Zeit nicht verfügbar. Planen Sie diese Ausfallzeit ein.
Verwaltung	REDSHIFT-EREIGNIS-3603	INFO	Die Wiederherstellungsoperation zur Erstellung des Clusters [Clustername] von Snapshot [Snapshotname] ist aufgrund eines internen Fehlers fehlgeschlagen. Der Cluster wird in den Status der inkompatiblen Wiederherstellung versetzt und kann gelöscht werden. Versuchen Sie, den Snapshot in einem Cluster mit einer anderen Konfiguration wiederherzustellen.
Verwaltung	REDSHIFT-EREIGNIS-3614	INFO	Die geplante Aktion [Name der geplanten Aktion] wurde zum [Zeitpunkt in UTC] erstellt. Der erste Aufruf wird für [Zeit in UTC] geplant.
Verwaltung	REDSHIFT-EREIGNIS-3615	INFO	Die geplante Aktion [Name der geplanten Aktion] ist für [Zeit in UTC] geplant.
Überwachung	REDSHIFT-EREIGNIS-3616	INFO	Die geplante Aktion [Name der geplanten Aktion] zum [Zeitpunkt in UTC] wurde mit dem Status ‚SUCCEEDED‘ (ERFOLGREICH) abgeschlossen.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Überwachung	REDSHIFT-EREIGNIS-3617	ERROR	Die geplante Aktion [Name der geplanten Aktion] wurde zum [Zeitpunkt in UTC] aufgrund einer Verzögerung übersprungen.
Überwachung	REDSHIFT-EREIGNIS-3618	INFO	Der Vorgang zum Anhalten des Clusters [Clustername] hat um [UTC-Zeit] begonnen. Anhalten gestartet
Überwachung	REDSHIFT-EREIGNIS-3619	INFO	Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit UTC] erfolgreich angehalten.
Verwaltung	REDSHIFT-EREIGNIS-3626	INFO	Die geplante Aktion[Name der geplanten Aktion] wurde zum [Zeitpunkt in UTC] geändert. Der erste Aufruf wird für [Zeit in UTC] geplant.
Verwaltung	REDSHIFT-EREIGNIS-3627	INFO	Die geplante Aktion [Name der geplanten Aktion] wurde zum [Zeitpunkt in UTC] gelöscht.
Überwachung	REDSHIFT-EREIGNIS-3628	ERROR	Die geplante Aktion [Name der geplanten Aktion] zum [Zeitpunkt in UTC] wurde mit dem Status ‚FAILED‘ (FEHLGESCHLAGEN) abgeschlossen.
Verwaltung	REDSHIFT-EREIGNIS-3629	INFO	Amazon Redshift [Clustername] hat Ihre Verschiebungsanforderung erhalten. Wenn die Verschiebung der Availability Zone abgeschlossen ist, sendet Amazon Redshift eine Ereignisbenachrichtigung.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-3630	INFO	Amazon-Redshift-Cluster [Clustername] wurde erfolgreich von [Availability Zone] in [Availability Zone] verschoben. Sie können den Cluster jetzt verwenden.
Verwaltung	REDSHIFT-EREIGNIS-3631	INFO	Amazon Redshift hat Ihren Amazon-Redshift-Cluster [Clustername] für die Wiederherstellung erfolgreich von [Availability Zone] in [Availability Zone] verschoben.
Verwaltung	REDSHIFT-EREIGNIS-3632	INFO	Amazon Redshift hat aufgrund von Konfigurationsänderungen die Clusterverschiebung für Ihren Amazon-Redshift-Cluster [Clustername] vorübergehend deaktiviert. Versuchen Sie später erneut die Clusterverschiebung.
Überwachen	REDSHIFT-EVENT-3658	ERROR	Die Migration von EC2-Classic zu EC2-VPC ist für Redshift-Cluster [Cluster-ID] fehlgeschlagen.
Überwachung	REDSHIFT-EVENT-3659	INFO	Die Migration von EC2-Classic zu EC2-VPC war für Redshift-Cluster [Cluster-ID] erfolgreich.
Überwachung	REDSHIFT-EVENT-3660	INFO	Der Cluster wird in den Hardware-Fehlerstatus versetzt. Löschen Sie den EC2-Classic-Cluster und stellen Sie ihn vom letzten Snapshot [Snapshot-Name] der um [Uhrzeit in UTC] erstellt wurde, zu einem EC2-VPC-Cluster wieder her.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-3666	INFO	Der Amazon Redshift Multi-AZ-Cluster [Clustername] hat zu [Uhrzeit in UTC] einen Fehler erkannt und eine automatische Wiederherstellung ausgelöst.
Verwaltung	REDSHIFT-EREIGNIS-3667	INFO	Der Amazon Redshift Multi-AZ-Cluster [Clustername] wurde erfolgreich zum [Zeitpunkt in UTC] wiederhergestellt und ist für die Verwendung in der [ersten Verfügbarkeitszone] verfügbar. Sekundäre Rechenleistung in einer anderen AZ wird in Kürze verfügbar sein.
Überwachen	REDSHIFT-EVENT-3668	ERROR	Der Amazon Redshift Multi-AZ-Cluster [Clustername] konnte zu [Uhrzeit in UTC] nicht wiederhergestellt werden.
Verwaltung	REDSHIFT-EREIGNIS-3669	INFO	Der Amazon Redshift Multi-AZ-Cluster [Clustername] wurde erfolgreich zu [Uhrzeit in UTC] wiederhergestellt und ist für die Verwendung mit Rechenressourcen sowohl aus der [ersten Verfügbarkeitszone] als auch aus der [zweiten Verfügbarkeitszone] verfügbar.
Verwaltung	REDSHIFT-EVENT-3670	INFO	Die Wartung des Amazon Redshift Redshift-Clusters [Clustername] wurde um [Uhrzeit in UTC] abgeschlossen und ist für die Verwendung mit Rechenressourcen in [erster Verfügbarkeitszone] verfügbar. Sekundäre Rechenleistung in einer anderen AZ wird in Kürze verfügbar sein.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EVENT-3671	INFO	Die Größenänderung auf dem Amazon Redshift Redshift-Cluster [Clustername] wurde um [Uhrzeit in UTC] abgeschlossen und ist für die Verwendung in [erster Verfügbarkeitszone] verfügbar. Sekundäre Rechenleistung in einer anderen AZ wird in Kürze verfügbar sein.
Verwaltung	REDSHIFT-EVENT-3672	INFO	Der Amazon Redshift Multi-AZ-Cluster [Clustername] hat zu [Uhrzeit in UTC] einen Fehler in der [zweiten Verfügbarkeitszone] erkannt und eine automatische Wiederherstellung ausgelöst.
Verwaltung	REDSHIFT-EREIGNIS-3673	INFO	Der Vorgang zur Aktivierung von Multi-AZ für den Amazon Redshift Redshift-Cluster [Clustername] wurde um [Uhrzeit in UTC] gestartet.
Verwaltung	REDSHIFT-EREIGNIS-3674	INFO	Der Vorgang zur Aktivierung von Multi-AZ für den Amazon Redshift Redshift-Cluster [Clustername] wurde um [Uhrzeit in UTC] erfolgreich abgeschlossen.
Überwachen	REDSHIFT-EREIGNIS-3675	ERROR	Der Vorgang zur Aktivierung von Multi-AZ für den Amazon Redshift Redshift-Cluster [Clustername] ist um [Uhrzeit in UTC] fehlgeschlagen.
Verwaltung	REDSHIFT-EREIGNIS-3676	INFO	Der Vorgang zur Deaktivierung von Multi-AZ für Ihren Amazon Redshift Multi-AZ-Cluster [Clustername] wurde um [Uhrzeit in UTC] gestartet.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-3677	INFO	Der Vorgang zur Deaktivierung von Multi-AZ für Ihren Amazon Redshift Redshift-Cluster [Clustername] wurde um [Uhrzeit in UTC] erfolgreich abgeschlossen.
Überwachen	REDSHIFT-EREIGNIS-3678	ERROR	Der Vorgang zur Deaktivierung von Multi-AZ für Ihren Amazon Redshift Redshift-Cluster [Clustername] ist um [Uhrzeit in UTC] fehlgeschlagen.
Konfiguration	REDSHIFT-EREIGNIS-3679	INFO	Der Port des Amazon Redshift Redshift-Clusters [Clustername] wurde erfolgreich geändert.
Konfiguration	REDSHIFT-EREIGNIS-3680	ERROR	Amazon Redshift konnte den Cluster [Clustername] nicht erstellen, da auf die für diesen Vorgang erforderliche verknüpfte Service-Rolle (SLR) nicht zugegriffen werden kann. Versuchen Sie die Erstellung erneut über die Amazon-Redshift-Konsole. Amazon Redshift erstellt die SLR automatisch.
Überwachen	REDSHIFT-EREIGNIS-3684	ERROR	Ihr Amazon S3 S3-Bucket [Bucket-Name] wurde mit einem unbekannten oder unzugänglichen AWS KMS Schlüssel verschlüsselt. Ändern Sie die Verschlüsselung Ihres Amazon-S3-Buckets.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EVENT-3685	ERROR	Der Wiederherstellungsvorgang auf dem Cluster [Clustername] ist fehlgeschlagen, da nicht genügend Festplattenspeicher verfügbar ist. Der Vorgang wird rückgängig gemacht. Versuchen Sie, die Wiederherstellung auf einem Cluster mit einer anderen Konfiguration durchzuführen.
Verwaltung	REDSHIFT-EVENT-3686	ERROR	Die Größenänderung auf dem Cluster [Clustername] ist fehlgeschlagen, da nicht genügend Festplattenspeicher verfügbar ist. Der Vorgang wird rückgängig gemacht. Versuchen Sie, die Größe auf einen Cluster mit einer anderen Konfiguration zu ändern.
Sicherheit	REDSHIFT-EREIGNIS-4000	INFO	Ihre Admin-Anmeldeinformationen für Ihren Amazon-Redshift-Cluster [Cluster-Name] wurden um [Uhrzeit] aktualisiert.
Sicherheit	REDSHIFT-EREIGNIS-4001	INFO	Die Sicherheitsgruppe [Name der Sicherheitsgruppe] wurde um [Uhrzeit] modifiziert. Die Änderungen werden für alle verbundenen Cluster automatisch durchgeführt.
Sicherheit	REDSHIFT-EREIGNIS-4500	ERROR	Die von Ihnen angegebene Sicherheitsgruppe [Name der Sicherheitsgruppe] ist nicht gültig. Ihre Konfigurationsänderungen für den Cluster [Clustername] wurden nicht angewendet. Bitte besuchen Sie die AWS Management Console , um das Problem zu beheben.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Sicherheit	REDSHIFT-EREIGNIS-4501	ERROR	Die Sicherheitsgruppe [Name der Sicherheitsgruppe], die in der Cluster-Sicherheitsgruppe [Name der Cluster-Sicherheitsgruppe] angegeben wurde, konnte nicht gefunden werden. Die Autorisierung konnte nicht abgeschlossen werden.
Sicherheit	REDSHIFT-EREIGNIS-4502	ERROR	Die Admin-Anmeldeinformationen für Amazon-Redshift-Cluster [Cluster-Name] konnten um [Uhrzeit] aufgrund gleichzeitiger Aktivitäten nicht aktualisiert werden. Warten Sie, bis der aktuelle Workload abgeschlossen, ist, oder reduzieren Sie den aktiven Workload und wiederholen Sie den Vorgang.
Sicherheit	REDSHIFT-EVENT-4503	ERROR	Amazon Redshift kann nicht auf das Secret für Ihren Cluster [Cluster-Name] zugreifen.
Sicherheit	REDSHIFT-EVENT-4504	ERROR	Amazon Redshift kann nicht auf den KMS-Schlüssel [KMS-Schlüssel] zugreifen, der zur Verschlüsselung des Secrets für die Administratoranmeldeinformationen für Ihren Cluster [Cluster-Name] verwendet wurde.
Sicherheit	REDSHIFT-EVENT-4505	ERROR	Amazon Redshift kann das Secret für Ihren Cluster [Cluster-Name] aufgrund einer laufenden Operation auf dem Cluster nicht rotieren.
Sicherheit	REDSHIFT-EVENT-4506	ERROR	Ihr Amazon-Redshift-Cluster [Cluster-Name] wurde angehalten. Amazon Redshift kann die Secrets von angehaltenen Clustern nicht rotieren.

Die folgende Tabelle zeigt den Ereignistyp sowie eine Liste der Ereignisse für den Fall, dass der Quelltyp „Parametergruppe“ ist.

Kategorien und Ereignisse für den Quelltyp „Parametergruppe

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Konfiguration	REDSHIFT-EREIGNIS-1002	INFO	Der Parameter [Parametername] wurde um [Uhrzeit] von [Wert] zu [Wert] aktualisiert.
Konfiguration	REDSHIFT-EREIGNIS-1003	INFO	Die Cluster-Parametergruppe [Name der Gruppe] wurde erstellt.
Konfiguration	REDSHIFT-EREIGNIS-1004	INFO	Die Cluster-Parametergruppe [Name der Gruppe] wurde gelöscht.
Konfiguration	REDSHIFT-EREIGNIS-1005	INFO	Die Cluster-Parametergruppe [Name der Gruppe] wurde um [Uhrzeit] aktualisiert. Wenn Sie nur dynamische Parameter geändert haben, werden die zugehörigen Cluster jetzt geändert. Wenn Sie auch statische Parameter geändert haben, werden alle Aktualisierungen, auch die der dynamischen Parameter, installiert, wenn Sie die zugehörigen Cluster neu starten.

Die folgende Tabelle zeigt den Ereignistyp sowie eine Liste der Ereignisse für den Fall, dass der Quelltyp „Sicherheitsgruppe“ ist.

Kategorien und Ereignisse für den Quelltyp „Sicherheitsgruppe

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Sicherheit	REDSHIFT-EREIGNIS-4002	INFO	Die Cluster-Sicherheitsgruppe [Name der Gruppe] wurde erstellt.
Sicherheit	REDSHIFT-EREIGNIS-4003	INFO	Die Cluster-Sicherheitsgruppe [Name der Gruppe] wurde gelöscht.
Sicherheit	REDSHIFT-EREIGNIS-4004	INFO	Die Cluster-Sicherheitsgruppe [Name der Gruppe] wurde um [Uhrzeit] geändert. Die Änderungen werden automatisch an allen verbundenen Clustern vorgenommen.

Die folgende Tabelle zeigt den Ereignistyp sowie eine Liste der Ereignisse für den Fall, dass der Quelltyp „Snapshot“ ist.

Kategorien und Ereignisse für den Quelltyp „Snapshot

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-2009	INFO	Ein Benutzer-Snapshot [Snapshotname] für den Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] gestartet. Wechseln Sie zur , um den Fortschritt des Snapshots zu überwachen AWS Management Console.
Verwaltung	REDSHIFT-EREIGNIS-2010	INFO	Der Benutzer-Snapshot [Snapshot name] für Ihren Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] abgebrochen.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Verwaltung	REDSHIFT-EREIGNIS-2011	INFO	Der Benutzer-Snapshot [Snapshotname] für den Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] gelöscht.
Verwaltung	REDSHIFT-EREIGNIS-2012	INFO	Der abschließende Snapshot [Snapshot name] für den Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] gestartet.
Überwachung	REDSHIFT-EREIGNIS-3004	INFO	Der Benutzer-Snapshot [Snapshot name] für Ihren Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] erfolgreich abgeschlossen.
Überwachung	REDSHIFT-EREIGNIS-3005	INFO	Der abschließende Snapshot [Snapshot name] für den Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] erfolgreich abgeschlossen.
Überwachung	REDSHIFT-EREIGNIS-3006	INFO	Der abschließende Snapshot [Snapshot name] für den Amazon-Redshift-Cluster [Clustername] wurde um [Uhrzeit] abgebrochen.
Überwachung	REDSHIFT-EREIGNIS-3502	ERROR	Der abschließende Snapshot [Snapshot name] für den Amazon-Redshift-Cluster [Clustername] schlug um [Uhrzeit] fehl. Das Team untersucht dieses Problem. Bitte besuchen Sie die AWS Management Console , um den Vorgang erneut zu versuchen.

Amazon-Redshift-Kategorie	Ereignis-ID	Schweregrad des Ereignisses	Beschreibung
Überwachen	REDSHIFT-EREIGNIS-3503	ERROR	Der Benutzer-Snapshot [Snapshot name] für Ihren Amazon-Redshift-Cluster [Clustername] schlug um [Uhrzeit] fehl. Das Team untersucht dieses Problem. Bitte besuchen Sie die AWS Management Console , um den Vorgang erneut zu versuchen.

Ereignisbenachrichtigungen von Amazon Redshift Serverless mit Amazon EventBridge

Amazon Redshift Serverless verwendet Amazon EventBridge zur Verwaltung von Ereignisbenachrichtigungen, um Sie in up-to-date Bezug auf Änderungen in Ihrem Data Warehouse zu halten. Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus verschiedenen Quellen verbinden können. In diesem Fall ist die Ereignisquelle Amazon Redshift. Ereignisse, bei denen es sich um überwachte Änderungen in einer Umgebung handelt, werden automatisch EventBridge von Ihrem Amazon Redshift Data Warehouse an gesendet. Ereignisse werden nahezu in Echtzeit übermittelt.

Zu den Funktionen von EventBridge gehört die Bereitstellung einer Umgebung, in der Sie Ereignisregeln schreiben können, die Aktionen angeben können, die für bestimmte Ereignisse ausgeführt werden sollen. Sie können auch Ziele einrichten, bei denen es sich um Ressourcen handelt, an die ein Ereignis gesendet werden EventBridge kann. Ein Ziel kann ein API-Ziel, eine Amazon- CloudWatch Protokollgruppe und andere enthalten. Weitere Informationen zu -Regeln finden Sie unter Amazon- EventBridge Regeln. Weitere Informationen zu Zielen finden Sie unter Amazon- EventBridge Ziele.

Ereignisse können in Schweregrade und Kategorien eingeteilt werden. Die folgenden Filter sind verfügbar:

- Ressourcen-Filterung – Empfangen Sie Nachrichten basierend auf der Ressource, mit der die Ereignisse verknüpft sind. Zu den Ressourcen gehören eine Arbeitsgruppe, ein Snapshot usw.

- Zeitfenster-Filterung – Erfassen Sie Ereignisse in einem bestimmten Zeitraum.
- Kategorie-Filterung – Erhalten Sie Ereignisbenachrichtigungen für alle Ereignisse in bestimmten Kategorien.

Die folgende Tabelle enthält Ereignisse von Amazon Redshift Serverless mit zusätzlichen Metadaten:

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
RateChange	REDSHIFT-SERVERLESS-EVENT-1001	INFO	Änderung der Arbeitsgruppen-Basis-RPU wurde um <Uhrzeit in UTC> erfolgreich abgeschlossen.
RateChange	REDSHIFT-SERVERLESS-EVENT-1002	ERROR	Die Änderung der Arbeitsgruppen-Basis-RPU konnte um <Uhrzeit in UTC> nicht abgeschlossen werden.
Überwachen	REDSHIFT-SERVERLESS-EVENT-1003	INFO	Die Software wurde auf Ihrem Amazon Redshift Data Warehouse <Endpunktname> um <Uhrzeit in UTC> aktualisiert.
Konfiguration	REDSHIFT-SERVERLESS-EREIGNIS-1011	ERROR	Amazon Redshift Serverless konnte die Arbeitsgruppe [Name der Arbeitsgr

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
			uppe] nicht erstellen, da auf die für diesen Vorgang erforderliche verknüpfte Service-Rolle (SLR) nicht zugegriffen werden kann. Versuchen Sie die Erstellung erneut auf der Amazon-Redshift-Konsole. Amazon Redshift erstellt die SLR automatisch.
Überwachen	REDSHIFT-SERVERLESS-EVENT-1500	ERROR	Die Arbeitsgruppe <Name der Arbeitsgruppe> kann nicht erstellt oder aktualisiert werden, da Sie das Limit Ihres Kontos für elastische IP-Adressen überschritten haben. Löschen Sie ungenutzte elastische IP-Adressen oder fordern Sie eine Limiterhöhung mit Amazon EC2 an.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Überwachen	REDSHIFT-SERVERLESS-EVENT-1501	ERROR	Subnetz <Subnetz-ID> hat keine verfügbaren IP-Adressen. Dies verhindert, dass die folgenden Abfragetypen erfolgreich auf Arbeitsgruppe <Arbeitsgruppenname> ausgeführt werden: EMR, gleichzeitige Abfragen, COPY/UNLOAD von Amazon EC2. Um das Problem zu beheben, geben Sie IPs in Ihrem Subnetz frei, indem Sie ENIs löschen.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Überwachen	REDSHIFT-SERVERLESS-EVENT-1502	ERROR	Subnetz <Subnetz-ID> hat keine verfügbaren IP-Adressen. Dadurch wird verhindert, dass die Abfragetypen Amazon EMR, gleichzeitige Redshift-Abfragen, Redshift COPY/UNLOAD und Redshift ML erfolgreich in der Arbeitsgruppe <Name der Arbeitsgruppe> ausgeführt werden. Um das Problem zu beheben, geben Sie IPs in Ihrem Subnetz frei, indem Sie ungenutzte Elastic-Network-Schnittstellen (ENIs) löschen.
Verwaltung	REDSHIFT-SERVERLESS-EVENT-1008	INFO	Ihre Amazon-Redshift-Arbeitsgruppe <Arbeitsgruppenname> wurde erstellt und ist einsatzbereit.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Verwaltung	REDSHIFT-SERVERLESS-EVENT-1009	INFO	Ihre Amazon-Redshift-Arbeitsgruppe <Arbeitsgruppenname> wurde um <Uhrzeit in UTC> gelöscht.
Überwachen	REDSHIFT-SERVERLESS-EVENT-1000	INFO	Snapshot <Snapshot-Name> wurde um <Zeit in UTC> erfolgreich abgeschlossen.
Verwaltung	REDSHIFT-SERVERLESS-EVENT-1004	INFO	Die Wiederherstellung aus dem Snapshot auf Namespace <Namespace-Name> wurde um <Uhrzeit in UTC> erfolgreich abgeschlossen.
Verwaltung	REDSHIFT-SERVERLESS-EVENT-1005	ERROR	Die Wiederherstellung aus dem Snapshot auf Namespace <Namespace-Name> ist um <Uhrzeit in UTC> fehlgeschlagen.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Verwaltung	REDSHIFT-SERVERLESS-EVENT-1006	INFO	Die Wiederherstellung vom Wiederherstellungspunkt auf Namespace <Namespace-Name> wurde um <Uhrzeit in UTC> erfolgreich abgeschlossen.
Verwaltung	REDSHIFT-SERVERLESS-EVENT-1007	INFO	Die Wiederherstellung vom Wiederherstellungspunkt auf Namespace <Namespace-Name> ist um <Uhrzeit in UTC> fehlgeschlagen.
Sicherheit	REDSHIFT-SERVERLESS-EREIGNIS-1012	ERROR	Amazon Redshift kann nicht auf das Secret für Ihren Namespace <namespace name> zugreifen.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Sicherheit	REDSHIFT-SERVERLESS-EREIGNIS-1013	ERROR	Amazon Redshift kann nicht auf den KMS-Schlüssel zugreifen, der zur Verschlüsselung des Secrets mit den Administratoranmeldeinformationen für Ihren Namespace <namespace name> verwendet wurde.
Sicherheit	REDSHIFT-SERVERLESS-EREIGNIS-1014	ERROR	Amazon Redshift kann das Secret für Ihren Namespace <namespace name> aufgrund einer Operation, die für Ihre Arbeitsgruppe ausgeführt wird, nicht rotieren.
Sicherheit	REDSHIFT-SERVERLESS-EREIGNIS-1015	ERROR	Ihrem Namespace <namespace name> ist keine Arbeitsgruppe angefügt. Amazon Redshift kann nur Secrets für Namespaces rotieren, denen Arbeitsgruppen angefügt sind.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Sicherheit	REDSHIFT-SERVERLESS-EREIGNIS-1016	INFO	Die Administratoranmeldeinformationen für Ihren Namespace <namespace name> wurden um <time in UTC> aktualisiert.

Ereignisbenachrichtigungen zur Null-ETL-Integration mit Amazon EventBridge

Die Null-ETL-Integration verwendet Amazon EventBridge , um Ereignisbenachrichtigungen zu verwalten, um Sie up-to-date über Änderungen an Ihren Integrationen zu informieren. Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus verschiedenen Quellen verbinden können. In diesem Fall ist die Ereignisquelle Amazon Redshift. Ereignisse, bei denen es sich um überwachte Änderungen in einer Umgebung handelt, werden automatisch EventBridge von Ihrem Amazon Redshift Data Warehouse an gesendet. Ereignisse werden nahezu in Echtzeit übermittelt.

EventBridge bietet eine Umgebung, in der Sie Ereignisregeln schreiben können, die Aktionen angeben können, die für bestimmte Ereignisse ausgeführt werden sollen. Sie können auch Ziele einrichten, bei denen es sich um Ressourcen handelt, an die ein Ereignis gesendet werden EventBridge kann. Ein Ziel kann ein API-Ziel, eine Amazon- CloudWatch Protokollgruppe und andere enthalten. Weitere Informationen zu -Regeln finden Sie unter Amazon- EventBridge Regeln. Weitere Informationen zu Zielen finden Sie unter Amazon- EventBridge Ziele.

Ereignisse können in Schweregrade und Kategorien eingeteilt werden. Die folgenden Filter sind verfügbar:

- Ressourcen-Filterung – Empfangen Sie Nachrichten basierend auf der Ressource, mit der die Ereignisse verknüpft sind. Zu den Ressourcen gehören eine Arbeitsgruppe oder ein Snapshot.

- Zeitfenster-Filterung – Erfassen Sie Ereignisse in einem bestimmten Zeitraum.
- Kategorie-Filterung – Erhalten Sie Ereignisbenachrichtigungen für alle Ereignisse in bestimmten Kategorien.

Die folgende Tabelle enthält Ereignisse der Null-ETL-Integration mit zusätzlichen Metadaten:

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Überwachen	REDSHIFT-INTEGRATION-EVENT-0000	INFO	Die Null-ETL-Integration <Integrationsname> wurde erstellt und ist jetzt AKTIV.
Überwachen	REDSHIFT-INTEGRATION-EVENT-0001	INFO	Die Null-ETL-Integration <Integrationsname> wurde um <Zeit in UTC> gelöscht.
Überwachen	REDSHIFT-INTEGRATION-EVENT-0002	INFO	Die Löschung der Null-ETL-Integration <Integrationsname> wurde um <Zeit in UTC> eingeleitet.
Überwachen	REDSHIFT-INTEGRATION-EVENT-0003	INFO	Die Null-ETL-Integration <Integrationsname>synchronisiert Transaktionsdaten mit dem Ziel-Data-Warehouse.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Überwachen	REDSHIFT-INTEGRATION-EVENT-0004	WARNING	Eine oder mehrere Tabellen haben keinen Primärschlüssel und können nicht synchronisiert werden. Erstellen Sie ein Backup auf Amazon RDS, löschen Sie diese Tabellen und erstellen Sie sie erneut unter Beachtung der bewährten Methoden von Amazon Redshift für das Entwerfen von Tabellen.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Überwachen	REDSHIFT-INTEGRATION-EVENT-0005	WARNING	Eine oder mehrere Tabellen können nicht synchronisiert werden, da sie nicht unterstützte Datentypen oder -längen enthalten. Korrigieren Sie die Tabellen und versuchen Sie es erneut. Weitere Informationen zu nicht unterstützten Datentypen finden Sie unter Nicht unterstützte Datentypen.
Überwachen	REDSHIFT-INTEGRATION-EVENT-0006	ERROR	Die Integration konnte nicht erstellt werden. Löschen Sie die Integration und erstellen Sie sie erneut.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Überwachen	REDSHIFT-INTEGRATION-EVENT-0007	ERROR	Aufgrund eines internen Fehlers können keine Daten geladen werden. Löschen Sie die Integration und erstellen Sie sie erneut.
Überwachen	REDSHIFT-INTEGRATION-EVENT-0008	ERROR	Die Autorisierung ist fehlgeschlagen, da dem Aurora-DB-Quell-Cluster die Berechtigungen entzogen wurden. Löschen Sie die Integration und erstellen Sie sie erneut.
Überwachen	REDSHIFT-INTEGRATION-EVENT-0009	ERROR	Es können keine Daten an Amazon Redshift gesendet werden, da die Anzahl der Tabellen und Schemas das Amazon-Redshift-Limit überschreitet. Löschen Sie die Integration und erstellen Sie sie erneut.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Überwachen	REDSHIFT-INTEGRATION-EVENT-0012	ERROR	Auf dem Ziel-Serverless-Namespace wurde eine Wiederherstellung vom Wiederherstellungspunkt aus aufgerufen. Löschen Sie die Integration und erstellen Sie sie erneut.
Überwachen	REDSHIFT-INTEGRATION-EVENT-0013	INFO	Die Null-ETL-Integration <Integrationsname> ist jetzt AKTIV.
Überwachen	REDSHIFT-INTEGRATION-EVENT-0014	ERROR	Die Integration <Integrationsname> ist fehlgeschlagen, da sie aufgrund eines internen Fehlers nicht geändert werden konnte. Löschen Sie die Integration und erstellen Sie sie erneut. Wenn das Problem weiterhin besteht, wenden Sie sich bitte an den AWS-Support.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Operation	REDSHIFT-INTEGRATION-EVENT-0015	INFO	Eine DDL-Änderung <DDL-Änderung> wurde auf die Tabelle <schema.name> angewendet.
Operation	REDSHIFT-INTEGRATION-EVENT-0016	INFO	Ihre Null-ETL-Integration <Integrationsname> verarbeitet eine Änderungsanforderung mit den folgenden Argumenten: <Kopie der Anforderungsargumente>.
Operation	REDSHIFT-INTEGRATION-EVENT-0017	INFO	Ihre Änderung an der Null-ETL-Integration <Integrationsname> wurde angewendet.
Operation	REDSHIFT-INTEGRATION-EVENT-0018	WARNING	Der Amazon-Redshift-Ziel-Cluster wird angehalten. Warten Sie, bis der Cluster angehalten wurde, und setzen Sie dann den Betrieb des Clusters fort, um mit dem Streamen von Daten fortzufahren.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Operation	REDSHIFT-INTEGRATION-EVENT-0019	WARNING	Der Amazon-Redshift-Ziel-Cluster wird angehalten. Setzen Sie den Betrieb des Clusters fort, um mit dem Daten-Streaming fortzufahren.
Operation	REDSHIFT-INTEGRATION-EVENT-0020	WARNING	Der Betrieb des Amazon-Redshift-Ziel-Clusters wird fortgesetzt. Warten Sie, bis der Cluster aktiv ist, um mit dem Streamen von Daten fortzufahren.
Konfiguration	REDSHIFT-INTEGRATION-EVENT-1000	ERROR	Ein oder mehrere Parameter auf dem Aurora-DB-Quell-Cluster sind falsch konfiguriert. Korrigieren Sie die Parametergruppe und starten Sie den Cluster neu, um die Änderungen anzuwenden. Erstellen Sie anschließend die Integration erneut.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Konfiguration	REDSHIFT-INTEGRATION-EVENT-1001	ERROR	Die Integration ist fehlgeschlagen, da der Wert des Parameters enable_case_sensitive_identifier falsch ist. Setzen Sie den Wert für den Aurora-DB-Quell-Cluster auf „true“, löschen Sie anschließend die Integration und erstellen Sie sie erneut.
Konfiguration	REDSHIFT-INTEGRATION-EVENT-1002	ERROR	Die Integration ist fehlgeschlagen, da der Wert des Parameters cdc_insert_enabled falsch ist. Setzen Sie den Wert für den Aurora-DB-Quell-Cluster auf „true“, löschen Sie anschließend die Integration und erstellen Sie sie erneut.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Konfiguration	REDSHIFT-INTEGRATION-EVENT-1003	ERROR	Der Parameter binlog_format in der Quell-DB-Cluster-Parametergruppe muss auf ROW gesetzt sein. Korrigieren Sie die Parametergruppe und starten Sie den Cluster neu, um die Änderung anzuwenden. Erstellen Sie anschließend die Integration erneut.
Konfiguration	REDSHIFT-INTEGRATION-EVENT-1004	ERROR	Daten konnten nicht geladen werden, da der Cluster-Parameter binlog_transaction_compression aktiviert ist. Setzen Sie den Parameterwert auf OFF und starten Sie die Writer-Instance neu, um die Änderung anzuwenden. Erstellen Sie anschließend die Integration erneut.

Amazon-Redshift-Kategorie	Externe Ereignis-ID	Schweregrad des Ereignisses	Beschreibung der Nachricht
Konfiguration	REDSHIFT-INTEGRATION-EVENT-1005	ERROR	Daten konnten nicht geladen werden, da der Cluster-Parameter binlog_row_value_options auf PARTIAL_JSON gesetzt ist, was nicht unterstützt wird. Korrigieren Sie die Parametergruppe und starten Sie die Writer-Instance neu, um die Änderung anzuwenden. Erstellen Sie anschließend die Integration erneut.
Konfiguration	REDSHIFT-INTEGRATION-EVENT-1006	WARNING	Der Integrationsfilter kann nicht analysiert werden. Korrigieren Sie die Filtersyntax.

Kontingente und Limits in Amazon Redshift

Amazon Redshift verfügt über Kontingente, die die Nutzung mehrerer Ressourcen in Ihrem AWS Konto pro AWS Region einschränken. Es gibt einen Standardwert für jedes Kontingent. Einige Kontingente sind anpassbar. Für anpassbare Kontingente können Sie eine Erhöhung für Ihr AWS Konto in einer - AWS Region beantragen, indem Sie ein Formular zur Erhöhung des Amazon-Redshift-Limits einreichen.

Kontingente für Amazon-Redshift-Objekte

Amazon Redshift verfügt über Kontingente, die die Verwendung verschiedener Objekttypen einschränken. Es gibt jeweils einen Standardwert.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
AWS -Konten, die Sie zur Wiederherstellung eines Snapshots pro Snapshot autorisieren können	20	Nein	Die maximale Anzahl von AWS Konten, die Sie pro Snapshot zur Wiederherstellung eines Snapshots autorisieren können.
AWS -Konten, die Sie zur Wiederherstellung eines Snapshots	100	Nein	Die maximale Anzahl von AWS Konten, die Sie pro KMS-Schlüssel zur Wiederherstellung eines Snapshots autorisieren können. Wenn Sie 10 Snapshots haben, die mit einem einzigen KMS-Schlüssel verschlüsselt sind, können Sie also 10 AWS -Konten autorisieren, jeden Snapshot wiederherzustellen, oder andere Kombinationen, die in Summe

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
pro autorisieren können AWS KMS key			100 Konten ergeben und 20 Konten für jeden Snapshot nicht übersteigen.
Cluster-IAM-Rollen für Amazon Redshift für den Zugriff auf andere - AWS Services	50[1]	Nein	Die maximale Anzahl von IAM-Rollen, die Sie einem Cluster zuordnen können, um Amazon Redshift für den Zugriff auf andere - AWS Services für den Benutzer zu autorisieren, der Eigentümer des Clusters und der IAM-Rollen ist. [1]Das Kontingent beträgt 10 in den folgenden AWS-Regionen: us-iso-east-1, us-iso-west-1, us-isob-east-1.
Nebenläufigkeitsstufe (Abfrageslots) für alle benutzerdefinierten manuellen WLM-Warteschlangen	50	Nein	Die maximalen Abfrageslots für alle benutzerdefinierten Warteschlangen, die durch das manuelle Workload-Management definiert werden.
Cluster mit Nebenläufigkeitsskalierung	10	Ja	Die maximale Anzahl der Cluster mit Nebenläufigkeitsskalierung.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
DC2-Knoten in einem Cluster	128	Ja	Die maximale Anzahl der DC2-Knoten, die Sie einem Cluster zuweisen können. Weitere Informationen zu den aktuellen Knotenlimits für jeden Knotentyp finden Sie unter Cluster und Knoten in Amazon Redshift.
DS2-Knoten in einem Cluster	128	Ja	Die maximale Anzahl der DS2-Knoten, die Sie einem Cluster zuweisen können. Weitere Informationen zu den aktuellen Knotenlimits für jeden Knotentyp finden Sie unter Cluster und Knoten in Amazon Redshift.
Ereignisabonnements	20	Ja	Die maximale Anzahl von Ereignisabonnements für dieses Konto in der aktuellen AWS Region.
Knoten	200	Ja	Die maximale Anzahl von Knoten für alle Datenbank-Instances für dieses Konto in der aktuellen AWS Region.
Parametergruppen	20	Nein	Die maximale Anzahl von Parametergruppen für dieses Konto in der aktuellen AWS Region.
RA3-Knoten in einem Cluster	128	Ja	Die maximale Anzahl der RA3-Knoten, die Sie einem Cluster zuweisen können. Weitere Informationen zu den aktuellen Knotenlimits für jeden Knotentyp finden Sie unter Cluster und Knoten in Amazon Redshift.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Von Redshift verwaltete VPC-Endpunkte, die mit einem Cluster verbunden sind	30	Ja	Die maximale Anzahl der von Redshift verwalteten VPC-Endpunkte, die Sie mit einem Cluster verbinden können. Weitere Informationen zu von Redshift verwalteten VPC-Endpunkten finden Sie unter Arbeiten mit von RedShift verwalteten VPC-Endpunkten.
Berechtigungsempfänger für Cluster, auf den über einen von RedShift verwalteten VPC-Endpunkt zugegriffen wird	5	Ja	Die maximale Anzahl von Berechtigungsempfängern, die ein Cluster-Inhaber zum Erstellen eines von RedShift verwalteten VPC-Endpunkts für einen Cluster autorisieren kann. Weitere Informationen zu von Redshift verwalteten VPC-Endpunkten finden Sie unter Arbeiten mit von RedShift verwalteten VPC-Endpunkten.
Von Redshift verwaltete VPC-Endpunkte pro Autorisierung	5	Ja	Die maximale Anzahl der von Redshift verwalteten VPC-Endpunkte, die Sie pro Autorisierung erstellen können. Weitere Informationen zu von Redshift verwalteten VPC-Endpunkten finden Sie unter Arbeiten mit von RedShift verwalteten VPC-Endpunkten.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Reservierte Knoten	200	Ja	Die maximale Anzahl reservierter Knoten für dieses Konto in der aktuellen AWS Region.
Schemas in jeder Datenbank pro Cluster	9 900	Nein	Die maximale Anzahl von Schemas pro Cluster, die Sie in jeder Datenbank erstellen können. `pg_temp_*` -Schemas zählen allerdings nicht zu diesem Kontingent.
Sicherheitsgruppen	20	Ja	Die maximale Anzahl von Sicherheitsgruppen für dieses Konto in der aktuellen AWS Region.
Einzelzeilengröße beim Laden durch COPY	4	Nein	Die maximale Größe einer einzelnen Zeile (in MB) beim Laden mithilfe des Befehls COPY.
-Snapshots	20	Ja	Die maximale Anzahl von Benutzer-Snapshots für dieses Konto in der aktuellen AWS Region.
Subnetzgruppen	20	Ja	Die maximale Anzahl von Subnetzgruppen für dieses Konto in der aktuellen AWS Region.
Subnetze in einer Subnetzgruppe	20	Ja	Die maximale Anzahl von Subnetzen für eine Subnetzgruppe.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Tabellen für `large`-Cluster-Knotentyp	9 900	Nein	Die maximale Anzahl von Tabellen für den großen Cluster-Knotentyp. Diese Begrenzung schließt permanente Tabellen, temporäre Tabellen, Datashare-Tabellen und materialisierte Ansichten ein. Externe Tabellen werden als temporäre Tabellen gezählt. Zu den temporären Tabellen gehören benutzerdefinierte temporäre Tabellen und temporäre Tabellen, die von Amazon Redshift während der Abfrageverarbeitung oder Systemwartung erstellt wurden. Ansichten und Systemtabellen unterliegen nicht dieser Beschränkung.
Tabellen für `xlarge`-Cluster-Knotentyp	9 900	Nein	Die maximale Anzahl von Tabellen für den `xlarge`-Cluster-Knotentyp. Diese Begrenzung schließt permanente Tabellen, temporäre Tabellen, Datashare-Tabellen und materialisierte Ansichten ein. Externe Tabellen werden als temporäre Tabellen gezählt. Zu den temporären Tabellen gehören benutzerdefinierte temporäre Tabellen und temporäre Tabellen, die von Amazon Redshift während der Abfrageverarbeitung oder Systemwartung erstellt wurden. Ansichten und Systemtabellen unterliegen nicht dieser Beschränkung.
Tabellen für den `xlplus`-Cluster-Knotentyp mit einem Einzelknoten-Cluster.	9 900	Nein	Die maximale Anzahl von Tabellen für den `xlplus`-Cluster-Knotentyp mit einem Einzelknoten-Cluster. Diese Begrenzung schließt permanente Tabellen, temporäre Tabellen, Datashare-Tabellen und materialisierte Ansichten ein. Externe Tabellen werden als temporäre Tabellen gezählt. Zu den temporären Tabellen gehören benutzerdefinierte temporäre Tabellen und temporäre Tabellen, die von Amazon Redshift während der Abfrageverarbeitung oder Systemwartung erstellt wurden. Ansichten und Systemtabellen unterliegen nicht dieser Beschränkung.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Tabellen für den `xlplus`-Cluster-Knotentyp mit einem Cluster mit mehreren Knoten.	20 000	Nein	Die maximale Anzahl von Tabellen für den `xlplus`-Cluster-Knotentyp mit einem Cluster mit mehreren Knoten. Diese Begrenzung schließt permanente Tabellen, temporäre Tabellen, Datashare-Tabellen und materialisierte Ansichten ein. Externe Tabellen werden als temporäre Tabellen gezählt. Zu den temporären Tabellen gehören benutzerdefinierte temporäre Tabellen und temporäre Tabellen, die von Amazon Redshift während der Abfrageverarbeitung oder Systemwartung erstellt wurden. Ansichten und Systemtabellen unterliegen nicht dieser Beschränkung.
Tabellen für `4xlarge`-Cluster-Knotentyp	200 000	Nein	Die maximale Anzahl von Tabellen für den `4xlarge`-Cluster-Knotentyp. Diese Begrenzung schließt permanente Tabellen, temporäre Tabellen, Datashare-Tabellen und materialisierte Ansichten ein. Externe Tabellen werden als temporäre Tabellen gezählt. Zu den temporären Tabellen gehören benutzerdefinierte temporäre Tabellen und temporäre Tabellen, die von Amazon Redshift während der Abfrageverarbeitung oder Systemwartung erstellt wurden. Ansichten und Systemtabellen unterliegen nicht dieser Beschränkung.
Tabellen für `8xlarge`-Cluster-Knotentyp	200 000	Nein	Die maximale Anzahl von Tabellen für den `8xlarge`-Cluster-Knotentyp. Diese Begrenzung schließt permanente Tabellen, temporäre Tabellen, Datashare-Tabellen und materialisierte Ansichten ein. Externe Tabellen werden als temporäre Tabellen gezählt. Zu den temporären Tabellen gehören benutzerdefinierte temporäre Tabellen und temporäre Tabellen, die von Amazon Redshift während der Abfrageverarbeitung oder Systemwartung erstellt wurden. Ansichten und Systemtabellen unterliegen nicht dieser Beschränkung.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Tabellen für `16xlarge`-Cluster-Knotentyp	200 000	Nein	Die maximale Anzahl von Tabellen für den `16xlarge`-Cluster-Knotentyp. Diese Begrenzung schließt permanente Tabellen, temporäre Tabellen, Datashare-Tabellen und materialisierte Ansichten ein. Externe Tabellen werden als temporäre Tabellen gezählt. Zu den temporären Tabellen gehören benutzerdefinierte temporäre Tabellen und temporäre Tabellen, die von Amazon Redshift während der Abfrageverarbeitung oder Systemwartung erstellt wurden. Ansichten und Systemtabellen unterliegen nicht dieser Beschränkung.
Anzahl der Datenbanken	60	Nein	Die maximal zulässige Anzahl von Datenbanken in einem Amazon-Redshift-Cluster. Dies schließt Datenbanken aus, die aus Datashares erstellt wurden.
Timeout für inaktive Sitzungen	4 Stunden	Nein	Diese Einstellung gilt für den Cluster. Informationen zum Festlegen des Timeout-Werts für inaktive Sitzungen für einen Benutzer finden Sie unter ALTER USER im Datenbankentwicklerhandbuch zu Amazon Redshift. Die Benutzereinstellung hat Vorrang vor der Cluster-Einstellung.
Timeout für Transaktionen im Leerlauf	6 Stunden	Nein	Die maximale Inaktivitätsdauer für eine offene Transaktion, bevor Amazon Redshift die mit der Transaktion verknüpfte Sitzung beendet. Diese Einstellung hat Vorrang vor allen benutzerdefinierten Timeout-Einstellungen. Sie gilt für den Cluster.
Gespeicherte Prozeduren in einer Datenbank	10.000	Nein	Die maximale Anzahl gespeicherter Prozeduren. Weitere Limits finden Sie unter Limits und Unterschiede bei der Unterstützung gespeicherter Prozeduren.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Maximale Anzahl von Verbindungen für RA3-Knoten	2.000	Nein	Die maximale Anzahl von Verbindungen zu einem RA3-Cluster. (Dies gilt speziell für die Knotentypen ra3.xlplus, ra3.4xlarge und ra3.16xlarge.) Die maximal zulässigen Verbindungen sind je nach Knotentyp unterschiedlich.
Maximale Anzahl von Verbindungen für DC2- und DS2-Knoten	Variiert	Nein	Die maximale Anzahl von Verbindungen zu einem dc2.large- oder ds2.large-Cluster beträgt 500. Die maximale Anzahl von Sammlungen für einen dc2.8xlarge- oder ds2.8xlarge-Cluster beträgt 2000.
Anzahl der Amazon-Redshift-Rollen in einem Cluster	1.000	Ja	Die maximale Anzahl von Amazon-Redshift-Rollen, die Sie pro Cluster erstellen können. Weitere Informationen zu Rollen für die rollenbasierte Zugriffssteuerung (RBAC) finden Sie unter Rollenbasierte Zugriffskontrolle (RBAC) im Amazon-Redshift-Datenbanken twicklerhandbuch.

Kontingente für Objekte von Amazon Redshift Serverless

Amazon Redshift verfügt über Kontingente, die die Verwendung verschiedener Objekttypen in Ihrer Amazon-Redshift-Serverless-Instance einschränken. Es gibt jeweils einen Standardwert.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Anzahl der Datenbanken	100	Nein	Die maximal zulässige Anzahl von Datenbanken in einem Amazon-Redshift-Serverless-Namespace. Dies schließt Datenbanken aus, die aus Datashares erstellt wurden.
Anzahl der Schemata	9 900	Nein	Die maximal zulässige Anzahl von Schemas in einer Amazon-Redshift-Serverless-Instance.
Anzahl der Tabellen	200 000	Nein	Die maximal zulässige Anzahl von Tabellen in einer Amazon-Redshift-Serverless-Instance.
Timeout für inaktive Sitzungen	1 Stunde	Nein	Informationen zum Festlegen des Timeout-Werts für inaktive Sitzungen für einen Benutzer finden Sie unter ALTER USER im Datenbankentwicklerhandbuch zu Amazon Redshift. Die Benutzereinstellung hat Vorrang.
Timeout für eine laufende Abfrage	86 399 Sekunden (24 Stunden)	Nein	Die maximale Zeit für eine laufende Abfrage, bevor Amazon Redshift sie beendet.
Timeout für Transaktionen im Leerlauf	6 Stunden	Nein	Die maximale Inaktivitätsdauer für eine offene Transaktion, bevor Amazon Redshift Serverless die mit der Transaktion verknüpfte Sitzung beendet. Diese Einstellung hat Vorrang vor allen benutzerdefinierten Timeout-Einstellungen.
Anzahl der maximalen Verbindungen	2000	Nein	Die maximale Anzahl von Verbindungen, die eine Verbindung zu einer Arbeitsgruppe herstellen können.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Anzahl der Arbeitsgruppen	25	Ja	Die Anzahl der unterstützten Arbeitsgruppen.
Anzahl der Namespaces	25	Ja	Die Anzahl der unterstützten Namespaces.
Anzahl der Amazon-Redshift-Rollen in einer Arbeitsgruppe	1.000	Ja	Die maximale Anzahl von Amazon-Redshift-Rollen, die Sie pro Arbeitsgruppe erstellen können. Weitere Informationen zu Rollen für die rollenbasierte Zugriffssteuerung (RBAC) finden Sie unter Rollenbasierte Zugriffskontrolle (RBAC) im Amazon-Redshift-Datenbankentwicklerhandbuch.

Weitere Informationen dazu, wie die Abrechnung bei Amazon Redshift Serverless von der Zeitüberschreitungskonfiguration beeinflusst wird, finden Sie unter Fakturierung für Amazon Redshift Serverless.

Kontingente für die Amazon-Redshift-Daten-API

Amazon Redshift verfügt über Kontingente, die die Verwendung der Redshift-Daten-API einschränken. Es gibt jeweils einen Standardwert. Weitere Informationen zur Amazon-Redshift-Daten-API finden Sie unter Verwenden der Amazon Redshift Data API.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Transaktionen pro Sekunde	20	Nein	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
(TPS) für die `BatchExecuteStatement` -API			
Transaktionen pro Sekunde (TPS) für die `CancelStatement` -API	3	Nein	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.
Transaktionen pro Sekunde (TPS) für die `DescribeStatement` -API	100	Nein	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.
Transaktionen pro Sekunde (TPS) für die `DescribeTable` -API	3	Nein	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Transaktionen pro Sekunde (TPS) für die `ExecuteStatement` -API	30	Nein	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.
Transaktionen pro Sekunde (TPS) für die `GetStatementResult` -API	20	Nein	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.
Transaktionen pro Sekunde (TPS) für die `ListDatabases` -API	3	Nein	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.
Transaktionen pro Sekunde (TPS) für die `ListSchemas` -API	3	Nein	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Transaktionen pro Sekunde (TPS) für die `ListStatements` -API	3	Nein	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.
Transaktionen pro Sekunde (TPS) für die `ListTables` -API	3	Nein	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.

Kontingente für Objekte im Abfrage-Editor v2

Amazon Redshift verfügt über Kontingente, die die Verwendung verschiedener Objekttypen in Ihrem Abfrage-Editor v2 von Amazon Redshift einschränken. Es gibt jeweils einen Standardwert.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Verbindungen	500	Ja	Die maximale Anzahl von Verbindungen, die Sie mit dem Abfrage-Editor v2 in diesem Konto in der aktuellen Region erstellen können.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Aktive Prinzipale pro Konto	50	Ja	Maximale Anzahl gleichzeitiger Prinzipale, die den Abfrage-Editor v2 in diesem Konto in der aktuellen Region verwenden können.
Gespeicherte Abfragen	2.500	Ja	Die maximale Anzahl gespeicherter Abfragen, die Sie mit dem Abfrage-Editor v2 in diesem Konto in der aktuellen Region erstellen können.
Abfrageversionen	20	Ja	Die maximale Anzahl von Versionen pro Abfrage, die Sie mit dem Abfrage-Editor v2 in diesem Konto in der aktuellen Region erstellen können.
Gespeicherte Diagramme	500	Ja	Die maximale Anzahl gespeicherter Diagramme, die Sie mit dem Abfrage-Editor v2 in diesem Konto in der aktuellen Region erstellen können.
Pro Abfrage abgerufene Zeilen	100 000	Nein	Die maximale Anzahl von Zeilen, die vom Abfrage-Editor v2 in diesem Konto in der aktuellen Region pro Abfrage abgerufen werden.
Größe der pro Abfrage abgerufenen Daten	5	Nein	Die maximale Größe der Daten (in Megabyte), die vom Abfrage-Editor v2 in diesem Konto in der aktuellen Region pro Abfrage abgerufen werden.
Gleichzeitige Socket-Verbindungen pro Prinzipal	10	Ja	Die maximale Anzahl an gleichzeitigen Socket-Verbindungen mit dem Abfrage-Editor v2, die ein einzelner Prinzipal in der aktuellen Region einrichten kann. Prüfen Sie, ob dieses Kontingent erhöht werden soll, wenn Sie Fehlermeldungen erhalten, dass Ihre Socket-Verbindungen das Limit überschreiten.

Kontingentname	AWS Standardwert	Anpassbar	Beschreibung
Gleichzeitige Socket-Verbindungen pro Konto	250	Ja	Die maximale Anzahl an gleichzeitigen Socket-Verbindungen mit dem Abfrage-Editor v2, die alle Prinzipale im Konto in der aktuellen Region einrichten können. Prüfen Sie, ob dieses Kontingent erhöht werden soll, wenn Sie Fehlermeldungen erhalten, dass Ihre Socket-Verbindungen das Limit überschreiten.
Maximale Anzahl gleichzeitiger Verbindungen	3	Nein	Maximale Anzahl der Datenbankverbindungen pro Benutzer (einschließlich isolierter Sitzungen). Dieser Wert kann vom Administrator des Abfrage-Editors v2 in den Account settings (Kontoeinstellungen) zwischen 1 und 10 festgelegt werden. Wenn Sie das von Ihrem Administrator festgelegte Limit erreichen, sollten Sie erwägen, bei Ausführung Ihrer SQL gemeinsame Sitzungen anstelle von isolierten Sitzungen zu verwenden. Weitere Informationen zu Verbindungen finden Sie unter Öffnen des Abfrage-Editors v2. Weitere Informationen zur Festlegung dieses Limits finden Sie unter Ändern von Kontoeinstellungen.

Kontingente und Limits in Objekten von Amazon Redshift Spectrum

Amazon Redshift Spectrum verfügt über folgende Kontingente und Limits:

- Die maximale Anzahl von Datenbanken pro AWS Konto bei Verwendung eines AWS Glue Data Catalog. Informationen zu diesem Wert finden Sie unter AWS Glue -Servicekontingente im Allgemeine Amazon Web Services-Referenz.
- Die maximale Anzahl von Tabellen pro Datenbank bei Verwendung von AWS Glue Data Catalog. Informationen zu diesem Wert finden Sie unter AWS Glue -Servicekontingente im Allgemeine Amazon Web Services-Referenz.

- Die maximale Anzahl von Partitionen pro Tabelle bei Verwendung von AWS Glue Data Catalog. Informationen zu diesem Wert finden Sie unter AWS Glue -Servicekontingente im Allgemeine Amazon Web Services-Referenz.
- Die maximale Anzahl von Partitionen pro AWS Konto bei Verwendung eines AWS Glue Data Catalog. Informationen zu diesem Wert finden Sie unter AWS Glue -Servicekontingente im Allgemeine Amazon Web Services-Referenz.
- Die maximale Anzahl von Spalten für externe Tabellen bei Verwendung von AWS Glue Data Catalog, 1 597 bei aktivierten Pseudospalten und 1 600 bei nicht aktivierten Pseudospalten.
- Die maximale Größe eines Zeichenfolgenwerts in einer ION- oder JSON-Datei bei Verwendung eines AWS Glue Data Catalog beträgt 16 KB. Die Zeichenfolge kann gekürzt werden, wenn Sie dieses Limit erreichen.
- Sie können maximal 100 Partitionen mit einer einzelnen ALTER TABLE-Anweisung hinzufügen.
- Alle S3-Daten müssen sich in derselben AWS Region wie der Amazon-Redshift-Cluster befinden.
- Zeitstempel in ION und JSON müssen das ISO8601-Format verwenden.
- Die externe Kompression von ORC-Dateien wird nicht unterstützt.
- Text, OpenCSV und Regex SERDEs unterstützen keine oktalen Trennzeichen größer als „\177“.
- Sie müssen ein Prädikat in der Partitionsspalte angeben, um zu vermeiden, dass aus allen Partitionen gelesen wird.

  Das folgende Prädikat filtert beispielsweise die Spalte `ship_dtm`, wendet den Filter jedoch nicht auf die Partitionsspalte `ship_yyyymm` an:

  ```
  WHERE ship_dtm > '2018-04-01'.
  ```

  Um nicht benötigte Partitionen zu überspringen, müssen Sie das Prädikat hinzufügen `WHERE ship_yyyymm = '201804'`. Dieses Prädikat begrenzt Lesevorgänge auf die Partition `\ship_yyyymm=201804\`.

Diese Limits gelten nicht für einen Apache Hive-Metastore.

Benennungseinschränkungen:

Die folgende Tabelle beschreibt die Benennungseinschränkungen innerhalb von Amazon Redshift.

Cluster Identifier (Cluster-Kennung)	•

	Ein Cluster identifier darf nur zwei Kleinbuchstaben enthalten. • Er muss zwischen 1 und 63 alphanumerische Zeichen oder Bindestriche enthalten. • Das erste Zeichen muss ein Buchstabe sein. • Er darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten. • Sie muss innerhalb eines AWS -Kontos für alle Cluster eindeutig sein.
Datenbankname	• Ein Datenbankname muss 1 bis 64 alphanumerische Zeichen enthalten. • Er darf nur Kleinbuchstaben enthalten. • Es darf sich dabei nicht um ein reserviertes Wort handeln. Eine Liste der reservierten Wörter finden Sie unter Reservierte Wörter im Datenbankentwickle rhandbuch zu Amazon Redshift.
Endpunktname eines von RedShift verwalteten VPC-Endpunkts	• Ein Endpunktname muss 1 bis 30 Zeichen enthalten. • Gültige Zeichen sind a–z, A–Z, 0–9 und Bindestrich (-). • Das erste Zeichen muss ein Buchstabe sein. • Der Name darf nicht zwei aufeinanderfolgende Bindestri che enthalten oder mit einem Bindestrich enden.

Administratorbenutzername	• Ein Administratorbenutzername darf nur Kleinbuchstaben enthalten. • Er muss 1–128 alphanumerische Zeichen enthalten. • Das erste Zeichen muss ein Buchstabe sein. • Es darf sich dabei nicht um ein reserviertes Wort handeln. Eine Liste der reservierten Wörter finden Sie unter Reservierte Wörter im Datenbankentwicklerhandbuch zu Amazon Redshift.
Administratorpasswort	• Ein Administratorpasswort muss 8–64 Zeichen enthalten. • Es muss mindestens einen Großbuchstaben enthalten. • Es muss mindestens einen Kleinbuchstaben enthalten. • Es muss mindestens eine Ziffer enthalten. • Es kann alle ASCII-Zeichen mit den ASCII-Codes 33–126 enthalten, außer einfachen Anführungszeichen ('), doppelten Anführungszeichen ("), \, / und @.
Parametergruppenname	• Ein Parametergruppenname muss 1–255 alphanumerische Zeichen oder Bindestriche enthalten. • Er darf ausschließlich Kleinbuchstaben enthalten. • Das erste Zeichen muss ein Buchstabe sein. • Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.

Cluster-Sicherheitsgruppenname	• Ein Cluster-Sicherheitsgruppenname darf nicht mehr als 255 alphanumerische Zeichen oder Bindestriche enthalten. • Er darf ausschließlich Kleinbuchstaben enthalten. • Der Name darf nicht **`Default`**. • Er muss für alle Sicherheitsgruppen, die von Ihrem AWS Konto erstellt werden, eindeutig sein.
Subnetzgruppenname	• Ein Subnetzgruppenname darf nicht mehr als 255 alphanumerische Zeichen oder Bindestriche enthalten. • Er darf ausschließlich Kleinbuchstaben enthalten. • Der Name darf nicht **`Default`**. • Er muss für alle Subnetzgruppen, die von Ihrem AWS Konto erstellt werden, eindeutig sein.
Cluster-Snapshot-ID	• Eine Cluster-Snapshot-ID darf nicht mehr als 255 alphanumerische Zeichen oder Bindestriche enthalten. • Er darf ausschließlich Kleinbuchstaben enthalten. • Der Name darf nicht **`Default`**. • Er muss für alle Snapshot-Kennungen, die von Ihrem AWS Konto erstellt werden, eindeutig sein.

Markieren von Ressourcen in Amazon Redshift

Themen

- Markieren – Übersicht
- Verwalten der Ressourcen-Tags über die Konsole
- Verwalten von Tags über die Amazon Redshift API

Markieren – Übersicht

In sind Tags benutzerdefinierte Labels AWS, die aus Schlüssel-Wert-Paaren bestehen. Amazon Redshift unterstützt Markierungen, um auf einen Blick die Metadaten zu Ressourcen einsehen und Ihre Fakturierungsberichte anhand der Kostenzuweisung kategorisieren zu können. Um Tags für die Kostenzuweisung verwenden zu können, müssen Sie diese Tags zunächst im Service aktivieren. AWS Billing and Cost Management Weitere Informationen zur Einrichtung und Verwendung von Tags für die Fakturierung finden Sie unter Verwenden von Kostenzuordnungs-Tags für benutzerdefinierte Fakturierungsberichte und Einrichten Ihres monatlichen Kostenzuordnungsberichts.

Es müssen keine Tags für Ressourcen in Amazon verwendet werden, sie helfen jedoch, indem Sie Kontextinformationen bereitstellen. Sie können Tags beispielsweise einsetzen, um Ressourcen mit Metadaten über Kostenstellen, Projektnamen und andere relevante Informationen zur Ressource zu versehen. Beispiel: Nehmen Sie an, Sie möchten nachverfolgen, welche Ressourcen zu einer Testumgebung und welche zu einer Produktionsumgebung gehören. Dazu könnten Sie einen Schlüssel `environment` erstellen und dann einen Wert `test` oder `production` angeben, über den die Ressourcen als einer der beiden Umgebungen angehörig gekennzeichnet werden können. Wenn Sie Tagging in anderen AWS Diensten verwenden oder Standardkategorien für Ihr Unternehmen haben, empfehlen wir Ihnen, aus Konsistenzgründen dieselben Schlüssel-Wert-Paare für Ressourcen in Amazon Redshift zu erstellen.

Markierungen für Ressourcen bleiben erhalten, wenn Sie Cluster vergrößern oder verkleinern, und auch, wenn Sie einen Snapshot eines Clusters in derselben Region wiederherstellen. Die Markierungen gehen jedoch verloren, wenn Sie einen Snapshot in eine andere Region kopieren. Sie müssen in diesem Fall in der neuen Region die Tags erneut erstellen. Wenn Sie eine Ressource löschen, werden alle Tags der Ressource ebenfalls gelöscht.

Jede Ressource verfügt über genau einen Tag-Satz, d. h. eine Zusammenstellung von einem oder mehreren Tags, die der Ressource zugewiesen sind. Jede Ressource kann pro Tag-Satz bis zu

50 Tags enthalten. Sie können Tags beim Erstellen der Ressource hinzufügen, aber auch noch, nachdem die Ressource erstellt wurde. Sie können den folgenden Ressourcentypen in Amazon Redshift: Tags hinzufügen:

- CIDR/IP
- Cluster
- Cluster-Sicherheitsgruppe
- Zugangsregel für Clustersicherheitsgruppe
- Amazon EC2-Sicherheitsgruppe
- Verbindung mit dem Hardware-Sicherheitsmodul (HSM)
- HSM-Clientzertifikat
- Parametergruppe
- Snapshot
- Subnetzgruppe

Um das Markieren über die Amazon-Redshift-Konsole zu verwenden, kann Ihr Benutzer die von AWS verwaltete Richtlinie `AmazonRedshiftFullAccess` anfügen. Ein Beispiel für eine IAM-Richtlinie mit eingeschränkten Markierungsberechtigungen, die Sie einem Benutzer der Amazon-Redshift-Konsole zuweisen können, finden Sie unter Beispiel 7: Benutzer erlauben, mit der Amazon-Redshift-Konsole Ressourcen zu markieren. Weitere Informationen zum Taggen finden Sie unter Was sind AWS Resource Groups? .

Anforderungen zum Markieren

Für Tags gelten zwei Anforderungen:

- Schlüssel dürfen nicht mit dem Präfix `aws:` beginnen.
- Schlüssel müssen in einem Tag-Satz eindeutig sein.
- Schlüssel müssen zwischen 1 und 128 Zeichen lang sein.
- Ein Wert muss zwischen 0 und 256 Zeichen haben.
- Werte brauchen pro Tag-Satz nicht eindeutig zu sein.
- Zulässige Zeichen für Schlüssel und Werte sind Unicode-Buchstaben, Ziffern, Leerzeichen sowie die folgenden Sonderzeichen: _ . : / = + - @.

- Bei Schlüsseln und Werten wird die Groß-/Kleinschreibung berücksichtigt.

Verwalten der Ressourcen-Tags über die Konsole

So verwalten Sie Tags für Ihre Amazon-Redshift-Ressourcen

1. Melden Sie sich bei der Amazon Redshift Redshift-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/redshiftv2/.
2. Wählen Sie im Navigationsmenü Configurations (Konfigurationen) und dann Manage tags (Tags verwalten) aus.
3. Geben Sie Ihre Auswahl für die Ressourcen ein und wählen Sie aus, welche Tags hinzugefügt, geändert oder gelöscht werden sollen. Wählen Sie dann Manage tags of the resources that you chose (Tags der von Ihnen gewählten Ressourcen verwalten) aus.

   Zu den Ressourcen, die Sie taggen können, gehören Cluster, Parametergruppen, Subnetzgruppen, HSM-Client-Zertifikate, HSM-Verbindungen und Snapshots.
4. Wählen Sie auf der Navigationsseite Manage tags (Tags verwalten) Review and apply tag changes (Tag-Änderungen prüfen und anwenden) aus. Wählen Sie dann Apply (Anwenden) aus, um Ihre Änderungen zu speichern.

Verwalten von Tags über die Amazon Redshift API

Sie können die folgenden AWS CLI Operationen verwenden, um Tags in Amazon Redshift zu verwalten.

- create-tags
- delete-tags
- describe-tags

Sie können zur Verwaltung von Tags die folgenden Amazon Redshift API-Vorgänge verwenden:

- CreateTags
- DeleteTags
- DescribeTags
- Markierung

- TaggedResource

Außerdem können Sie die folgenden Amazon Redshift API-Vorgänge zur Verwaltung und Anzeige von Tags für eine bestimmte Ressource verwenden:

- CreateCluster
- CreateClusterParameterGroup
- CreateClusterSecurityGroup
- CreateClusterSnapshot
- CreateClusterSubnetGroup
- CreateHsmClientCertificate
- CreateHsmConfiguration
- DescribeClusters
- DescribeClusterParameterGroups
- DescribeClusterSecurityGroups
- DescribeClusterSnapshots
- DescribeClusterSubnetGroups
- DescribeHsmClientCertificates
- DescribeHsmConfigurations

Cluster-Versionen für Amazon Redshift

Amazon Redshift veröffentlicht regelmäßig Cluster-Versionen. Das Patching Ihrer Amazon-Redshift-Cluster erfolgt während Ihres Systemwartungsfensters. Der Zeitpunkt des Patches hängt von Ihren Einstellungen für das Wartungsfenster AWS-Region und ab. Sie können die Einstellungen für das Wartungsfenster über die Amazon-Redshift-Konsole anzeigen und ändern. Weitere Informationen zur Wartung finden Sie unter Clusterwartung.

Sie können die Cluster-Version Ihres Clusters in der Amazon-Redshift-Konsole auf der Registerkarte Maintenance (Wartung) der Cluster-Details einsehen. Auch in der Ausgabe des folgenden SQL-Befehls ist die Cluster-Version angegeben:

```
SELECT version();
```

Themen

- Amazon-Redshift-Patch 180
- Amazon-Redshift-Patch 179
- Amazon-Redshift-Patch 178
- Amazon-Redshift-Patch 177
- Amazon-Redshift-Patch 176
- Amazon-Redshift-Patch 175
- Amazon-Redshift-Patch 174
- Amazon-Redshift-Patch 173
- Amazon-Redshift-Patch 172
- Amazon-Redshift-Patch 171
- Amazon-Redshift-Patch 170
- Amazon-Redshift-Patch 169
- Amazon-Redshift-Patch 168

Amazon-Redshift-Patch 180

Clusterversionen in diesem Patch:

- 1.0.63590 – Aktuelle Track-Version – veröffentlicht am 19. Februar 2024

- 1.0.63567 – Amazon-Redshift-Serverless-Version – veröffentlicht am 16. Februar 2024
- 1.0.63282 – Amazon-Redshift-Serverless-Version – veröffentlicht am 13. Februar 2024
- 1.0.63269 – Aktuelle Track-Version – veröffentlicht am 13. Februar 2024
- 1.0.63215 – Amazon-Redshift-Serverless-Version – veröffentlicht am 12. Februar 2024
- 1.0.63205 – Aktuelle Track-Version – veröffentlicht am 12. Februar 2024
- 1.0.63030 – Amazon-Redshift-Serverless-Version – veröffentlicht am 7. Februar 2024
- 1.0.62913 – Aktuelle Track-Version – veröffentlicht am 7. Februar 2024
- 1.0.62922 – Amazon-Redshift-Serverless-Version – veröffentlicht am 5. Februar 2024
- 1.0.62878 – Aktuelle Track-Version – veröffentlicht am 5. Februar 2024
- 1.0.62698 – Amazon-Redshift-Serverless-Version – veröffentlicht am 31. Januar 2024
- 1.0.62614 – Aktuelle Track-Version – veröffentlicht am 31. Januar 2024
- 1.0.61687 – Version von Amazon Redshift Serverless – veröffentlicht am 5. Januar 2024
- 1.0.61678 – aktuelle Track-Version – veröffentlicht am 5. Januar 2024
- 1.0.61567 – Version von Amazon Redshift Serverless – veröffentlicht am 31. Dezember 2023
- 1.0.61559 – aktuelle Track-Version – veröffentlicht am 31. Dezember 2023
- 1.0.61430 – Version von Amazon Redshift Serverless – veröffentlicht am 29. Dezember 2023
- 1.0.61395 – aktuelle Track-Version – veröffentlicht am 29. Dezember 2023

Neue Funktionen und Verbesserungen in diesem Patch

- Änderung an CURRENT_USER: der zurückgegebene Benutzername wird nicht mehr auf 64 Zeichen gekürzt.
- Hinzufügung der Möglichkeit, Datenmaskierungsrichtlinien auf Standardansichten und spätbindende Ansichten anzuwenden.
- Hinzufügung der Möglichkeit, dynamische Datenmaskierung (DDM) auf skalare Attribute in Spalten des Datentyps SUPER anzuwenden.
- Hinzufügung der SQL-Funktion OBJECT_TRANSFORM. Weitere Informationen finden Sie unter Funktion OBJECT_TRANSFORM im Datenbankentwicklerhandbuch zu Amazon Redshift.
- Fügt die Möglichkeit hinzu, eine differenzierte Zugriffskontrolle auf Ihre verschachtelten Daten anzuwenden und Abfragen mit Data AWS Lake Formation -Lake-Analysen von Amazon Redshift durchzuführen.
- Hinzufügung des Datentyps INTERVAL.

- Hinzufügung von CONTINUE_HANDLER, einem Ausnahme-Handler-Typ, der den Ablauf einer gespeicherten Prozedur steuert. Sie können damit Ausnahmen abfangen und verarbeiten, ohne den vorhandenen Anweisungsblock zu beenden.
- Hinzufügung der Möglichkeit, Berechtigungen nicht nur für einzelne Objekte, sondern auch für einen Bereich (Schema oder Datenbank) zu definieren. Auf diese Weise können Benutzern und Rollen Berechtigungen für alle aktuellen und zukünftigen Objekte innerhalb des Bereichs erteilt werden.
- Hinzufügung der Möglichkeit, eine Datenbank aus einem Datashare mit Berechtigungen zu erstellen, mit denen Administratoren auf Konsumentenseite Benutzern und Rollen auf Konsumentenseite individuelle Berechtigungen für gemeinsam genutzte Datenbankobjekte gewähren können.
- Unterstützung für den Rückgabedatentyp SUPER von Remote-BYOM-Modellen. Dadurch wird das Spektrum der akzeptierten SageMaker Modelle erweitert, sodass es auch Modelle mit komplexeren Rückgabeformaten umfasst.
- Änderungen an externen Funktionen, die jetzt Zahlen mit oder ohne Nachkommastellen implizit in den numerischen Datentyp der Spalte umwandeln. Bei Spalten vom Typ int2, int4 und int8 werden Zahlen mit Nachkommastellen durch Kürzen akzeptiert, sofern die Zahl nicht außerhalb des zulässigen Bereichs liegt. Für Float4- und Float8-Spalten werden Zahlen ohne Nachkommastellen akzeptiert.
- Fügt drei räumliche Funktionen hinzu, die mit dem hierarchischen koordinatenbasierten H3-Indizierungsrastersystem funktionieren: H3_FromLongLat, H3_ FromPointund H3_Polyfill.

Amazon-Redshift-Patch 179

Clusterversionen in diesem Patch:

- 1.0.62317 – Amazon-Redshift-Serverless-Version – veröffentlicht am 29. Januar 2024
- 1.0.62312 – Trailing-Track-Version – veröffentlicht am 29. Januar 2024
- 1.0.61631 – Version von Amazon Redshift Serverless – veröffentlicht am 5. Januar 2024
- 1.0.61626 – aktuelle Track-Version – veröffentlicht am 5. Januar 2024
- 1.0.61191 – aktuelle Track-Version – veröffentlicht am 16. Dezember 2023
- 1.0.61150 – Version von Amazon Redshift Serverless – veröffentlicht am 16. Dezember 2023
- 1.0.60982 – Version von Amazon Redshift Serverless – veröffentlicht am 13. Dezember 2023
- 1.0.60854 – aktuelle Track-Version – veröffentlicht am 10. Dezember 2023

- 1.0.60354 – Version von Amazon Redshift Serverless – veröffentlicht am 22. November 2023
- 1.0.60353 – aktuelle Track-Version – veröffentlicht am 21. November 2023
- 1.0.60293 – Version von Amazon Redshift Serverless – veröffentlicht am 21. November 2023
- 1.0.60292 – aktuelle Track-Version – veröffentlicht am 22. November 2023
- 1.0.60161 – Version von Amazon Redshift Serverless – veröffentlicht am 18. November 2023
- 1.0.60140 – aktuelle Track-Version – veröffentlicht am 18. November 2023
- 1.0.60139 – Version von Amazon Redshift Serverless – veröffentlicht am 18. November 2023
- 1.0.59947 – Version von Amazon Redshift Serverless – veröffentlicht am 16. November 2023
- 1.0.59945 – aktuelle Track-Version – veröffentlicht am 16. November 2023
- 1.0.59118 – Version von Amazon Redshift Serverless – veröffentlicht am 9. November 2023
- 1.0.59117 – aktuelle Track-Version – veröffentlicht am 9. November 2023

Neue Funktionen und Verbesserungen in diesem Patch

- Unterstützung dafür, dass Verbundbenutzer mit entsprechenden Berechtigungen Systemansichten für Sicherheit auf Zeilenebene und dynamische Datenmaskierung einsehen können, darunter:
  - SVV_ATTACHED_MASKING_POLICY
  - SVV_MASKING_POLICY
  - SVV_RLS_ATTACHED_POLICY
  - SVV_RLS_POLICY
  - SVV_RLS_RELATION
- Neue Funktionalität, die bewirkt, dass eine Abfrage, die nur skalare Funktionen in der FROM-Klausel enthält, jetzt zu einem Fehler führt.
- Hinzufügung von Anweisungen CREATE TABLE AS (CTAS) mit Funktionalität für permanente Zieltabellen zu Nebenläufigkeitsskalierungs-Clustern. Nebenläufigkeitsskalierungs-Cluster unterstützen jetzt mehr Abfragen.
- Hinzufügung der folgenden Systemtabellen, um den Status der Tabellenumverteilung nach Ausführung der klassischen Größenanpassung auf RA3-Clustern zu verfolgen:
  - Die Systemtabelle SYS_RESTORE_STATE zeigt den Fortschritt der Umverteilung auf Tabellenebene.
  - Die Systemtabelle SYS_RESTORE_LOG zeigt den historischen Durchsatz der Datenumverteilung.

- Verbesserung der Slice-Skew-Minimierung bei EVEN-Tabellen nach Ausführung der klassischen Größenanpassung auf RA3-Knotentypen. Dies gilt auch für Patch-178-Cluster, auf denen eine klassische Größenanpassung ausgeführt wurde.
- Unterstützung für UNLOAD mit EXTENSION auf Nebenläufigkeitsskalierungs-Clustern.
- Verbessert die Leistung für Abfragen, die UDFs in HashJoins und NestLoop Joins enthalten.
- Verbesserung der Leistung der elastischen Größenanpassung auf RA3-Knotentypen.
- Verbesserung der Leistung von Datenfreigabeabfragen.
- Verbesserung der Leistung von manuell initiierten Analyseabfragen in bereitgestellten Clustern und Serverless-Arbeitsgruppen, deren Größe elastisch angepasst wurde.
- Verbesserung der Leistung von automatischen WLM-Abfragen durch eine bessere Ressourcenvorhersage im Workload-Management.
- Wegfall der Funktionalität zum Starten von Clustern in Dedicated-Tenancy-VPCs. Diese Änderung wirkt sich nicht auf die Tenancy von EC2-Instances in der VPC aus. Sie können die Tenancy Ihrer VPC mit dem `modify-vpc-tenancy` AWS CLI Befehl auf Standard ändern.
- Die manuelle Aktualisierung von materialisierten Ansichten wird jetzt auf bereitgestellten Nebenläufigkeitsskalierungs-Clustern und bei Serverless-Autoscaling-Berechnungen unterstützt.
- Unterstützung für INTERVAL-Literale für die Funktion EXTRACT. `EXTRACT('hours' from Interval '50 hours')` gibt beispielsweise 2 zurück, da 50 Stunden als 2 Tage und 2 Stunden interpretiert werden und die Stundenkomponente 2 extrahiert wird.

Amazon-Redshift-Patch 178

Clusterversionen in diesem Patch:

- 1.0.63327 – Aktuelle Track-Version – veröffentlicht am 9. Februar 2024
- 1.0.63313 – Trailing-Track-Version – veröffentlicht am 9. Februar 2024
- 1.0.60977 – Trailing-Track-Version – veröffentlicht am 15. Dezember 2023
- 1.0.59596 – aktuelle Track-Version – veröffentlicht am 9. November 2023
- 1.0.58593 – Version von Amazon Redshift Serverless – veröffentlicht am 23. Oktober 2023
- 1.0.58558 – aktuelle Track-Version – veröffentlicht am 23. Oktober 2023
- 1.0.57864 – aktuelle Track-Version – veröffentlicht am 12. Oktober 2023
- 1.0.57850 – Version von Amazon Redshift Serverless – veröffentlicht am 12. Oktober 2023

- 1.0.56952 – Aktuelle Track-Version – am 25. September 2023 veröffentlicht
- 1.0.56970 – Version von Amazon Redshift Serverless – veröffentlicht am 25. September 2023

Neue Funktionen und Verbesserungen in diesem Patch

- Amazon Redshift hat jetzt die Leistung von Abfragen für den Datenaustausch verbessert, indem die Aktualisierung der Metadaten auf Consumer-Instances beschleunigt wurde, während gleichzeitig Datenänderungen auf der Producer-Instance vorgenommen werden.
- Hinzufügung von Unterstützung für die automatische und inkrementelle Aktualisierung von materialisierten Ansichten auf Amazon-Redshift-Datenaustausch-Consumer-Instances, wenn die Basistabellen der materialisierten Ansicht auf die gemeinsam genutzten Daten verweisen.
- Hinzufügung von Unterstützung für das Speichern großer Objekte mit einer Größe von bis zu 16 MB im SUPER-Datentyp. Bei der Aufnahme aus JSON-, PARQUET-, TEXT- und CSV-Quelldateien können Sie halb strukturierte Daten oder Dokumente als Werte im SUPER-Datentyp bis zu 16 MB laden.
- Hinzufügung von Unterstützung für elastische Größenänderung zur Skalierung zu und von einem Amazon-Redshift-RA3-Cluster mit einem Knoten.
- Amazon-Redshift-RA3-Cluster mit einem Knoten können jetzt von Verschlüsselungsverbesserungen profitieren, wodurch die Gesamtverschlüsselungszeit verkürzt und die Verfügbarkeit des Data Warehouse während des Verschlüsselungsprozesses verbessert wird.
- Verbesserte Unterstützung für Abfragen beim Entfernen von Verschachtelungen und Entpivotieren von Daten, die im SUPER-Datentyp gespeichert sind.
- Verbesserte Leistung beim Aktualisieren von materialisierten Ansichten mit SUPER-Datentypen.
- Hinzufügung von Unterstützung für die Aggregation von INTERVAL-Literalen mit der Funktion ANY_VALUE.
- Die Streaming-Aufnahme unterstützt jetzt den folgenden neuen SQL-Befehl zum Löschen von Streaming-Daten: `DELETE FROM streaming_materialized_views WHERE <where filter clause>`.
- Die DECODE-Funktion ersetzt einen spezifischen Wert entweder durch einen anderen spezifischen Wert oder einen Standardwert, abhängig vom Ergebnis einer Gleichheitsbedingung. DECODE benötigt jetzt die folgenden drei Parameter:
  - Ausdruck
  - search

  - Ergebnis
- Neue Funktionen für gespeicherte Prozeduren, die das Abfangen von Datenüberlauf-Datentypkonvertierungsfehlern und die Verarbeitung innerhalb eines Blocks zur Ausnahmebehandlung ermöglichen.
- Sie erhalten jetzt eine Fehlermeldung, wenn Sie Sicherheits- oder durch dynamische Datenmaskierung geschützte Beziehungen auf Zeilenebene abfragen und enable_case_sensitive_identifier so ändern, dass es sich von der Standardeinstellung der Sitzung unterscheidet. Darüber hinaus wird die folgende Konfiguration blockiert, wenn Sicherheits- oder dynamische Datenmaskierungsrichtlinien auf Zeilenebene in Ihrem bereitgestellten Cluster oder Serverless-Namespace angewendet werden:

  `ALTER USER <current_user> SET case-sensitive identifier.`
- Der MERGE-Befehl unterstützt jetzt eine vereinfachte Syntax, die nur die Ziel- und Quelltabelle benötigt. Weitere Informationen finden Sie unter MERGE im Entwicklerhandbuch für Amazon Redshift Database.
- Hinzufügung von Unterstützung für das Anhängen identischer dynamischer Datenmaskierungsrichtlinien an mehrere Benutzer oder Rollen mit derselben Priorität oder ohne Angabe der Priorität.
- Sie können jetzt eine COLLATION angeben, wenn Sie über ALTER TABLE ADD COLUMN eine neue Spalte hinzufügen.
- Behebung eines Problems, das die Durchsetzung von QMR-Regeln für Parallelitätsskalierungs-Cluster und Amazon Redshift Serverless verzögert.
- Amazon Redshift Federated Query hat die Pushdown-Unterstützung für Zeitzone mit Zeitstempel auf Amazon RDS für PostgreSQL und Amazon Aurora PostgreSQL erweitert.
- Sie können jetzt Amazon RDS für MySQL- und Aurora-MySQL-Datenbanknamen benutzen, die mit Ziffern beginnen und Verbundabfragen enthalten.
- Die Ansicht SYS_ANALYZE_HISTORY enthält jetzt Details zu ANALYZE-Vorgängen.
- Die Ansicht SYS_ANALYZE_COMPRESSION_HISTORY enthält jetzt Datensatzdetails für Komprimierungsanalyseoperationen während der Befehle COPY oder ANALYZE COMPRESSION.
- Die Ansicht SYS_SESSION_HISTORY enthält jetzt Datensatzdetails zu aktiven, historischen und neu gestarteten Sitzungen.
- Die Ansicht SYS_TRANSACTION_HISTORY enthält jetzt Datensatzdetails zur Analyse auf Transaktionsebene, die die für das Commit aufgewendete Zeit, die Anzahl der festgeschriebenen Blöcke und die Isolationsstufe angibt.

- Die Ansicht SVV_REDSHIFT_SCHEMA_QUOTA enthält jetzt Datensätze zu Kontingenten und der aktuellen Festplattennutzung für jedes Schema in einer Datenbank.
- Die Ansicht SYS_PROCEDURE_CALL enthält jetzt Datensätze zu Aufrufen gespeicherter Prozeduren, einschließlich Startzeit, Endzeit, Status des gespeicherten Prozeduraufrufs und Aufrufhierarchie für verschachtelte Aufrufe gespeicherter Prozeduren.
- Die Ansicht SYS_CROSS_REGION_DATASHARING_USAGE enthält jetzt Datensätze zur Nachverfolgung der Nutzung von regionsübergreifendem Datenaustausch.
- Die Ansicht SYS_PROCEDURE_MESSAGES enthält jetzt Datensätze, die sich auf Nachverfolgungsinformationen über protokollierte Meldungen gespeicherter Prozeduren beziehen.
- Die Ansicht SYS_UDF_LOG enthält jetzt gegebenenfalls Datensätze zur Nachverfolgung von Systemprotokollmeldungen aus benutzerdefinierten Funktionsaufrufen, Fehlern, Warnungen oder Ablaufverfolgungen.
- Hinzufügung der neuen Spalten IS_RECURSIVE, IS_NESTED, S3LIST_TIME und GET_PARTITION_TIME zu SYS_EXTERNAL_QUERY_DETAIL.
- Hinzufügung von MaxRPU, einer neuen Einstellung zur Kontrolle der Datenverarbeitungskosten für Redshift Serverless. Mit MaxRPU können Sie optional einen oberen Verarbeitungsschwellenwert angeben, um die Data-Warehouse-Kosten zu jedem Zeitpunkt zu kontrollieren, indem Sie das maximale Verarbeitungsniveau auswählen, das Redshift Serverless pro Arbeitsgruppe skalieren kann.
- Korrektur der Ausgabe des INTERVAL-Literals mit numerischen Intervallzeichenfolgen. Beispiel: Ein Intervall, das als `INTERVAL '1' YEAR` angegeben ist, gibt jetzt `1 YEAR` anstelle von `"00:00:00` zurück. Außerdem wird die Ausgabe des INTERVAL-Literals auf die kleinste angegebene INTERVAL-Komponente gekürzt. Beispiel: `INTERVAL '1 day 1 hour 1 minute 1.123 seconds' HOUR TO MINUTE` wird gekürzt auf `1 day 01:01:00`.

Amazon-Redshift-Patch 177

Clusterversionen in diesem Patch:

- 1.0.57922 – Trailing-Track-Version – veröffentlicht am 12. Oktober 2023
- 1.0.57799 – Version von Amazon Redshift Serverless – veröffentlicht am 10. Oktober 2023
- 1.0.57798 – aktuelle Track-Version – veröffentlicht am 10. Oktober 2023
- 1.0.57085 – Trailing-Track-Version – am 26. September 2023 veröffentlicht
- 1.0.56899 – Version von Amazon Redshift Serverless – Veröffentlicht am 21. September 2023

- 1.0.56754 – Aktuelle Track-Version – am 21. September 2023 veröffentlicht
- 1.0.56242 – aktuelle Track-Version – am 11. September 2023 veröffentlicht
- 1.0.55539 – Version von Amazon Redshift Serverless – veröffentlicht am 28. August 2023
- 1.0.55524 – aktuelle Track-Version – veröffentlicht am 28. August 2023
- 1.0.54899 – aktuelle Track-Version – veröffentlicht am 15. August 2023
- 1.0.54899 – aktuelle Track-Version – veröffentlicht am 14. August 2023
- 1.0.54899 – aktuelle Track-Version – veröffentlicht am 15. August 2023
- 1.0.54239 – aktuelle Track-Version – veröffentlicht am 3. August 2023
- 1.0.54321 – Version von Amazon Redshift Serverless – veröffentlicht am 3. August 2023

Neue Funktionen und Verbesserungen in diesem Patch

- Fügt die Ansicht STL_MV_STATE hinzu, die eine Zeile für jeden Statusübergang einer materialisierten Ansicht enthält. SYS_MV_STATE kann für die MV-Aktualisierungsüberwachung für bereitgestellte Instances von Amazon Redshift Serverless und Amazon Redshift verwendet werden.
- Fügt die SYS_USERLOG-Ansicht hinzu, die Details zu den Änderungen an einem Datenbankbenutzer für „Benutzer erstellen“, „Benutzer entfernen“, „Benutzer ändern“ (umbenennen), „Benutzer ändern“ (Eigenschaften ändern) aufzeichnet.
- Fügt die SYS_COPY_REPLACEMENTS-Ansicht hinzu, die ein Protokoll anzeigt, das aufzeichnet, wann ungültige UTF-8-Zeichen vom COPY-Befehl mit der Option ACCEPTINVCHARS ersetzt wurden.
- Fügt die SYS_SPATIAL_SIMPLIFY-Ansicht hinzu, die Informationen zu vereinfachten räumlichen Geometrieobjekten mit dem Befehl COPY enthält.
- Fügt die SYS_VACUUM_HISTORY-Ansicht hinzu, mit der Sie sich die Details und Ergebnisse von VACUUM-Operationen anzeigen lassen können.
- Fügt die SYS_SCHEMA_QUOTA_VIOLATIONS-Ansicht hinzu, um das Auftreten, den Zeitstempel, die XID und andere nützliche Informationen aufzuzeichnen, wenn ein Schema-Kontingent überschritten wird.
- Fügt die SYS_RESTORE_STATE-Ansicht hinzu, mit der Sie den Weiterverteilungsfortschritt jeder Tabelle im Cluster während der asynchronen klassischen Größenänderung überwachen können.
- Fügt die SYS_EXTERNAL_QUERY_ERROR-Ansicht hinzu, die Informationen über Redshift-Spectrum-Scanfehler zurückgibt.

- Fügt dem Befehl CREATE MODEL den Tag-Parameter hinzu, sodass Sie jetzt die Trainingskosten anhand von Autopilot-Trainingsaufträgen verfolgen können.
- Fügt benutzerdefinierte Domain-Namen (CNAME) für Amazon-Redshift-Cluster hinzu.
- Fügt Vorschauunterstützung für Apache Iceberg hinzu, sodass Kunden Analyseabfragen für Apache-Iceberg-Tabellen in Amazon Redshift ausführen können.
- Fügt Unterstützung für die Verwendung von Benutzerrollen mit Parametergruppen im Workload-Management (WLM) hinzu.
- Fügt Unterstützung für das automatische Mounten von hinzu AWS Glue Data Catalog, was es Kunden erleichtert, Abfragen in ihren Data Lakes auszuführen.
- Fügt Funktionen hinzu, sodass die Verwendung von Gruppierungsfunktionen ohne eine GROUP BY-Klausel oder die Verwendung von Gruppierungsoperationen in einer WHERE-Klausel zu einem Fehler führt.
- Fügt gespeicherten Prozeduren Funktionen hinzu, die das Abfangen von Dividierungsfehlern durch Null und die Verarbeitung innerhalb eines Blocks zur Ausnahmebehandlung ermöglichen.
- Behebt einen Fehler, der verhindert hat, dass Abfragen die Nebenläufigkeitsskalierung verwenden, um Daten in Tabellen zu schreiben, wenn es sich bei der Quelltabelle um eine Datashare-Tabelle handelt.
- Korrigiert den unter enable_case_sensitive_identifier dokumentierten Bezeichner, der zwischen Groß- und Kleinschreibung unterscheidet, sodass er jetzt mit MERGE-Anweisungen funktioniert.
- Behebt den Fehler, dass eine Abfrage in der Funktion pg_get_late_binding_view_cols() gelegentlich ignoriert wurde. Sie können solche Abfragen jetzt jederzeit abbrechen.
- Verbessert die Leistung bei Datashare-Abfragen, die auf Consumer ausgeführt werden, wenn Bereinigungsaufträge auf dem Producer laufen.
- Verbessert die Leistung bei Datashare- und Nebenläufigkeitsskalierungs-Abfragen, insbesondere bei gleichzeitigen Datenänderungen beim Producer oder beim Auslagern auf eine an den Consumer angeschlossene Nebenläufigkeitsskalierungs-Instance.

Amazon-Redshift-Patch 176

Clusterversionen in diesem Patch:

- 1.0.56738 – Trailing-Track-Version – am 21. September 2023 veröffentlicht
- 1.0.55837 – aktuelle Track-Version – am 11. September 2023 veröffentlicht

- 1.0.54776 – aktuelle Track-Version – veröffentlicht am 15. August 2023
- 1.0.54052 – aktuelle Track-Version – veröffentlicht am 26. Juli 2023
- 1.0.53642 – Version von Amazon Redshift Serverless – veröffentlicht am 20. Juli 2023
- 1.0.53301 – aktuelle Track-Version – veröffentlicht am 20. Juli 2023
- 1.0.52943 – Version von Amazon Redshift Serverless – veröffentlicht am 7. Juli 2023
- 1.0.52931 – Aktuelle Track-Version – veröffentlicht am 7. Juli 2023
- 1.0.52194 – Version von Amazon Redshift Serverless – veröffentlicht am 21. Juni 2023
- 1.0.51986 – Aktuelle Track-Version – veröffentlicht am 16. Juni 2023
- 1.0.51594 – Aktuelle Track-Version – veröffentlicht am 9. Juni 2023

Neue Funktionen und Verbesserungen in diesem Patch

- Verbesserte Fehlerbehandlung beim Schreiben von GROUP BY () für einen leeren Gruppierungssatz. Dies wurde zuvor ignoriert und gibt jetzt einen Parserfehler zurück.
- Leistungsverbesserungen für die schrittweise Aktualisierung materialisierter Ansichten mit SUPER-Spalten.
- ALTER TABLE <target_tbl> APPEND FROM <streaming_mv> – (ATA) Der SQL-Befehl unterstützt jetzt das Verschieben aller Datensätze aus einer materialisierten Streaming-Ansicht (Materialized View, MV) als Quelle, zusätzlich zu Tabellen als Quelle, in eine Zieltabelle. Die Unterstützung von ATA in Streaming-MVs ermöglicht es Benutzern, alle Datensätze in einer Streaming-MV schnell zu löschen, indem sie sie in eine andere Tabelle verschieben, um das Datenwachstum zu bewältigen.
- TRUNCATE <streaming_mv> – Der SQL-Befehl unterstützt jetzt das Abschneiden aller Datensätze in einer materialisierten Streaming-Ansicht (Materialized View, MV), zusätzlich zu den Tabellen. TRUNCATE löscht alle Datensätze in der Streaming-MV, wobei die Streaming-MV-Struktur intakt bleibt. Wenn TRUNCATE in Streaming-MVs ausgeführt wird, können Kunden schnell alle Datensätze in einer Streaming-MV löschen, um das Datenwachstum zu bewältigen.
- Dem SELECT-Befehl wurden Funktionen für die QUALIFY-Klausel hinzugefügt.
- Redshift-Unterstützung für Machine Learning für Zeitreihenprognosen durch Integration in Amazon Forecast.
- AWS Glue Data Catalog Das automatische Mounting wird unterstützt, um das Abfragen eines Data Lake ohne zusätzliche Schritte zum Erstellen externer Schemareferenzen zu vereinfachen.
- Das Ändern einer RLS-Richtlinie wird jetzt unterstützt. Weitere Informationen finden Sie in der Dokumentation unter ALTER RLS POLICY.

- Lambda-UDFs unterstützen jetzt den STABLE-Funktions-Volatilitätsparameter in der CREATE FUNCTION-Anweisung. Wenn der STABLE-Parameter in der CREATE FUNCTION-Anweisung verwendet und die Lambda-UDF mehrfach mit denselben Argumenten aufgerufen wird, verringert sich die erwartete Anzahl von Lambda-UDF-Funktionsaufrufen. Die Funktions-Volatilitätskategorie STABLE wird in den CREATE FUNCTION-Parametern näher erläutert.
- Mehrere Lambda-UDF-Leistungsverbesserungen. Insbesondere verbesserte Unterstützung für das Batching von Datensätzen beim Abfragen einer Tabelle, die durch eine Richtlinie für die Sicherheit auf Zeilenebene (RLS) geschützt ist.
- Verkürzung der Gesamtverschlüsselungszeit für RA3-Cluster von Amazon Redshift und Verbesserung der Verfügbarkeit des Data Warehouse während der Verschlüsselung. Weitere Informationen finden Sie unter Datenbankverschlüsselung in Amazon Redshift.
- Eine neue Systemansicht, SYS_MV_REFRESH_HISTORY, wurde zu Redshift hinzugefügt. Die Ansicht SYS_MV_REFRESH_HISTORY enthält eine Zeile für die Aktualisierungsaktivität materialisierter Ansichten. Mit SYS_MV_REFRESH_HISTORY können Sie den Aktualisierungsverlauf materialisierter Ansichten überprüfen. SYS_MV_REFRESH_HISTORY ist für alle Benutzer sichtbar. Superuser können alle Zeilen sehen; reguläre Benutzer können nur ihre eigenen Daten sehen.

  Eine neue Spalte SPILLED_BLOCK_LOCAL_DISK wurde der Systemansicht SYS_QUERY_DETAIL hinzugefügt. Die neue Spalte SPILLED_BLOCK_LOCAL_DISK hilft Kunden dabei, Blöcke zu ermitteln, die auf die lokale Festplatte übertragen wurden. Sie können SYS_QUERY_DETAIL verwenden, um Details für Abfragen auf Schrittebene anzuzeigen. SYS_QUERY_DETAIL ist für alle Benutzer sichtbar. Superuser können alle Zeilen anzeigen, während normale Benutzer nur die Metadaten anzeigen können, auf die sie Zugriff haben.
- Eine neue Systemansicht, SYS_QUERY_TEXT, wurde zu Amazon Redshift Serverless hinzugefügt und von Amazon Redshift bereitgestellt. Die Ansicht SYS_QUERY_TEXT ähnelt SVL_STATEMENTTEXT für bereitgestellte Cluster. Verwenden Sie die Spalte `sequence` in der SYS_QUERY_TEXT-Ansicht, um den vollständigen SQL-Anweisungstext abzurufen.

Amazon-Redshift-Patch 175

Clusterversionen in diesem Patch:

- 1.0.53064 – Aktuelle Track-Version – veröffentlicht am 7. Juli 2023
- 1.0.51973 – Aktuelle Track-Version – veröffentlicht am 16. Juni 2023
- 1.0.51781 – Aktuelle Track-Version – veröffentlicht am 10. Juni 2023

- 1.0.51314 – Version von Amazon Redshift Serverless – veröffentlicht am 3. Juni 2023
- 1.0.51304 – Aktuelle Track-Version – veröffentlicht am 2. Juni 2023
- 1.0.50708 – Aktuelle Track-Version – veröffentlicht am 19. Mai 2023
- 1.0.50300 – Aktuelle Track-Version – veröffentlicht am 8. Mai 2023
- 1.0.49710 – Version von Amazon Redshift Serverless – veröffentlicht am 28. April 2023
- 1.0.49676 – Aktuelle Track-Version – veröffentlicht am 28. April 2023

Neue Funktionen und Verbesserungen in diesem Patch

- Kleinere Fehlerbehebungen.
- Die Streaming-Erfassung von Amazon Redshift unterstützt jetzt die regionsübergreifende Streaming-Erfassung, bei der sich Ihr Quellthema Amazon Kinesis Data Streams (KDS) oder Ihr Amazon Managed Streaming for Apache Kafka (MSK) in einer AWS Region befinden kann, die sich von der AWS Region unterscheidet, in der sich Ihr Amazon Redshift Data Warehouse befindet. Die Dokumentation unter Erste Schritte mit der Streaming-Erfassung aus Amazon Kinesis Data Streams wurde überarbeitet und erläutert die Verwendung des REGION-Schlüsselworts.
- Anpassung der Sommerzeit in Ägypten
- Verbesserung der Gesamtzeiten für die Verschlüsselung von RA3-Clustern

Amazon-Redshift-Patch 174

1.0.51296 – veröffentlicht am 2. Juni 2023

Veröffentlichung im nachgestellten Pfad. Keine Versionshinweise.

1.0.50468 – veröffentlicht am 12. Mai 2023

Wartungsversion. Keine Versionshinweise.

1.0.49780, 1.0.49868 und 1.0.49997 – veröffentlicht am 28. April 2023

Versionshinweise für diese Version:

- Verbesserte Batching-Unterstützung für Lambda UDF

- Inkrementelles Batching für Lambda UDF
- Neuer SQL-Befehl MERGE zum Anwenden von Quelldatenänderungen auf Amazon-Redshift-Tabellen
- Neue dynamische Datenmaskierungsfunktion zur Vereinfachung des Schutzes vertraulicher Daten in einem Amazon-Redshift-Data-Warehouse
- Neue zentrale Zugriffskontrolle für die Datenfreigabe mit Lake Formation, die die Verwaltung von Berechtigungsgewährungen, die Anzeige von Zugriffskontrollen und die Prüfung von Berechtigungen für die Tabellen und Ansichten in den Amazon-Redshift-Datashares mithilfe von Lake-Formation-APIs und der AWS Konsole ermöglicht.
- Anpassung der Sommerzeit in Ägypten

1.0.49087 – Veröffentlicht am 12. April 2023

Wartungsversion. Keine Versionshinweise.

1.0.48805 – Veröffentlicht am 5. April 2023

Versionshinweise für diese Version:

- Amazon Redshift hat mithilfe von BYTEDICT, einer neuen Komprimierungskodierung in Amazon Redshift, die die zeichenfolgenbasierte Datenverarbeitung im Vergleich zu alternativen Komprimierungskodierungen wie LZO oder ZSTD um das 5- bis 63-Fache beschleunigt, zusätzliche Leistungsverbesserungen für Abfragen mit vielen Zeichenfolgen eingeführt. Weitere Informationen zu dieser Funktion finden Sie unter Byte-Verzeichnis-Kodierung im Datenbankentwicklerhandbuch zu Amazon Redshift.

1.0.48004 – Veröffentlicht am 17. März 2023

Wartungsversion. Keine Versionshinweise.

1.0.47470 – Veröffentlicht am 11. März 2023

Versionshinweise für diese Version:

- Verbesserung der Abfrageleistung für `pg_catalog.svv_table_info`. Zudem Hinzukommen einer neuen Spalte `create_time`. Beim Erstellen einer Tabelle speichert diese Spalte den Datums-/Uhrzeitstempel in UTC.

- Hinzufügen von Unterstützung für die Angabe eines Timeouts auf Sitzungsebene für eine Verbundabfrage.

Amazon-Redshift-Patch 173

1.0.49788 – veröffentlicht am 28. April 2023

Versionshinweise für diese Version:

- Anpassung der Sommerzeit in Ägypten

1.0.49074 – Veröffentlicht am 12. April 2023

Versionshinweise für diese Version:

- Aktualisierung der Zeitzonenkonfiguration auf die IANA-Bibliotheksversion 2022g.

1.0.48766 – Veröffentlicht am 5. April 2023

Wartungsversion. Keine Versionshinweise.

1.0.48714 – Veröffentlicht am 5. April 2023

Wartungsversion. Keine Versionshinweise.

1.0.48022 – Veröffentlicht am 17. März 2023

Wartungsversion. Keine Versionshinweise.

1.0.47357 – Veröffentlicht am 7. März 2023

Wartungsversion. Keine Versionshinweise.

1.0.46987 – Veröffentlicht am 24. Februar 2023

Wartungsversion. Keine Versionshinweise.

1.0.46806 – Veröffentlicht am 18. Februar 2023

Wartungsversion. Keine Versionshinweise.

1.0.46607 – Veröffentlicht am 13. Februar 2023

Versionshinweise für diese Version:

- Wir konvertieren jetzt automatisch Tabellen mit verschachtelten Sortierschlüsseln, die manuell auf zusammengesetzte Sortierschlüssel festgelegt wurden, wenn ihr Verteilungsstil auf DISTSTYLE KEY eingestellt wurde, um die Leistung dieser Tabellen zu verbessern. Dieser Vorgang erfolgt zum Zeitpunkt der Wiederherstellung eines Snapshots in Amazon Redshift Serverless.

1.0.45698 – Veröffentlicht am 20. Januar 2023

Versionshinweise für diese Version:

- Hinzufügen eines Dateierweiterungsparameters zum Befehl UNLOAD, sodass automatisch Dateierweiterungen zu Dateinamen hinzugefügt werden.
- Unterstützung des standardmäßigen Schutzes von RLS-geschützten Objekten, wenn diese zu einem Datashare hinzugefügt werden oder wenn sie bereits Teil eines Datashares sind. Administratoren können jetzt RLS für Datashares deaktivieren, um Konsumenten den Zugriff auf das geschützte Objekt zu ermöglichen.
- Hinzufügen von neuen Systemtabellen für die Überwachung: `SVV_ML_MODEL_INFO`, `SVV_MV_DEPENDENCY` und `SYS_LOAD_DETAIL`. Zudem Hinzufügen der Spalten `data_skewness` und `time_skewness` zur Systemtabelle `SYS_QUERY_DETAIL`.

Amazon-Redshift-Patch 172

Clusterversionen in diesem Patch:

- 1.0.46534 – Veröffentlicht am 18. Februar 2023
- 1.0.46523 – Veröffentlicht am 13. Februar 2023
- 1.0.46206 – Veröffentlicht am 1. Februar 2023
- 1.0.45603 – Veröffentlicht am 20. Januar 2023
- 1.0.44924 – Veröffentlicht am 19. Dezember 2022
- 1.0.44903 – Veröffentlicht am 18. Dezember 2022
- 1.0.44540 – Veröffentlicht am 13. Dezember 2022
- 1.0.44126 – Veröffentlicht am 23. November 2022

- 1.0.43980 – Veröffentlicht am 17. November 2022

Neue Funktionen und Verbesserungen in diesem Patch

- Von CTAS erstellte Tabellen sind standardmäßig auf AUTO eingestellt.
- Hinzufügen von Unterstützung für Sicherheit auf Zeilenebene (RLS) für materialisierte Ansichten.
- Erhöhung des S3-Timeouts, um die regionsübergreifende Datenfreigabe zu verbessern.
- Hinzufügen einer neuen räumlichen Funktion `ST_GeomFromGeohash`.
- Verbessert die automatische Auswahl des Verteilungsschlüssels aus zusammengesetzten Primärschlüsseln, um die out-of-the-box Leistung zu verbessern.
- Fügt dem Verteilungsschlüssel für Tabellen mit zusammengesetzten Primärschlüsseln automatischen Primärschlüssel hinzu, wodurch die out-of-the-box Leistung verbessert wird.
- Verbesserung der Nebenläufigkeitsskalierung, damit mehr Abfragen skaliert werden können, auch wenn sich Daten ändern.
- Verbesserung der Abfrageleistung für die Datenfreigabe.
- Hinzufügen von Machine-Learning-Wahrscheinlichkeitsmetriken für Klassifikationsmodelle.
- Hinzufügen von Systemtabellen für die Überwachung: `SVV_USER_INFO`, `SVV_MV_INFO`, `SYS_CONNECTION_LOG`, `SYS_DATASHARE_USAGE_PRODUCER`, `SYS_DATASHARE_USAGE_CONSUMER` und `SYS_DATASHARE_CHANGE_LOG`.
- Hinzufügen von Unterstützung für die Abfrage von VARBYTE-Spalten in externen Tabellen für die Dateitypen Parquet und ORC.

Amazon-Redshift-Patch 171

Clusterversionen in diesem Patch:

- 1.0.43931 – Veröffentlicht am 16. November 2022
- 1.0.43551 – Veröffentlicht am 5. November 2022
- 1.0.43331 – Veröffentlicht am 29. September 2022
- 1.0.43029 – Veröffentlicht am 26. September 2022

Neue Funktionen und Verbesserungen in diesem Patch

- CONNECT BY-Unterstützung: Hinzufügen von Unterstützung für das SQL-Konstrukt CONNECT BY, sodass Sie die hierarchischen Daten in Ihrem Data Warehouse rekursiv auf der Grundlage der Beziehung übergeordneter und untergeordneter Elemente innerhalb dieses Datensatzes abfragen können.

Amazon-Redshift-Patch 170

Clusterversionen in diesem Patch:

- 1.0.43922 – Veröffentlicht am 21. November 2022
- 1.0.43573 – Veröffentlicht am 7. November 2022
- 1.0.41881 – Veröffentlicht am 20. September 2022
- 1.0.41465 – am 7. September 2022 veröffentlicht
- 1.0.40325 – Veröffentlicht am 27. Juli 2022

Neue Funktionen und Verbesserungen in diesem Patch

- ST_GeomfromGeoJSON: Konstruiert ein Geogeometrieobjekt von Amazon Redshift aus VARCHAR in GeoJSON-Darstellung.

Amazon-Redshift-Patch 169

Clusterversionen in diesem Patch:

- 1.0.41050 – Veröffentlicht am 7. September 2022
- 1.0.40083 – Veröffentlicht am 16. Juli 2022
- 1.0.39734 – Veröffentlicht am 07. Juli 2022
- 1.0.39380 – Veröffentlicht am 23. Juni 2022
- 1.0.39251 – Veröffentlicht am 15. Juni 2022
- 1.0.39009 – Veröffentlicht am 08. Juni 2022

Neue Funktionen und Verbesserungen in diesem Patch

- Fügt Rolle als Parameter für den Befehl Alter Default Privileges hinzu, um die rollenbasierte Zugriffssteuerung zu unterstützen.
- Fügt den Parameter ACCEPTINVCHARS hinzu, um das Ersetzen ungültiger UTF-8-Zeichen beim Kopieren aus PARQUET- und ORC-Dateien zu unterstützen.
- Fügt die Funktion OBJECT(k,v) hinzu, um SUPER-Objekte aus Schlüssel-Wert-Paaren zu erstellen.

Amazon-Redshift-Patch 168

Clusterversionen in diesem Patch:

- 1.0.38698 – Veröffentlicht am 25. Mai 2022
- 1.0.38551 – Veröffentlicht am 20. Mai 2022
- 1.0.38463 – Veröffentlicht am 18. Mai 2022
- 1.0.38361 – Veröffentlicht am 13. Mai 2022
- 1.0.38199 – Veröffentlicht am 09. Mai 2022
- 1.0.38112 – Veröffentlicht am 6. Mai 2022
- 1.0.37684 – Veröffentlicht am 20. April 2022

Neue Funktionen und Verbesserungen in diesem Patch

- Fügt Unterstützung für den Modelltyp für lineares Lernen in Amazon Redshift ML hinzu.
- Fügt eine SNAPSHOT-Option für die SQL-Transaktionsisolationsstufe hinzu.
- Fügt `farmhashFingerprint64` als neuem Hashing-Algorithmus für `VARBYTE`- und `VARCHAR`-Daten hinzu.
- Unterstützt die AVG-Funktion bei der inkrementellen Aktualisierung materialisierter Ansichten.
- Unterstützt korrelierte Unterabfragen für externe Tabellen in Redshift Spectrum.
- Um die out-of-the-box Abfrageleistung zu verbessern, wählt Amazon Redshift automatisch einen Einzelspalten-Primärschlüssel für bestimmte Tabellen als Verteilungsschlüssel aus.

Codebeispiele für Amazon Redshift mit SDKs AWS

Die folgenden Codebeispiele zeigen, wie Amazon Redshift mit einem AWS Software Development Kit (SDK) verwendet wird.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Servicefunktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarien und serviceübergreifenden Beispiele sehen.

Szenarien sind Codebeispiele, die Ihnen zeigen, wie Sie eine bestimmte Aufgabe ausführen können, indem Sie mehrere Funktionen innerhalb desselben Services aufrufen.

Serviceübergreifende Beispiele sind Beispielanwendungen, die über mehrere AWS-Services hinweg arbeiten.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erste Schritte

Hallo Amazon Redshift

Das folgende Codebeispiel zeigt die ersten Schritte mit Amazon Redshift.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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()));
    }
}
```

- Einzelheiten zur API finden Sie unter DescribeClusters in der AWS SDK for Java 2.x API-Referenz.

Codebeispiele

- Aktionen für Amazon Redshift mithilfe von SDKs AWS
  - Erstellen Sie einen Amazon Redshift Redshift-Cluster mithilfe eines SDK AWS
  - Erstellen Sie eine Amazon Redshift Redshift-Tabelle mit einem SDK AWS
  - Löschen Sie einen Amazon Redshift Redshift-Cluster mithilfe eines SDK AWS

- Beschreiben Sie eine Amazon Redshift Redshift-Abfrageanweisung mithilfe eines SDK AWS
- Beschreiben Sie Cluster mithilfe eines AWS SDK
- Rufen Sie das Ergebnis der Amazon Redshift Redshift-Abrechnung mithilfe eines AWS SDK ab
- Daten mithilfe eines SDK in eine Amazon Redshift AWS Redshift-Tabelle einfügen
- Ändern Sie einen Amazon Redshift Redshift-Cluster mithilfe eines SDK AWS
- Eine Amazon Redshift Redshift-Tabelle mithilfe eines AWS SDK abfragen

- Szenarien für Amazon Redshift mit SDKs AWS
  - Erste Schritte mit Amazon Redshift Redshift-Tabellen, -Elementen und -Abfragen
- Serviceübergreifende Beispiele für Amazon Redshift mit SDKs AWS
  - Erstellen eines Amazon-Redshift-Element-Trackers

Aktionen für Amazon Redshift mithilfe von SDKs AWS

Die folgenden Codebeispiele zeigen, wie einzelne Amazon Redshift Redshift-Aktionen mit AWS SDKs ausgeführt werden. Diese Auszüge rufen die Amazon Redshift Redshift-API auf und sind Codeauszüge aus größeren Programmen, die im Kontext ausgeführt werden müssen. Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der Amazon Redshift API-Referenz.

Beispiele

- Erstellen Sie einen Amazon Redshift Redshift-Cluster mithilfe eines SDK AWS
- Erstellen Sie eine Amazon Redshift Redshift-Tabelle mit einem SDK AWS
- Löschen Sie einen Amazon Redshift Redshift-Cluster mithilfe eines SDK AWS
- Beschreiben Sie eine Amazon Redshift Redshift-Abfrageanweisung mithilfe eines SDK AWS
- Beschreiben Sie Cluster mithilfe eines AWS SDK
- Rufen Sie das Ergebnis der Amazon Redshift Redshift-Abrechnung mithilfe eines AWS SDK ab
- Daten mithilfe eines SDK in eine Amazon Redshift AWS Redshift-Tabelle einfügen
- Ändern Sie einen Amazon Redshift Redshift-Cluster mithilfe eines SDK AWS
- Eine Amazon Redshift Redshift-Tabelle mithilfe eines AWS SDK abfragen

Erstellen Sie einen Amazon Redshift Redshift-Cluster mithilfe eines SDK AWS

Die folgenden Codebeispiele zeigen, wie Sie einen Amazon Redshift Redshift-Cluster erstellen.

CLI

AWS CLI

Das ParametersThis Beispiel „Cluster mit minimalem Wert erstellen“ erstellt einen Cluster mit einem minimalen Parametersatz. Standardmäßig erfolgt die Ausgabe im JSON-Format.Befehl:

```
aws redshift create-cluster --node-type dw.hs1.xlarge --number-of-nodes 2 --
master-username adminuser --master-user-password TopSecret1 --cluster-identifier
 mycluster
```

Ergebnis:

```
{
   "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"
   }
}
```

- Einzelheiten zur API finden Sie CreateClusterin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Erstellen Sie den -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);
        }
    }
```

- Einzelheiten zur API finden Sie CreateClusterin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Erstellen Sie den Client.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Erstellen Sie den -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();
```

- Einzelheiten zur API finden Sie CreateClusterin der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Erstellen Sie den -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}")
    }
}
```

- Einzelheiten zur API finden Sie CreateClusterin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erstellen Sie eine Amazon Redshift Redshift-Tabelle mit einem SDK AWS

Das folgende Codebeispiel zeigt, wie eine Amazon Redshift Redshift-Tabelle erstellt wird.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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);
        }
    }
```

- Einzelheiten zur API finden Sie CreateTablein der AWS SDK for Java 2.x API-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Löschen Sie einen Amazon Redshift Redshift-Cluster mithilfe eines SDK AWS

Die folgenden Codebeispiele zeigen, wie ein Amazon Redshift Redshift-Cluster gelöscht wird.

CLI

AWS CLI

Das SnapshotThis Beispiel „Cluster ohne endgültigen Cluster löschen“ löscht einen Cluster und erzwingt das Löschen von Daten, sodass kein endgültiger Cluster-Snapshot erstellt wird.Befehl:

```
aws redshift delete-cluster --cluster-identifier mycluster --skip-final-cluster-
snapshot
```

Das SnapshotThis Beispiel „Cluster löschen, einen finalen Cluster zulassen“ löscht einen Cluster, gibt aber einen endgültigen Cluster-Snapshot an.Befehl:

```
aws redshift delete-cluster --cluster-identifier mycluster --final-cluster-
snapshot-identifier myfinalsnapshot
```

- Einzelheiten zur API finden Sie in der Befehlsreferenz DeleteCluster.AWS CLI

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Löschen Sie den 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);
       }
   }
```

- Einzelheiten zur API finden Sie DeleteClusterin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Erstellen Sie den Client.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Erstellen Sie den -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();
```

- Einzelheiten zur API finden Sie DeleteClusterin der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Löschen Sie den 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}")
    }
}
```

- Einzelheiten zur API finden Sie DeleteClusterin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Beschreiben Sie eine Amazon Redshift Redshift-Abfrageanweisung mithilfe eines SDK AWS

Das folgende Codebeispiel zeigt, wie eine Amazon Redshift Redshift-Abfrageanweisung beschrieben wird.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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);
        }
    }
```

- Einzelheiten zur API finden Sie DescribeStatementin der AWS SDK for Java 2.x API-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Beschreiben Sie Cluster mithilfe eines AWS SDK

Die folgenden Codebeispiele zeigen, wie Amazon Redshift Redshift-Cluster beschrieben werden.

CLI

AWS CLI

Das ClustersThis Beispiel Get a Description of All gibt eine Beschreibung aller Cluster für das Konto zurück. Standardmäßig erfolgt die Ausgabe im JSON-Format.Befehl:

```
aws redshift describe-clusters
```

Ergebnis:

```
{
   "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"
   }
}
```

Mit der Option.COMMAND können Sie dieselben Informationen auch im Textformat abrufen: `--output text`

`--output text`Option.Befehl:

Option.Befehl:

```
aws redshift describe-clusters --output text
```

Ergebnis:

```
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
```

- Einzelheiten zur API finden Sie DescribeClustersin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Beschreiben Sie den 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);
        }
    }
```

- Einzelheiten zur API finden Sie DescribeClustersunter AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Erstellen Sie den Client.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Beschreiben Sie Ihre Cluster.

```
// 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();
```

- Einzelheiten zur API finden Sie DescribeClustersin der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Beschreiben Sie den 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}")
            }
        }
    }
}
```

- Einzelheiten zur API finden Sie DescribeClustersin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Rufen Sie das Ergebnis der Amazon Redshift Redshift-Abrechnung mithilfe eines AWS SDK ab

Das folgende Codebeispiel zeigt, wie das Ergebnis der Anweisung abgerufen wird.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Überprüfe das Ergebnis der Abrechnung.

```
   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);
       }
   }
```

- Einzelheiten zur API finden Sie GetStatementResultin der AWS SDK for Java 2.x API-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Daten mithilfe eines SDK in eine Amazon Redshift AWS Redshift-Tabelle einfügen

Das folgende Codebeispiel zeigt, wie Daten in eine Amazon Redshift Redshift-Tabelle eingefügt werden.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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. ");
    }
```

- Einzelheiten zur API finden Sie unter In die AWS SDK for Java 2.x API-Referenz einfügen.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Ändern Sie einen Amazon Redshift Redshift-Cluster mithilfe eines SDK AWS

Die folgenden Codebeispiele zeigen, wie ein Amazon Redshift Redshift-Cluster geändert wird.

CLI

AWS CLI

Eine Sicherheitsgruppe einem ClusterThis Beispiel zuordnen zeigt, wie eine Cluster-Sicherheitsgruppe dem angegebenen Cluster zugeordnet wird. Befehl:

```
aws redshift modify-cluster --cluster-identifier mycluster --cluster-security-
groups mysecuritygroup
```

Das Wartungsfenster ändern für ClusterThis zeigt, wie das bevorzugte wöchentliche Wartungsfenster für einen Cluster so geändert werden kann, dass es mindestens vier Stunden dauert und sonntags um 23:15 Uhr beginnt und montags um 3:15 Uhr endet. Befehl:

```
aws redshift modify-cluster --cluster-identifier mycluster --preferred-
maintenance-window Sun:23:15-Mon:03:15
```

Das Master-Passwort ändern Das ClusterThis Beispiel zeigt, wie das Master-Passwort für einen Cluster geändert wird. Befehl:

```
aws redshift modify-cluster --cluster-identifier mycluster --master-user-password
 A1b2c3d4
```

- Einzelheiten zur API finden Sie ModifyClusterin AWS CLI der Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Modifizieren Sie einen 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);
       }
   }
```

- Einzelheiten zur API finden Sie ModifyClusterunter AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Erstellen Sie den Client.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Modifizieren Sie einen 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();
```

- Einzelheiten zur API finden Sie ModifyClusterunter AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Modifizieren Sie einen 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")
    }
}
```

- Einzelheiten zur API finden Sie ModifyClusterin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Eine Amazon Redshift Redshift-Tabelle mithilfe eines AWS SDK abfragen

Das folgende Codebeispiel zeigt, wie eine Amazon Redshift Redshift-Tabelle abgefragt wird.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Eine Tabelle abfragen.

```
    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 "";
```

```
    }
```

- Weitere API-Informationen finden Sie unter Query in der AWS SDK for Java 2.x -API-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Szenarien für Amazon Redshift mit SDKs AWS

Die folgenden Codebeispiele zeigen Ihnen, wie Sie gängige Szenarien in Amazon Redshift mit AWS SDKs implementieren. Diese Szenarien zeigen Ihnen, wie Sie bestimmte Aufgaben erledigen können, indem Sie mehrere Funktionen in Amazon Redshift aufrufen. Jedes Szenario enthält einen Link zu GitHub, über den Sie Anweisungen zur Einrichtung und Ausführung des Codes finden.

Beispiele

- Erste Schritte mit Amazon Redshift Redshift-Tabellen, -Elementen und -Abfragen

Erste Schritte mit Amazon Redshift Redshift-Tabellen, -Elementen und -Abfragen

Das folgende Codebeispiel zeigt, wie Sie mit Amazon Redshift Redshift-Tabellen, -Elementen und -Abfragen arbeiten.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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);
        }
    }
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for Java 2.x -API-Referenz.
  - createCluster

- Beschreiben Sie Cluster
- DESCRIBE-Aussage
- Anweisung ausführen
- getStatementResult
- listDatabasesPaginator
- Cluster ändern

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden Sie diesen Dienst mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Serviceübergreifende Beispiele für Amazon Redshift mit SDKs AWS

Die folgenden Beispielanwendungen verwenden AWS SDKs, um Amazon Redshift mit anderen zu kombinieren. AWS-Services Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zur Einrichtung und Ausführung der Anwendung finden.

Beispiele

- Erstellen eines Amazon-Redshift-Element-Trackers

Erstellen eines Amazon-Redshift-Element-Trackers

Die folgenden Code-Beispiele zeigen, wie Sie eine Webanwendung erstellen, die Arbeitselemente mit einer Amazon-Redshift-Datenbank verfolgt und darüber berichtet.

Java

SDK für Java 2.x

Zeigt, wie eine Webanwendung erstellt wird, die in einer Amazon-Redshift-Datenbank gespeicherte Arbeitselemente verfolgt und darüber berichtet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung einer Spring REST-API, die Amazon Redshift Redshift-Daten abfragt und von einer React-Anwendung verwendet werden kann, finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Redshift
- Amazon SES

Kotlin

SDK für Kotlin

Zeigt, wie eine Webanwendung erstellt wird, die in einer Amazon-Redshift-Datenbank gespeicherte Arbeitselemente verfolgt und darüber berichtet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung einer Spring REST-API, die Amazon Redshift Redshift-Daten abfragt und von einer React-Anwendung verwendet werden kann, finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Redshift
- Amazon SES

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Dokumentverlauf

> **Note**
>
> Eine Beschreibung der neuen Funktionen in Amazon Redshift finden Sie unter Was ist neu.

In der folgenden Tabelle werden die wichtigen Änderungen der Dokumentation zum Amazon Redshift Management Guide nach Juni 2018 beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

API-Version: 2012-12-01

Eine Liste der Änderungen am Datenbankentwicklerhandbuch zu Amazon Redshiftfinden Sie unter Dokumentverlauf für Datenbankentwicklerhandbuch zu Amazon Redshift.

Weitere Informationen zu neuen Funktionen, einschließlich einer Liste von Korrekturen und den zugehörigen Cluster-Versionsnummern, finden Sie im Cluster-Versionsverlauf.

Änderung	Beschreibung	Datum
Aktualisierung der verwalteten Richtlinien des Abfrage-Editors v2	Aktualisierungen von`AmazonRedshiftQueryEditorV2FullAccess` , `AmazonRedshiftQueryEditorV2NoSharing` `AmazonRedshiftQueryEditorV2ReadSharing` , und `AmazonRedshiftQueryEditorV2ReadWriteSharing` verwalteten Richtlinien mit Berechtigungen `redshift-serverless:ListNamespaces` und`redshift-serverless:ListWorkgroups` .	21. Februar 2024

Aktualisieren Sie die verwaltete Amazon Redshift Redshift-Richtlinie für schreibgeschützten Zugriff	Aktualisierungen der `AmazonRedshiftReadOnlyAccess` verwalteten Richtlinie mit der Erlaubnis `redshift:ListRecommendations`, Empfehlungen von Amazon Redshift Advisor aufzulisten.	7. Februar 2024
Amazon-Redshift-Patch 180 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 180.	29. Dezember 2023
Amazon-Redshift-Patch 179 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 179.	9. November 2023

Aktualisierung der von Amazon Redshift verwalteten Richtlinien	Aktualisierungen der verwalteten Richtlinie `AmazonRedshiftServiceLinkedRolePolicy` mit den Berechtigungen `ec2:AssignIpv6Addresses` und `ec2:UnassignIpv6Addresses` .	31. Oktober 2023
Amazon-Redshift-Patch 178 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 178.	25. September 2023
Aktualisierung der verwalteten Richtlinien des Abfrage-Editors v2	Aktualisierung der verwalteten Richtlinien `AmazonRedshiftQueryEditorV2NoSharing` , `AmazonRedshiftQueryEditorV2ReadSharing` und `AmazonRedshiftQueryEditorV2ReadWriteSharing` mit den Berechtigungen `sqlworkbench:GetAutocompletionMetadata` und `sqlworkbench:GetAutocompletionResource` .	16. August 2023

Aktualisierung der von Amazon Redshift verwalteten Richtlinie	Aktualisierungen der `AmazonRedshiftServiceLinkedRolePolicy` verwalteten Richtlinie zur Gewährung von Berechtigungen AWS Secrets Manager zur Erstellung und Verwaltung geheimer Administratoranmeldedaten.	14. August 2023
Amazon-Redshift-Patch 177 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 177.	3. August 2023
Amazon-Redshift-Patch 176 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 176.	08. Juni 2023

Amazon-Redshift-Patch 175 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 175.	28. April 2023
Aktualisierung der von Amazon Redshift verwalteten Richtlinie	Aktualisierungen der verwalteten Richtlinie `AmazonRedshiftServiceLinkedRolePolicy` zum Entfernen von Berechtigungen für ec2-Netzwerkaktionen. Diese wurden speziell mit dem RedshiftMigrateToVpc Resource-Tag Purpose: verknüpft.	27. April 2023
Aktualisierung der verwalteten Richtlinie für die Amazon Redshift Data API	Aktualisierungen der verwalteten Richtlinie `AmazonRedshiftDataFullAccess` mit der Berechtigung `redshift:GetClusterCredentialsWithIAM` .	7. April 2023

Aktualisierung der verwalteten Richtlinien des Abfrage-Editors v2	Aktualisierung der verwalteten Richtlinien `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` und `AmazonRedshiftQueryEditorV2ReadWriteSharing` mit der Berechtigung `sqlworkbench:GetSchemaInference`.	21. März 2023
Amazon-Redshift-Patch 174 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 174.	11. März 2023
Aktualisierung der verwalteten Richtlinien des Abfrage-Editors v2	Aktualisierung der verwalteten Richtlinien `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` und `AmazonRedshiftQueryEditorV2ReadWriteSharing` mit der Berechtigung `sqlworkbench:AssociateNotebookWithTab`.	2. Februar 2023

Amazon-Redshift-Patch 173 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 173.	20. Januar 2023
Amazon-Redshift-Patch 172 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 172.	17. November 2022
Amazon-Redshift-Patch 171 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 171.	9. November 2022

Amazon-Redshift-Patch 170 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 170.	20. Juli 2022
Amazon-Redshift-Patch 169 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 169.	08. Juni 2022
Amazon-Redshift-Patch 168 veröffentlicht.	Ein neuer Amazon-Redshift-Patch wird bereitgestellt. Es dauert mehrere Wochen, bis eine neue Version in allen unterstützten AWS-Regionen Amazon Redshift Redshift-Versionen verfügbar ist. Weitere Informationen über diese Version finden Sie unter Amazon-Redshift-Patch 168.	19. April 2022
Support für Authentifizierungsprofile mit Amazon-Redshift-Treibern	Sie können sich jetzt über ein Authentifizierungsprofil mit Amazon Redshift verbinden.	2. August 2021

Support für VPC-überg reifende Endpunkte für Amazon Redshift bereitgestellt von AWS PrivateLink	Sie können jetzt von Redshift verwaltete VPC-Endpunkte mit Amazon Redshift verwenden.	01. April 2021
Support für Verbesserungen beim Abfrage-Editor von Amazon Redshift	Sie können den Abfrage-Editor jetzt mit erweitertem VPC-Routing, längeren Abfrage-L aufzeiten und mehr Cluster-K notentypen verwenden.	17. Februar 2021
Unterstützung für die Konsolenintegration mit Partnern	Sie können über die Amazon-Redshift-Konsole eine Integrati on mit Partnern durchführen.	9. Dezember 2020
Unterstützung für das Verschieben von Clustern zwischen Availability Zones	Sie können RA3-Cluster jetzt zwischen Availability Zones verschieben.	9. Dezember 2020
Unterstützung für ra3.xlplus-Knotentypen	Sie können jetzt ra3.xlplus-Knotentypen erstellen.	9. Dezember 2020
Unterstützung für JDBC-Trei berversion 2.0	Sie können jetzt die JDBC-Trei berversion 2.0 konfigurieren.	5. November 2020
Unterstützung für Lambda-UD Fs und Aufgliederung in Token	Sie können jetzt Lambda-UD Fs schreiben, um eine externe Aufgliederung von Daten in Token zu ermöglichen.	26. Oktober 2020
Unterstützung für die Planung der Ausführung einer SQL-Anweisung	Sie können jetzt eine Abfrage in der Amazon-Redshift-Ko nsole planen.	22. Oktober 2020

Unterstützung für die Data API für Amazon Redshift	Auf Amazon Redshift kann nun über die integrierte Data API zugegriffen werden. Aktualisierungen der Dokumentation umfassen eine Amazon-Redshift-Data-API-Referenz.	10. September 2020
Unterstützung für die Überwachung von Abfragen der Amazon-Redshift-Konsole	Das Handbuch enthält nun Informationen zu neuen Abfrageüberwachungsdiagrammen.	7. Mai 2020
Unterstützung für Nutzungslimits	Das Handbuch zur Beschreibung der Nutzungslimits wurde aktualisiert.	23. April 2020
Multifaktor-Authentifizierung	Das Handbuch enthält nun Informationen zur Unterstützung von Multi-Faktor-Authentifizierung.	20. April 2020
Elastic Resize unterstützt jetzt Änderungen des Knotentyps	Die Beschreibung von Elastic Resize wurde aktualisiert.	6, 2020. April 2020
Unterstützung für ra3.4xlarge-Knotentypen mit verwaltetem Speicher	Das Handbuch wurde aktualisiert und enthält jetzt ra3.4xlarge-Knotentypen.	2. April 2020
Unterstützung für Anhalten und Fortsetzen	Das Handbuch wurde aktualisiert, um das Anhalten und Fortsetzen von Cluster-Operationen zu beschreiben.	11. März 2020

Unterstützung für Microsoft Azure AD als Identitätsanbieter	Das Handbuch wurde aktualisiert, um die Schritte zur Verwendung von Microsoft Azure AD als Identitätsanbieter zu beschreiben.	10. Februar 2020
Unterstützung für den RA3-Knotentyp	Das Handbuch enthält nun Informationen zum neuen RA3-Knotentyp.	3. Dezember 2019
Unterstützung für die neue Konsole	Das Handbuch enthält nun eine Beschreibung der neuen Amazon-Redshift-Konsole.	11. November 2019
Aktualisierungen der Sicherheitsinformationen	Aktualisierungen der Dokumentation in Bezug auf Sicherheitsinformationen.	24. Juni 2019
Snapshot-Erweiterungen	Amazon Redshift unterstützt jetzt mehrere Erweiterungen zum Verwalten und Planen von Snapshots.	4. April 2019
Nebenläufigkeitsskalierung	Sie können Workload-Management (WLM) für die Unterstützung des Nebenläufigkeitsskalierungsmodus konfigurieren. Weitere Informationen finden Sie unter Workload-Management-Konfiguration.	21. März 2019

Aktualisierte JDBC- und ODBC-Treiber	Amazon Redshift unterstützt jetzt neue Versionen der JDBC- und ODBC-Treiber. Weitere Informationen finden Sie unter Konfigurierung einer JDBC-Verbindung und Konfigurierung einer ODBC-Verbindung.	4. Februar 2019
Aufgeschobene Wartung	Wenn Sie den Zeitplan für das Wartungsfenster Ihres Clusters ändern müssen, können Sie die Wartung um bis zu 14 Tage aufschieben. Sollten während diesem Aufschub Hardware- oder andere obligatorische Updates durchgeführt werden müssen, setzen wir Sie diesbezüglich in Kenntnis und führen dann die Änderungen vor dem festgelegten Ende des Aufschubs durch. Während dieser Aktualisierungen ist Ihr Cluster nicht verfügbar. Weitere Informationen finden Sie unter Aufschieben der Wartung.	20. November 2018

Vorherige Benachrichtigung	Amazon Redshift informiert Sie bei bestimmten Ereignissen vorab. Diese Ereignisse haben die Ereigniskategorie `pending`. Wir informieren Sie beispielsweise vorab, wenn für einen der Knoten in Ihrem Cluster ein Hardwareupdate erforderlich ist. Sie können Ereignisse der Kategorie „pending“ wie andere Amazon Redshift-Ereignisse abonnieren. Weitere Informationen finden Sie unter Abonnieren von Amazon-Redshift-Ereignisbenachrichtigungen.	20. November 2018

Elastic resize (Elastische Größenanpassung	Die elastische Größenanpassung stellt die schnellste Möglichkeit für die Anpassung der Größe eines Clusters dar. Bei der elastischen Größenanpassung werden einem bestehenden Cluster Knoten hinzugefügt bzw. aus ihm entfernt. Anschließend werden die Daten automatisch auf die neuen Knoten umverteilt. Da bei diesem Vorgang kein neuer Cluster erstellt wird, nimmt die elastische Größenanpassung normalerweise nur wenige Minuten in Anspruch. Weitere Informationen finden Sie unter Größenanpassung von Clustern.	15. November 2018
Neue ODBC-Treiber	Die Amazon-Redshift-ODBC-Treiber wurden zu Version 1.4.3.1000 aktualisiert. Weitere Informationen finden Sie unter Konfigurierung einer ODBC-Verbindung.	8. November 2018
Abbrechen der Größenanpassung	Sie können jetzt eine Größenanpassung abbrechen, die gerade ausgeführt wird. Weitere Informationen finden Sie unter Übersicht über die Größenanpassung.	2. November 2018

Ändern der Verschlüsselung durch Anpassung des Clusters	Sie können einen unverschlüsselten Cluster so ändern, dass er die Verschlüsselung AWS Key Management Service (AWS KMS) verwendet, indem Sie entweder einen AWS-verwalteten Schlüssel oder einen vom Kunden verwalteten Schlüssel verwenden. Wenn Sie Ihren Cluster bearbeiten, um die KMS-Verschlüsselung zu aktivieren, migriert Amazon Redshift Ihre Daten automatisch in einen neuen, verschlüsselten Cluster. Sie können auch einen unverschlüsselten Cluster in einem verschlüsselten Cluster migrieren, indem Sie den Cluster anpassen.	16. Oktober 2018
Amazon Redshift Spectrum unterstützt Enhanced VPC Routing	Sie können jetzt für Ihren Cluster Redshift Spectrum mit Enhanced VPC Routing verwenden. Möglicherweise müssen Sie weiteren Schritte zur Konfigurierung durchführen. Weitere Informationen finden Sie unter Verwenden von Amazon Redshift Spectrum mit Enhanced VPC Routing.	10. Oktober 2018

Abfrage-Editor	Sie können jetzt über die Amazon-Redshift-Managementkonsole SQL-Abfragen ausführen.	4. Oktober 2018
Workload Execution Breakdown-Tabelle (Aufgliederung der Workload-Ausführung	Eine detaillierte Ansicht der Leistung Ihrer Workload finden jetzt Sie in der Workload Execution Breakdown-Tabelle (Aufgliederung der Workload-Ausführung) auf der Konsole. Weitere Informationen finden Sie unter Analysieren der Workload-Leistung.	30. Juli 2018
Wartungspfade	Sie können jetzt festlegen, ob Ihr Cluster stets auf die neueste Version von Amazon Redshift oder auf eine Vorversion aktualisiert wird, indem Sie einen Wartungspfad auswählen. Weitere Informationen finden Sie unter Auswählen des Cluster-Wartungspfads.	26. Juli 2018

In der folgenden Tabelle sind die wichtigsten Änderungen am Amazon-Redshift-Verwaltungshandbuch vor Juli 2018 beschrieben.

Änderung	Beschreibung	Datum der Veröffentlichung
Neue Metriken CloudWatch	Neue CloudWatch Metriken zur Überwachung der Abfrageleistung hinzugefügt. Weitere Informationen finden Sie unter Überwachung von Amazon Redshift mithilfe von Metriken CloudWatch	17. Mai 2018

Änderung	Beschreibung	Datum der Veröffentlichung
HSM-Verschlüsselung	Amazon Redshift unterstützt nur die Schlüsselverwaltung AWS CloudHSM für Hardware-Sicherheitsmodule (HSM). Weitere Informationen finden Sie unter Verschlüsselung von Amazon-Redshift-Datenbanken.	6. März 2018
Verketten von IAM-Rollen	Wenn eine an den Cluster angefügte IAM-Rolle keinen Zugriff auf die erforderlichen Ressourcen hat, können Sie eine andere Rolle verketten, die möglicherweise zu einem anderen Konto gehört. Ihr Cluster nimmt dann vorübergehend die verkettete Rolle an, um auf die Daten zuzugreifen. Sie können über verkettete Rollen auch kontoübergreifenden Zugriff gewähren. Jede Rolle in der Kette nimmt die nächste Rolle in der Kette an, bis hin zum Cluster, der die Rolle am Ende der Kette annimmt. Sie können maximal 10 Rollen miteinander verketten. Weitere Informationen finden Sie unter Verketten von IAM-Rollen in Amazon Redshift.	23. Februar 2018
Neue DC2-Knotentypen	Die neue Generation von Knoten der Dense Compute (DC)-Typen bietet eine deutlich bessere Leistung zum selben Preis wie DC1. Um von der verbesserten Leistung zu profitieren, können Sie ihre DC1-Cluster auf die neueren DC2-Knotentypen migrieren. Weitere Informationen finden Sie unter Cluster und Knoten in Amazon Redshift.	17. Oktober 2017

Änderung	Beschreibung	Datum der Veröffentlichung
ACM-Zertifikate	Amazon Redshift ersetzt die SSL-Zertifikate auf Ihren Clustern durch AWS Certificate Manager (ACM) ausgestellte Zertifikate. ACM ist eine vertrauen swürdige öffentliche Zertifizierungsstelle, der die meisten Systeme vertrauen. Sie müssen möglicher weise Ihre aktuellen vertrauenswürdigen CA-Stammzertifikate aktualisieren, um weiterhin mit SSL Verbindungen zu Ihren Clustern herstellen zu können. Weitere Informationen finden Sie unter Umstellung auf ACM-Zertifikate für SSL-Verbindungen.	18. September 2017
Service-verknüpfte Rollen	Eine serviceverknüpfte Rolle ist ein spezieller Typ von IAM-Rolle, der direkt mit Amazon Redshift verknüpft ist. Servicebezogene Rollen sind von Amazon Redshift vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um AWS Services im Namen Ihres Amazon Redshift Redshift-Clusters aufzurufe n. Weitere Informationen finden Sie unter Verwenden serviceverknüpfter Rollen für Amazon Redshift.	18. September 2017
IAM-Daten bankbenut zerauthentifizieru ng	Sie können Ihr System so konfigurieren, dass es Benutzern erlaubt, Benutzeranmeldeinformatione n zu erstellen und sich auf Basis ihrer IAM-Anmel deinformationen an der Datenbank anzumelden. Sie können Ihr System auch so konfigurieren, dass Benutzer durch einen SAML-2.0-konformen Identität sanbieter ein Verbund-Single-Sign-On nutzen können. Weitere Informationen finden Sie unter Verwenden der IAM-Authentifizierung zur Erstellung von Anmeldein formationen für Datenbankbenutzern.	11. August 2017

Änderung	Beschreibung	Datum der Veröffentlichung
Wiederherstellung auf Tabellenebene unterstützt Enhanced VPC Routing	Die Wiederherstellung auf Tabellenebene wird jetzt auf Clustern unterstützt, die verwenden Enhanced VPC routing (Erweitertes VPC-Routing. Weitere Informationen finden Sie unter Wiederherstellen einer Tabelle aus einem Snapshot.	19. Juli 2017
Abfrageüberwachungsregeln	Mithilfe der WLM-Abfrageüberwachungsregeln definieren Sie auf Metriken basierende Leistungsgrenzen für WLM-Warteschlangen und geben an, welche Aktion durchgeführt werden soll, wenn eine Abfrage diese Grenzwerte überschreitet (log, hop, abort). Sie definieren die Abfrageüberwachungsregeln im Rahmen Ihrer Workload Management (WLM)-Konfiguration. Weitere Informationen finden Sie unter Workload-Management-Konfiguration.	21. April 2017
Enhanced VPC routing (Erweitertes VPC-Routing	Wenn Sie Enhanced VPC Routing für Amazon Redshift verwenden, erzwingt Amazon Redshift, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Ihren Datenrepositorys über Ihre Amazon VPC erfolgt. Weitere Informationen finden Sie unter Enhanced VPC Routing in Amazon Redshift.	15. September 2016
Neue Verbindungsprotokoll-Felder	Das Auditprotokoll Verbindungsprotokoll hat zwei neue Felder zur Verfolgung von SSL-Verbindungen. Wenn Sie routinemäßig Audit-Protokolle in eine Amazon Redshift-Tabelle laden, müssen Sie der Zieltabelle die folgenden neuen Spalten hinzufügen: sslcompression und sslexpansion.	5. Mai 2016

Änderung	Beschreibung	Datum der Veröffentlichung
Neue ODBC-Treiber	Die Amazon-Redshift-ODBC-Treiber wurden zu Version 1.2.7.1007 aktualisiert. Weitere Informationen finden Sie unter Konfigurierung einer ODBC-Verbindung.	30. März 2016
IAM-Rollen für COPY und UNLOAD	Sie können jetzt eine oder mehrere AWS Identity and Access Management (IAM) -Rollen angeben, die Ihr Cluster für die Authentifizierung für den Zugriff auf andere Dienste verwenden kann. AWS IAM-Rollen bieten eine sicherere Alternative zur Authentifizierung mit den Befehlen COPY, UNLOAD oder CREATE LIBRARY. Weitere Informationen erhalten Sie unter Amazon Redshift autorisieren, in Ihrem Namen auf andere AWS Dienste zuzugreifen und Autorisieren der Vorgänge COPY, UNLOAD, CREATE EXTERNAL FUNCTION und CREATE EXTERNAL SCHEMA mithilfe von IAM-Rollen.	29. März 2016
Wiederherstellung aus Tabelle	Sie können eine Tabelle aus einem Cluster-Snapshot zu einer neuen Tabelle in einem aktiven Cluster wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen einer Tabelle aus einem Snapshot.	10. März 2016
Verwenden von IAM-Bedingungen in Richtlinien	Sie können den Zugriff auf Ressourcen weiter einschränken, indem Sie das Condition-Element in IAM-Richtlinien verwenden. Weitere Informationen finden Sie unter Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle.	10. Dezember 2015
Modifizierung der öffentlichen Zugänglichkeit	Sie können für einen bestehenden Cluster in einer VPC ändern, ob dieser öffentlich zugänglich ist oder nicht. Weitere Informationen finden Sie unter Modifizieren eines Clusters.	20. November 2015

Änderung	Beschreibung	Datum der Veröffentlichung
Korrekturen der Dokumentation	Veröffentlichung verschiedener Korrekturen an der Dokumentation.	28. August 2015
Aktualisierung der Dokumentation	Aktualisierung der Anleitung zur Fehlerbehebung zur Konfiguration der Netzwerkeinstellungen, um sicherzustellen, dass Hosts mit unterschiedlichen MTU- (Maximum Transmission Unit) Größen die Paketgröße für eine Verbindung bestimmen können. Weitere Informationen finden Sie unter Abfragen scheinen zu hängen und erreichen manchmal den Cluster nicht.	25. August 2015
Aktualisierung der Dokumentation	Revision des gesamten Abschnitts zu Parameter gruppen für eine bessere Organisation und größere Klarheit. Weitere Informationen finden Sie unter Amazon-Redshift-Parametergruppen.	17. August 2015
Dynamische WLM-Eigenschaften	Der WLM-Konfigurationsparameter unterstützt jetzt die dynamische Anwendung einiger Eigenschaften. Andere Eigenschaften bleiben weiterhin statische Änderungen und erfordern, dass die verbundenen Cluster neu gestartet werden, damit die Konfigura tionsänderungen wirksam werden. Weitere Informati onen erhalten Sie unter Dynamische und statische WLM-Eigenschaften und Amazon-Redshift-Pa rametergruppen.	3. August 2015
Kopieren Sie KMS-verschlüsselte Cluster in eine andere Region AWS	Es wurden Inhalte zur Konfiguration von Snapshot-Kopierberechtigungen hinzugefügt, um das Kopieren von AWS KMS-verschlüsselten Clustern in eine andere AWS Region zu ermöglichen. Weitere Informati onen finden Sie unter Kopieren von —verschlüsselten Snapshots in eine andere Region AWS KMSAWS.	28. Juli 2015

Änderung	Beschreibung	Datum der Veröffentlichung
Aktualisierung der Dokumentation	Der Abschnitt zur Datenbankverschlüsselung wurde aktualisiert, um besser zu erklären, wie Amazon Redshift HSMs für die Verwaltung von Schlüsseln verwendet AWS KMS und wie der Verschlüsselungsprozess mit jeder dieser Optionen funktioniert. Weitere Informationen finden Sie unter Verschlüsselung von Amazon-Redshift-Datenbanken.	28. Juli 2015
Neuer Knotentyp	Amazon Redshift bietet jetzt einen neuen Knotentyp , DS2. Die aktualisierte Dokumentation erwähnt, dass die vorhandenen Knotentypen in dieser Version eingeführte neue Namen verwenden. Dazu wurde der Abschnitt revidiert, um die Kombinationen von Knotentypen besser zu erläutern und die Standard-Kontingenttypen zu erklären. Weitere Informationen finden Sie unter Cluster und Knoten in Amazon Redshift.	9. Juni 2015
Angebote reservierter Knoten	Neuer Inhalt zu neuen Angeboten reservierter Knoten. Weitere Revision des Abschnitts zur besseren Erläuterung und zum Vergleich der verfügbaren Angebote sowie Beispiele, die zeigen, wie sich die Preise für On-Demand- und reservierte Knoten auf die Fakturierung auswirken. Weitere Informationen finden Sie unter Übersicht.	9. Juni 2015
Neue ODBC-Treiber	Die Amazon-Redshift-ODBC-Treiber wurden aktualisiert. Hinzufügung eines Abschnitts zu vorherigen Versionen dieser Treiber und eines Links zu den Versionshinweisen dazu. Weitere Informationen finden Sie unter Konfigurierung einer ODBC-Verbindung.	5. Juni 2015
Korrekturen der Dokumentation	Veröffentlichung verschiedener Korrekturen an der Dokumentation.	30. April 2015

Änderung	Beschreibung	Datum der Veröffentlichung
Neue Funktion	Mit dieser Version von Amazon Redshift werden neue ODBC- und JDBC-Treiber vorgestellt, die zur Verwendung mit Amazon Redshift optimiert sind. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu einem Amazon Redshift Data Warehouse mithilfe von SQL-Client-Tools.	26. Februar 2015
Neue Funktion	Mit dieser Version von Amazon Redshift werden Cluster-Leistungsmetriken eingeführt, mit deren Hilfe Sie Details zur Abfrageausführung anzeigen und analysieren können. Weitere Informationen finden Sie unter Anzeigen von Abfragen und Ladevorgänge.	26. Februar 2015
Aktualisierung der Dokumentation	Es wurde eine neue Beispielrichtlinie hinzugefügt, die die Erteilung von Berechtigungen für allgemeine AWS Serviceaktionen und Ressourcen demonstriert, auf die sich Amazon Redshift stützt. Weitere Informationen finden Sie unter Beispiele für vom Kunden verwaltete Richtlinien.	16. Januar 2015
Aktualisierung der Dokumentation	Aktualisierung der Anleitung zur Einrichtung der MTU (Maximum Transmission Unit) zur Deaktivierung von TCP/IP-Jumbo-Frames. Weitere Informationen erhalten Sie unter Verwenden von EC2-VPC beim Erstellen Ihres Clusters und Abfragen scheinen zu hängen und erreichen manchmal den Cluster nicht.	16. Januar 2015
Aktualisierung der Dokumentation	Der Inhalt des `wlm_json_configuration` Parameters wurde überarbeitet und eine Beispiels yntax für die Konfiguration dieses Parameters mithilfe der AWS CLI auf den Betriebssystemen Linux, Mac OS X und Microsoft Windows bereitgestellt. Weitere Informationen finden Sie unter Workload-Management-Konfiguration.	13. Januar 2015

Änderung	Beschreibung	Datum der Veröffentlichung
Aktualisierung der Dokumentation	Hinzufügung fehlender Ereignisbenachrichtigungen und -beschreibungen. Weitere Informationen finden Sie unter Amazon-Redshift-Ereigniskategorien und -Ereignismeldungen.	8. Januar 2015
Aktualisierung der Dokumentation	Aktualisierung der Anleitung zu IAM-Richtlinien für Amazon-Redshift-Aktionen und -Ressourcen. Revision des Abschnitts zur Verbesserung von Organisation und Klarheit. Weitere Informationen finden Sie unter Sicherheit in Amazon Redshift.	21. November 2014
Neues Feature	Diese Version von Amazon Redshift bietet die Möglichkeit, Cluster mithilfe von Verschlüsselungsschlüsseln von AWS Key Management Service ()AWS KMS zu verschlüsseln. AWS KMS kombiniert sichere, hochverfügbare Hardware und Software, um ein für die Cloud skaliertes Schlüsselverwaltungssystem bereitzustellen. Weitere Informationen zu AWS KMS und Verschlüsselungsoptionen für Amazon Redshift finden Sie unter Verschlüsselung von Amazon-Redshift-Datenbanken undVerwalten von Clustern mithilfe der Konsole.	12. November 2014
Neue Funktion	Mit dieser Version von Amazon Redshift wird die Möglichkeit zum Markieren von Ressourcen, wie Clustern und Snapshots, eingeführt. Mit Tags können Sie benutzerdefinierte Metadaten angeben, um Ihre Fakturierungsberichte auf der Grundlage der Kostenzuweisung zu kategorisieren, und um Ressourcen besser auf einen Blick identifizieren zu können. Weitere Informationen finden Sie unter Markieren von Ressourcen in Amazon Redshift.	4. November 2014

Änderung	Beschreibung	Datum der Veröffentlichung
Neue Funktion	Die maximale Knotengrenze wurde auf 128 Knoten für die Knotengrößen dw1.8xlarge und dw2.8xlarge erweitert. Weitere Informationen finden Sie unter Cluster und Knoten in Amazon Redshift.	30. Oktober 2014
Aktualisierung der Dokumentation	Hinzufügung von Links zu den Microsoft Visual C++ 2010 Redistributable Packages, die zur Verwendung der PostgreSQL-ODBC-Treiber durch Amazon Redshift erforderlich sind. Weitere Informationen finden Sie unter Installation und Konfigurierung des Amazon-Redshift-ODBC-Treibers auf Microsoft Windows.	30. Oktober 2014
Neue Funktion	Hinzufügung der Möglichkeit zum Beenden von Abfragen und Ladevorgängen über die Amazon-Redshift-Konsole. Weitere Informationen erhalten Sie unter Anzeigen von Abfragen und Ladevorgänge und Anzeigen von Cluster-Metriken während der Ausführung von Lade-Operationen.	28. Oktober 2014
Korrekturen der Dokumentation	Veröffentlichung verschiedener Korrekturen an der Dokumentation.	17. Oktober 2014
Neuer Inhalt	Hinzufügen von Inhalt zum Schließen und Löschen von Clustern. Weitere Informationen erhalten Sie unter Schließen und Löschen von Clustern und Löschen eines Clusters.	14. August 2014
Aktualisierung der Dokumentation	Klärung der Verhaltensweise der Einstellung Allow Version Upgrade für Cluster. Weitere Informationen finden Sie unter Überblick über Amazon Redshift.	14. August 2014

Änderung	Beschreibung	Datum der Veröffentlichung
Aktualisierung der Dokumentation	Überarbeitung der Verfahren, Screenshots und Organisation des Themas zur Arbeit mit Clustern in der Amazon-Redshift-Konsole. Weitere Informationen finden Sie unter Verwalten von Clustern mithilfe der Konsole.	11. Juli 2014
Neuer Inhalt	Hinzufügung eines neuen Tutorials zur Größenanpassung von Amazon-Redshift-Clustern, einschließlich der Vorgehensweise zur Größenanpassung eines Clusters bei gleichzeitiger Minimierung der Zeit, während der sich der Cluster im schreibgeschützten Modus befindet. Weitere Informationen finden Sie unter Größenanpassung von Clustern.	27. Juni 2014
Neue Funktion	Hinzufügung der Möglichkeit zum Umbenennen von Clustern. Weitere Informationen erhalten Sie unter Umbenennen von Clustern und Modifizieren eines Clusters.	2. Juni 2014
Aktualisierung der Dokumentation	Aktualisierung des .NET-Code-Beispiels zur Verwendung des ODBC-Datenanbieters bei der programmatischen Verbindung zu einem Cluster mit .NET. Weitere Informationen finden Sie unter Stellen Sie programmgesteuert Connect zu Ihrem Data Warehouse her.	15. Mai 2014
Neue Funktion	Hinzufügung von Optionen zur Auswahl einer anderen Parameter- und Sicherheitsgruppe bei der Wiederherstellung eines Clusters von einem Snapshot. Weitere Informationen finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot.	12. Mai 2014

Änderung	Beschreibung	Datum der Veröffentlichung
Neues Feature	Es wurde ein neuer Abschnitt hinzugefügt, in dem beschrieben wird, wie ein standardmäßiger CloudWatch Amazon-Alarm konfiguriert wird, um den Prozentsatz des in einem Amazon Redshift-Cluster verwendeten Festplattenspeichers zu überwachen. Dieser Alarm ist eine neue Option im Cluster-Erstellungsprozess. Weitere Informationen finden Sie unter Standard-Festplattenspeicherplatzalarm.	28. April 2014
Aktualisierung der Dokumentation	Klärung der Informationen zur Unterstützung von Elliptic Curve Diffie-Hellman Exchange (ECDHE) in Amazon Redshift. Weitere Informationen finden Sie unter Verbindung über SSL.	22. April 2014
Neue Funktion	Hinzufügung einer Aussage zur Amazon-Redshift-Unterstützung des Schlüsselverwaltungsprotokolls für Elliptic Curve Diffie-Hellman Exchange (ECDHE). Weitere Informationen finden Sie unter Verbindung über SSL.	18. April 2014
Aktualisierung der Dokumentation	Revision und Umorganisierung der Themen im Abschnitt Herstellen einer Verbindung zu einem Amazon Redshift Data Warehouse mithilfe von SQL-Client-Tools. Hinzufügung weiterer Informationen zu JDBC- und ODBC-Verbindungen sowie eines neuen Abschnitts zur Behebung von Verbindungsproblemen.	15. April 2014
Aktualisierung der Dokumentation	Hinzufügung der Version in Beispielen zu IAM-Richtlinien in der gesamten Anleitung.	3. April 2014
Aktualisierung der Dokumentation	Hinzufügung von Informationen zu den preisen bei der Größenanpassung eines Clusters. Weitere Informationen finden Sie unter Kaufen reservierter Amazon-Redshift-Knoten.	2. April 2014

Änderung	Beschreibung	Datum der Veröffentlichung
Neue Funktion	Hinzufügung eines Abschnitts über den neuen Parameter `max_cursor_result_set_size` der die maximale Größe des Ergebnisdatensatzes festlegt, der pro einzelnem Cursor gespeichert werden kann. Dieser Parameterwert wirkt sich auch auf die Anzahl der gleichzeitig aktiven Cursors für den Cluster aus. Weitere Informationen finden Sie unter Amazon-Redshift-Parametergruppen.	28. März 2014
Neue Funktion	Hinzufügung einer Erläuterung zum Feld Cluster Version, das jetzt die Cluster-Engine-Version und die Versionsnummer der Datenbank enthält. Weitere Informationen finden Sie unter Von Amazon Redshift bereitgestellte Cluster.	21. März 2014
Neue Funktion	Aktualisierung des Vorgangs der Größenanpassung zur Anzeige der Fortschrittsinformationen auf der Registerkarte Status des Clusters. Weitere Informationen finden Sie unter Größenanpassung eines Clusters.	21. März 2014
Aktualisierung der Dokumentation	Umorganisation und Aktualisierung von Was ist Amazon Redshift? sowie Revision von Bereitgestellte Amazon-Redshift-Cluster – Überblick. Veröffentlichung verschiedener Korrekturen an der Dokumentation.	21. Februar 2014
Neue Funktion	Hinzufügung neuer Knotentypen und -größen für Amazon-Redshift-Cluster und Umformulierung des zugehörigen Themas zur Cluster-Übersicht für bessere Organisation und mehr Klarheit auf der Grundlage von Feedback. Weitere Informationen finden Sie unter Von Amazon Redshift bereitgestellte Cluster.	23. Januar 2014

Änderung	Beschreibung	Datum der Veröffentlichung
Neue Funktion	Hinzufügung von Informationen zur Verwendung elastischer IP-Adressen (EIP) für öffentlich zugänglic he Amazon-Redshift-Cluster in Virtual Private Clouds. Weitere Informationen zu EIP in Amazon Redshift finden Sie unter Verwaltung von Clustern in einer VPC und Erstellen eines Clusters in einer VPC.	20. Dezember 2013
Neues Feature	Es wurden Informationen zu den AWS CloudTrail Protokollen für Amazon Redshift hinzugefügt. Weitere Informationen zur Amazon Redshift Redshift-Unterstüt zung für finden Sie CloudTrail unterProtokollieren mit CloudTrail.	13. Dezember 2013
Neue Funktion	Hinzufügung von Informationen zum neuen Benutzera ktivitätsprotokoll und zum `enable_user_activi ty_logging` -Datenbankparameter für die Datenbankprüfungs-Protokollierungsfunktion in Amazon Redshift. Weitere Informationen zur Datenbankaudit-Protokollierung finden Sie unter Datenbank-Prüfungsprotokollierung. Weitere Informati onen zu Datenbankparametern finden Sie unter Amazon-Redshift-Parametergruppen.	6. Dezember 2013
Neues Feature	Es wurde aktualisiert, um die Konfiguration von Amazon Redshift für das automatische Kopieren automatisierter und manueller Snapshots in eine sekundäre AWS Region zu beschreiben. Weitere Informationen zur Konfiguration der regionenübergreife nden Snapshot-Kopie finden Sie unter Kopieren von Snapshots in eine andere AWS -Region.	14. November 2013

Änderung	Beschreibung	Datum der Veröffentlichung
Neue Funktion	Hinzufügung eines Abschnitts zur Beschreibung der Amazon-Redshift-Prüfungsprotokollierung für Verbindungen und Benutzeraktivitäten sowie zur Speicherung dieser Protokolle in Amazon S3. Weitere Informationen zur Datenbankaudit-Protokollierung finden Sie unter Datenbank-Prüfungsprotokollierung.	11. November 2013
Neue Funktion	Hinzufügung eines Abschnitts zur Beschreibung der Amazon-Redshift-Verschlüsselung mit neuen Funktionen zur Verwaltung von Verschlüsselungsschlüsseln in einem Hardwaresicherheitsmodul (HSM) und zur Rotation von Verschlüsselungsschlüsseln. Für weitere Informationen zur Verschlüsselung, zu HSM und zur Schlüsselrotation vgl. Verschlüsselung von Amazon-Redshift-Datenbanken, Verschlüsselung für Amazon Redshift mit Hardwaresicherheitsmodulen und Rotation von Verschlüsselungsschlüsseln in Amazon Redshift.	11. November 2013
Neue Funktion	Aktualisierter Inhalt zur Beschreibung der Veröffentlichung von Benachrichtigungen zu Amazon-Redshift-Ereignissen über Amazon SNS. Informationen zu Amazon-Redshift-Ereignisbenachrichtigungen finden Sie unter Ereignisbenachrichtigungen zu Amazon Redshift.	11. November 2013
Neue Funktion	Aktualisierter Inhalt zur Beschreibung von IAM-Berechtigungen auf Ressourcenebene. Weitere Informationen zu Amazon-Redshift-IAM-Berechtigungen finden Sie unter Sicherheit in Amazon Redshift.	9. August 2013

Änderung	Beschreibung	Datum der Veröffentlichung
Neue Funktion	Aktualisierung zur Beschreibung der Metriken zum Wiederherstellungsvorgang. Weitere Informationen finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot.	9. August 2013
Neue Funktion	Aktualisierung zur Beschreibung der Freigabe von Cluster-Snapshots und der Erstellung von Metriken zum Snapshot-Fortschritt. Weitere Informationen finden Sie unter Freigeben eines Snapshots.	17. Juli 2013
Korrekturen der Dokumentation	Veröffentlichung verschiedener Korrekturen an der Dokumentation.	8. Juli 2013
Neue Konsolenbildschirme	Aktualisierung des Amazon-Redshift-Verwaltungshandbuchs, um Änderungen an der Amazon-Redshift-Konsole widerzuspiegeln.	22. April 2013
Neues Handbuch	Dies ist die erste Version des Amazon-Redshift-Verwaltungshandbuchs.	14. Februar 2013

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.