



Panduan Manajemen

Amazon Redshift



Amazon Redshift: Panduan Manajemen

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan antara para pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan kekayaan masing-masing pemiliknya, yang mungkin atau mungkin tidak berafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu Amazon Redshift?	1
Apakah Anda pengguna Amazon Redshift pertama kali?	1
Ikhtisar fitur Amazon Redshift Tanpa Server	2
Ikhtisar cluster yang disediakan Amazon Redshift	5
Manajemen klaster	5
Akses dan keamanan klaster	6
Cluster pemantauan	8
Basis Data	9
Membandingkan Amazon Redshift Tanpa Server dengan gudang data yang disediakan Amazon Redshift	9
Menggunakan antarmuka manajemen Amazon Redshift untuk cluster yang disediakan	35
Bekerja dengan AWS SDK	36
Menandatangani permintaan HTTP	37
Menyiapkan Amazon Redshift CLI	42
Amazon Redshift Tanpa Server	44
Apa itu Amazon Redshift Tanpa Server?	44
Konsol Tanpa Server Amazon Redshift	45
Pertimbangan saat menggunakan Amazon Redshift Serverless	48
Kapasitas komputasi untuk Amazon Redshift Serverless	51
Memahami kapasitas Amazon Redshift Tanpa Server	51
Penskalaan dan pengoptimalan berbasis AI (pratinjau)	52
Penagihan untuk Amazon Redshift Tanpa Server	54
Harga	54
Penagihan untuk kapasitas komputasi	54
Penagihan untuk penyimpanan	59
Menggunakan uji coba gratis Amazon Redshift Serverless	59
Catatan penggunaan penagihan	60
Menghubungkan ke Amazon Redshift Tanpa Server	61
Menghubungkan ke Amazon Redshift Tanpa Server	62
Menghubungkan ke Amazon Redshift Tanpa Server melalui driver JDBC	62
Menghubungkan ke Amazon Redshift Tanpa Server dengan API Data	64
Menghubungkan dengan SSL ke Amazon Redshift Tanpa Server	64
Menghubungkan ke Amazon Redshift Tanpa Server dari titik akhir VPC yang dikelola Amazon Redshift	67

Menghubungkan ke Amazon Redshift Tanpa Server dari titik akhir VPC Redshift di akun atau wilayah lain	67
Mengonfigurasi pengaturan lalu lintas jaringan yang sesuai untuk Amazon Redshift Serverless	72
Mendefinisikan peran database yang akan diberikan kepada pengguna federasi di Amazon Redshift Tanpa Server	72
Sumber daya tambahan	72
Mendefinisikan peran database yang akan diberikan kepada pengguna federasi di Amazon Redshift Tanpa Server	73
Manajemen identitas dan akses di Amazon Redshift Tanpa Server	76
Memberikan izin ke Amazon Redshift Tanpa Server	76
Memulai dengan kredensi IAM untuk Amazon Redshift	78
Mengelola akses ke objek database Amazon Redshift Tanpa Server dengan izin peran basis data	80
Memigrasi kluster yang disediakan ke Amazon Redshift Tanpa Server	81
Membuat snapshot dari kluster yang Anda sediakan	81
Menghubungkan ke Amazon Redshift Tanpa Server menggunakan driver	82
Menggunakan Amazon Redshift Serverless SDK	85
Ikhtisar grup kerja dan ruang nama Amazon Redshift Tanpa Server	85
Ikhtisar grup kerja dan ruang nama Amazon Redshift Tanpa Server	85
Mengelola Amazon Redshift Tanpa Server menggunakan konsol	88
Menyiapkan Amazon Redshift Tanpa Server untuk pertama kalinya	88
Bekerja dengan kelompok kerja	88
Bekerja dengan ruang nama	93
Mengelola batas penggunaan, batas kueri, dan tugas administratif lainnya	97
Memantau kueri dan beban kerja dengan Amazon Redshift Serverless	100
Memantau kueri dan beban kerja dengan Amazon Redshift Serverless	100
Pencatatan audit untuk Amazon Redshift Tanpa Server	104
Mengekspor log	104
Bekerja dengan snapshot dan titik pemulihan	114
Snapshot	115
Poin pemulihan	118
Menjadwalkan snapshot	119
Menyalin cadangan ke yang lain Wilayah AWS	121
Memulihkan tabel	123

Menggunakan API Tanpa AWS Command Line Interface Server Amazon Redshift dan Amazon	124
Berbagi data di Amazon Redshift Tanpa Server	127
Berbagi data di Amazon Redshift Tanpa Server	127
Memberi tag pada sumber daya	129
Cluster yang disediakan Amazon Redshift	131
Ikhtisar Amazon Redshift	131
Cluster dan node	131
Gunakan EC2-VPC saat Anda membuat cluster	137
EC2-VPC	138
Alarm ruang disk default	138
Status klaster	139
Pertimbangan untuk menggunakan cluster yang disediakan Amazon Redshift	141
Pertimbangan Wilayah dan Availability Zone	142
Pemeliharaan cluster	142
Mengelola batas penggunaan	148
Fitur jaringan yang didukung oleh node RA3	150
Jenis simpul	151
Operasi cluster	157
Mengubah ukuran cluster	158
Menjeda dan melanjutkan cluster	173
Mengganti nama cluster	175
Mematikan dan menghapus cluster	177
Merelokasi klaster Anda	177
Snapshot dan backup	182
Mengkonfigurasi penyebaran Multi-AZ	210
Menyiapkan penyebaran Multi-AZ	211
Mengelola penyebaran Multi-AZ	214
Gagal dalam penerapan Multi-AZ	221
Pemantauan kueri untuk Multi-AZ	223
Mengelola cluster menggunakan konsol	225
Membuat klaster	226
Membuat klaster pratinjau	229
Mengubah klaster	230
Menghapus klaster	232
Melakukan boot ulang klaster	233

Mengubah ukuran cluster	233
Memutakhirkan versi rilis cluster	234
Mendapatkan informasi tentang konfigurasi cluster	234
Mendapatkan ikhtisar status cluster	235
Membuat snapshot dari sebuah cluster	235
Membuat atau mengedit alarm ruang disk	235
Bekerja dengan data kinerja cluster	236
Mengelola cluster menggunakan API Amazon AWS CLI Redshift dan Amazon	236
Mengelola cluster dalam VPC	237
Gambaran Umum	237
Membuat cluster di VPC	240
Mengelola grup keamanan VPC untuk sebuah cluster	241
Mengonfigurasi setelan komunikasi grup keamanan untuk klaster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server	243
Bagaimana Amazon Redshift bekerja dengan berbagi VPC untuk sumber daya AWS	246
Grup subnet cluster	247
Riwayat versi cluster	250
Bekerja dengan integrasi nol-ETL	251
Pertimbangan	253
Mulai menggunakan integrasi nol-ETL	255
Membuat dan mengonfigurasi gudang data Amazon Redshift target	256
Nyalakan sensitivitas casing	258
Konfigurasi otorisasi di Amazon Redshift	260
Langkah selanjutnya	264
Membuat database tujuan	264
Membuat database tujuan di Amazon Redshift	265
Tambahkan data ke sumber Anda	266
Menanyakan dan membuat tampilan terwujud dengan data yang direplikasi	267
Menanyakan data yang direplikasi di Amazon Redshift	267
Membuat tampilan terwujud dengan data yang direplikasi	267
Mengelola integrasi nol-ETL	269
Berbagi data Anda di Amazon Redshift	271
Metrik untuk integrasi nol-ETL	272
Memecahkan masalah integrasi nol-ETL	274
Meminta database	284
Menghubungkan ke Amazon Redshift	285

Mengkueri database menggunakan editor kueri Amazon Redshift v2	285
Mengkonfigurasi Akun AWS	287
Bekerja dengan editor kueri v2	294
Berinteraksi dengan editor kueri v2 generatif SQL (pratinjau)	312
Memuat data ke dalam database	320
Menulis dan menjalankan kueri	329
Menulis dan menjalankan notebook	335
Menanyakan AWS Glue Data Catalog	339
Menanyakan data lake	342
Bekerja dengan datashares	345
Menjadwalkan kueri	348
Memvisualisasikan hasil	358
Berkolaborasi dan berbagi sebagai sebuah tim	364
Menanyakan database menggunakan editor kueri	366
Pertimbangan	367
Mengaktifkan akses	368
Menghubungkan dengan editor kueri	369
Menggunakan editor kueri	370
Menjadwalkan kueri	372
Menghubungkan ke gudang data menggunakan alat klien SQL	377
Rekomendasi untuk menghubungkan dengan alat klien	377
Mengonfigurasi koneksi di Amazon Redshift	378
Mengkonfigurasi opsi keamanan untuk koneksi	552
Menghubungkan dari alat dan kode klien	561
Menghubungkan dengan SQL Workbench/J	611
Connect ke gudang data Anda secara terprogram	612
Menggunakan profil otentikasi untuk terhubung ke Amazon Redshift	612
Memecahkan masalah koneksi di Amazon Redshift	615
Menggunakan API Data	623
Bekerja dengan API Data	624
Pertimbangan saat memanggil Data API	624
Menjalankan pernyataan SQL dengan token idempotensi	630
Mengizinkan akses	632
Memanggil API Data	638
Memecahkan masalah API Data	663
Menjadwalkan operasi API Data dengan Amazon EventBridge	664

Memantau API Data	668
Grup parameter	671
Gambaran Umum	671
Tentang grup parameter	671
Nilai parameter default	672
Mengkonfigurasi nilai parameter menggunakan AWS CLI	674
Mengkonfigurasi manajemen beban kerja	676
Sifat dinamis dan statis WLM	676
Properti untuk parameter <code>wlm_json_configuration</code>	676
Mengkonfigurasi parameter <code>wlm_json_configuration</code> menggunakan AWS CLI	683
Mengelola grup parameter menggunakan konsol	692
Membuat grup parameter	692
Mengubah grup parameter	693
Membuat atau memodifikasi aturan pemantauan kueri menggunakan konsol	696
Menghapus grup parameter	697
Mengaitkan grup parameter dengan cluster	697
Mengelola grup parameter menggunakan API Amazon Redshift AWS CLI dan Amazon	698
Integrasi dengan Mitra AWS	699
Mengintegrasikan dengan AWS Partner menggunakan konsol Amazon Redshift	699
Memuat data dengan AWS mitra	700
Membeli node cadangan	702
Gambaran Umum	702
Tentang penawaran node yang dicadangkan	703
Membandingkan harga di antara penawaran node yang dicadangkan	704
Cara kerja node yang dicadangkan	705
Node cadangan dan penagihan terkonsolidasi	706
Contoh simpul cadangan	706
Membeli penawaran node cadangan dengan konsol	708
Memutakhirkan node yang dicadangkan dengan AWS CLI	709
Membeli penawaran node cadangan menggunakan AWS CLI dan Amazon Redshift API	710
Keamanan	712
Perlindungan data	714
Enkripsi data	715
Tokenisasi data	733
Privasi lalu lintas antarjaringan	733
Pengelolaan identitas dan akses	734

Mengautentikasi dengan identitas	735
Kontrol akses	738
Gambaran umum pengelolaan akses	738
Menggunakan kebijakan berbasis identitas (kebijakan IAM)	745
Federasi penyedia identitas asli (iDP) untuk Amazon Redshift	803
Hubungkan Redshift dengan IAM Identity Center untuk memberi pengguna pengalaman masuk tunggal	807
Menggunakan peran terkait layanan	825
Menggunakan otentikasi IAM untuk menghasilkan kredensi pengguna basis data	831
Mengotorisasi Amazon Redshift untuk mengakses layanan AWS	888
Mengelola kata sandi admin Amazon Redshift menggunakan AWS Secrets Manager	923
Izin diperlukan untuk integrasi AWS Secrets Manager	924
Memutar rahasia kata sandi admin	925
Mengambil Nama Sumber Daya Amazon rahasia (ARN) di Amazon Redshift	925
Membuat rahasia untuk kredensi koneksi database	926
Pertimbangan menggunakan Amazon AWS Secrets Manager Redshift	929
Pencatatan dan pemantauan	930
Pencatatan audit basis data	930
Logging dengan CloudTrail	943
Validasi kepatuhan	955
Ketahanan	956
Keamanan infrastruktur	957
Isolasi jaringan	733
Grup keamanan	958
Menghubungkan menggunakan antarmuka VPC endpoint	959
Konfigurasi dan analisis kelemahan	965
Tugas jaringan	966
Menggunakan nama domain khusus untuk koneksi klien	966
Keamanan untuk nama domain khusus	967
Menyiapkan nama domain khusus	967
Bekerja dengan titik akhir VPC yang dikelola Redshift	975
Pertimbangan	976
Mengelola titik akhir menggunakan konsol Redshift	977
Mengelola menggunakan AWS CLI	979
Mengelola menggunakan operasi Amazon Redshift API	979
Mengelola menggunakan AWS CloudFormation	980

Perutean VPC yang disempurnakan	980
Bekerja dengan VPC endpoint	982
Perutean VPC yang disempurnakan	983
Redshift Spectrum dan perutean VPC yang disempurnakan	985
Memantau kinerja cluster	990
Gambaran Umum	990
Data kinerja	991
Metrik Pergeseran Merah Amazon	992
Dimensi untuk metrik Amazon Redshift	1002
Kueri Amazon Redshift dan memuat data kinerja	1005
Bekerja dengan data kinerja	1006
Melihat data kinerja cluster	1007
Melihat data riwayat kueri	1015
Melihat data kinerja database	1019
Melihat data konkurensi beban kerja dan penskalaan konkurensi	1022
Melihat kueri dan beban	1024
Melihat metrik cluster selama operasi pemuatan	1029
Menganalisis kinerja beban kerja	1029
Mengelola alarm-alarm	1032
Bekerja dengan metrik kinerja di konsol CloudWatch	1032
Peristiwa	1035
Ikhtisar acara cluster	1035
Bekerja dengan Amazon Simple Notification Service	1036
Berlangganan notifikasi acara klaster Amazon Redshift	1037
Melihat peristiwa cluster menggunakan konsol	1039
Melihat peristiwa klaster menggunakan API Amazon Redshift AWS CLI dan Amazon	1039
Mengelola notifikasi acara klaster	1039
Mengelola notifikasi peristiwa klaster menggunakan konsol Amazon Redshift	1040
Mengelola notifikasi peristiwa klaster menggunakan AWS CLI API Amazon Redshift dan Amazon	1040
Pemberitahuan Acara Amazon Redshift	1041
Kategori acara Amazon Redshift dan pesan acara	1041
Pemberitahuan acara Amazon Redshift Tanpa Server dengan Amazon EventBridge	1062
Pemberitahuan acara integrasi nol-ETL dengan Amazon EventBridge	1069
Kuota dan batas	1078
Kuota untuk objek Amazon Redshift	1078

Kuota untuk objek Amazon Redshift Tanpa Server	1086
Kuota untuk Amazon Redshift Data API	1087
Kuota untuk objek editor kueri v2	1090
Kuota dan batas untuk objek Amazon Redshift Spectrum	1092
Kendala penamaan	1093
Pemberian tag	1097
Ikhtisar penandaan	1097
Persyaratan penandaan	1098
Mengelola tag sumber daya menggunakan konsol	1099
Mengelola tag menggunakan Amazon Redshift API	1099
Versi cluster	1101
Tambahan 181	1101
Fitur baru	1102
Tambahan 180	1103
Fitur baru	1104
Tambahan 179	1105
Fitur baru	1106
Tambahan 178	1107
Fitur baru	1107
Tambahan 177	1110
Fitur baru	1111
Tambahan 176	1112
Fitur baru	1113
Tambahan 175	1114
Fitur baru	1114
Tambahan 174	1115
Fitur baru untuk versi ini	1115
Fitur baru untuk versi ini	1115
Fitur baru untuk versi ini	1115
Fitur baru untuk versi ini	1115
Fitur baru untuk versi ini	1115
Fitur baru untuk versi ini	1115
Fitur baru untuk versi ini	1115
Tambahan 173	1116
Fitur baru untuk versi ini	1116
Fitur baru untuk versi ini	1116

Fitur baru untuk versi ini	1116
Fitur baru untuk versi ini	1116
Fitur baru untuk versi ini	1116
Fitur baru untuk versi ini	1116
Fitur baru untuk versi ini	1116
Fitur baru untuk versi ini	1116
Fitur baru untuk versi ini	1116
Fitur baru untuk versi ini	1116
Tambalan 172	1118
Fitur baru	1118
Tambalan 171	1119
Fitur baru	1119
Tambalan 170	1119
Fitur baru	1120
Tambalan 169	1120
Fitur baru	1120
Tambalan 168	1120
Fitur baru	1121
Contoh kode	1122
Tindakan	1125
CreateCluster	1125
CreateTable	1132
DeleteCluster	1135
DescribeClusters	1139
DescribeStatement	1146
GetStatementResult	1148
Insert	1151
ModifyCluster	1153
Query	1158
Skenario	1159
Memulai Amazon Redshift	1160
Contoh lintas layanan	1186
Buat aplikasi web untuk melacak data Amazon Redshift	1186
Riwayat dokumen	1188
.....	mccxvii

Apa itu Amazon Redshift?

Selamat datang di Panduan Manajemen Pergeseran Merah Amazon. Amazon Redshift adalah layanan gudang data dengan skala petabyte yang terkelola penuh di cloud. Amazon Redshift Tanpa Server memungkinkan Anda mengakses dan menganalisis data tanpa semua konfigurasi gudang data yang disediakan. Sumber daya secara otomatis disediakan dan kapasitas gudang data diskalakan secara cerdas untuk memberikan kinerja yang cepat bahkan untuk beban kerja yang paling menuntut dan tidak dapat diprediksi. Anda tidak dikenakan biaya saat gudang data menganggur, jadi Anda hanya membayar untuk apa yang Anda gunakan. Anda dapat memuat data dan mulai melakukan kueri segera di editor kueri Amazon Redshift v2 atau di alat intelijen bisnis (BI) favorit Anda. Nikmati kinerja harga terbaik dan fitur SQL yang akrab di lingkungan easy-to-use administrasi nol.

Terlepas dari ukuran kumpulan data, Amazon Redshift menawarkan kinerja kueri cepat menggunakan alat berbasis SQL dan aplikasi intelijen bisnis yang sama yang Anda gunakan saat ini.

Apakah Anda pengguna Amazon Redshift pertama kali?

Jika Anda adalah pengguna pertama kali Amazon Redshift, kami sarankan Anda mulai dengan membaca bagian berikut:

- [Sorotan dan Harga Layanan](#) — Halaman detail produk ini menyediakan proposisi nilai Amazon Redshift, sorotan layanan, dan harga.
- [Memulai Amazon Redshift Serverless](#) — Topik ini memandu Anda melalui proses penyiapan gudang data tanpa server, membuat sumber daya, dan menanyakan data sampel.
- [Panduan Pengembang Database Amazon Redshift](#) — Jika Anda seorang pengembang database, panduan ini menjelaskan cara mendesain, membuat, menanyakan, dan memelihara database yang membentuk gudang data Anda.

Jika Anda lebih suka mengelola sumber daya Amazon Redshift secara manual, Anda dapat membuat kluster yang disediakan untuk kebutuhan kueri data Anda. Untuk informasi selengkapnya, lihat [kluster Amazon Redshift](#).

Sebagai pengembang aplikasi, Anda dapat menggunakan library Amazon Redshift API atau AWS Software Development Kit (SDK) untuk mengelola cluster secara terprogram. Jika Anda menggunakan Amazon Redshift API, Anda harus mengautentikasi setiap permintaan HTTP atau

HTTPS ke API dengan menandatangani. Untuk informasi lebih lanjut tentang penandatanganan permintaan, buka [Menandatangani permintaan HTTP](#).

Untuk informasi tentang API, CLI, dan SDK, buka tautan berikut:

- [Referensi API Tanpa Server Amazon Redshift](#)
- [Referensi API Amazon Redshift](#)
- [Referensi API API Data Amazon Redshift](#)
- [AWS CLI Referensi Perintah](#)
- Referensi SDK di [Alat untuk Amazon Web Services](#).

Ikhtisar fitur Amazon Redshift Tanpa Server

Sebagian besar fitur yang didukung oleh gudang data yang disediakan Amazon Redshift juga didukung oleh Amazon Redshift Serverless. Berikut ini adalah beberapa kemampuan utamanya.

Fitur	Deskripsi
Cuplikan	Anda dapat memulihkan snapshot Amazon Redshift Tanpa Server atau gudang data yang disediakan ke Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat Bekerja dengan snapshot dan titik pemulihan .
Poin pemulihan	Amazon Redshift Serverless secara otomatis menciptakan titik pemulihan setiap 30 menit. Poin pemulihan ini disimpan selama 24 jam. Anda dapat menggunakannya untuk memulihkan setelah menulis atau menghapus secara tidak sengaja. Saat Anda memulihkan dari titik pemulihan, semua data di database Amazon Redshift Tanpa Server Anda dikembalikan ke titik waktu sebelumnya. Anda juga dapat membuat snapshot dari titik pemulihan jika Anda perlu mempertahankan titik pemulihan untuk jangka waktu yang lebih lama. Untuk informasi selengkapnya, lihat Bekerja dengan snapshot dan titik pemulihan .
Kapasitas RPU dasar	Anda dapat mengatur kapasitas dasar di Redshift Processing Units (RPU). Satu RPU menyediakan memori 16 GB. Pengaturan ini memberi Anda kemampuan untuk mengontrol keseimbangan antara sumber daya yang digunakan dan biaya untuk beban kerja Anda. Anda dapat meningkatkan nilai ini untuk menumbuhkan sumber daya yang tersedia dan meningkatkan kinerja kueri, atau menurunkan nilai untuk membatasi pengeluaran Anda. Defaultnya adalah 128 RPU. Anda juga

Fitur	Deskripsi
	<p>dapat menetapkan batas penggunaan, seperti RPU yang digunakan per hari, untuk mengontrol biaya. Untuk informasi selengkapnya, lihat Penagihan untuk Amazon Redshift Tanpa Server.</p>
<p>Batas penggunaan berbagi data</p>	<p>Anda dapat membatasi jumlah data yang ditransfer dari Wilayah produsen ke Wilayah konsumen menggunakan konsol atau API. Biaya transfer data ini berbeda Wilayah AWS, dan diukur dalam terabyte. Untuk informasi selengkapnya tentang berbagi data, lihat Memulai berbagi data menggunakan konsol di Panduan Pengembang Database Amazon Redshift.</p>
<p>Fungsi yang ditentukan pengguna (UDF)</p>	<p>Anda dapat menjalankan fungsi yang ditentukan pengguna (UDF) di Amazon Redshift Tanpa Server. Untuk informasi selengkapnya, lihat Membuat fungsi yang ditentukan pengguna di Panduan Pengembang Database Amazon Redshift.</p>
<p>Prosedur tersimpan</p>	<p>Anda dapat menjalankan prosedur tersimpan di Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat Membuat prosedur tersimpan di Panduan Pengembang Database Amazon Redshift.</p>
<p>Pandangan terwujud</p>	<p>Anda dapat membuat tampilan terwujud di Amazon Redshift Tanpa Server. Untuk informasi selengkapnya, lihat Membuat tampilan terwujud di Panduan Pengembang Database Amazon Redshift.</p>
<p>Fungsi spasial</p>	<p>Anda dapat menjalankan fungsi spasial di Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat Mengkueri data spasial di Panduan Pengembang Database Amazon Redshift.</p>
<p>Kueri federasi</p>	<p>Anda dapat menjalankan kueri untuk menggabungkan data dengan cluster Aurora DB dan database Amazon RDS dari Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat Mengkueri data dengan kueri gabungan di Panduan Pengembang Database Amazon Redshift.</p>
<p>Kueri data lake</p>	<p>Anda dapat menjalankan kueri untuk menggabungkan data dari danau data Amazon S3 Anda dengan Amazon Redshift Tanpa Server. Untuk informasi selengkapnya, lihat Menanyakan data lake di Panduan Manajemen Pergeseran Merah Amazon.</p>

Fitur	Deskripsi
HyperLogLog	Anda dapat menjalankan HyperLogLog fungsi di Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat Menggunakan HyperLogLog sketsa di Panduan Pengembang Database Amazon Redshift.
Kueri data di seluruh basis data	Anda dapat melakukan kueri data di seluruh database dengan Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat Mengkueri data di seluruh database di Panduan Pengembang Database Amazon Redshift.
Berbagi data	Anda dapat mengakses datashares di gudang data yang disediakan dengan Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat Berbagi data di seluruh cluster di Panduan Pengembang Database Amazon Redshift.
Kueri data semi-terstruktur	Anda dapat menelan dan menyimpan data semi-terstruktur dengan tipe SUPER data dengan Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat Menyerap dan menayangkan data semi-terstruktur di Panduan Pengembang Database Amazon Redshift.
Sumber daya penandaan	Anda dapat menggunakan API Tanpa Server Amazon Redshift AWS CLI atau Amazon Redshift untuk menandai sumber daya dengan metadata yang terkait dengan sumber daya. Untuk informasi selengkapnya, lihat Menandai sumber daya .
Pembelajaran mesin	Anda dapat menggunakan pembelajaran mesin Amazon Redshift dengan Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat Menggunakan pembelajaran mesin di Panduan Pengembang Database Amazon Redshift.
Perintah dan fungsi SQL	Dengan beberapa pengecualian (seperti <code>REBOOT_CLUSTER</code>), Anda dapat menggunakan perintah dan fungsi Amazon Redshift SQL dengan Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat referensi SQL di Panduan Pengembang Database Amazon Redshift.

Fitur	Deskripsi
CloudFormation sumber daya	Dengan menggunakan CloudFormation templat, Anda dapat menerapkan dan memperbarui sumber daya Amazon Redshift Tanpa Server. Integrasi ini berarti Anda dapat menghabiskan lebih sedikit waktu untuk mengelola sumber daya dan fokus pada aplikasi Anda. Untuk informasi selengkapnya tentang CloudFormation sumber daya di Amazon Redshift Tanpa Server, lihat referensi jenis sumber daya Amazon Redshift Tanpa Server.
CloudTrail sumber daya	Amazon Redshift Serverless terintegrasi AWS CloudTrail untuk memberikan catatan tindakan yang diambil di Amazon Redshift Tanpa Server. CloudTrail menangkap semua panggilan API untuk Amazon Redshift Serverless sebagai peristiwa. Untuk informasi selengkapnya, lihat CloudTrail Amazon Redshift Tanpa Server.

Ikhtisar cluster yang disediakan Amazon Redshift

Layanan Amazon Redshift mengelola semua pekerjaan pengaturan, pengoperasian, dan penskalaan gudang data. Tugas-tugas ini termasuk penyediaan kapasitas, pemantauan dan pencadangan cluster, serta menerapkan tambalan dan peningkatan ke mesin Amazon Redshift.

Video berikut menunjukkan cara membuat klaster dan data kueri menggunakan editor kueri Amazon Redshift v2.

Manajemen klaster

Cluster Amazon Redshift adalah sekumpulan node, yang terdiri dari node pemimpin dan satu atau lebih node komputasi. Jenis dan jumlah node komputasi yang Anda butuhkan bergantung pada ukuran data Anda, jumlah kueri yang akan Anda jalankan, dan kinerja runtime kueri yang Anda butuhkan.

Membuat dan mengelola cluster

Bergantung pada kebutuhan pergudangan data Anda, Anda dapat memulai dengan cluster simpul tunggal yang kecil dan dengan mudah meningkatkan skala ke cluster multi-node yang lebih besar saat kebutuhan Anda berubah. Anda dapat menambah atau menghapus node komputasi ke cluster tanpa gangguan pada layanan. Untuk informasi selengkapnya, lihat [Cluster yang disediakan Amazon Redshift](#).

Reservasi node komputasi

Jika Anda berniat untuk menjaga kluster Anda berjalan selama satu tahun atau lebih, Anda dapat menghemat uang dengan memesan node komputasi untuk periode satu tahun atau tiga tahun. Reserving compute node menawarkan penghematan yang signifikan dibandingkan dengan tarif per jam yang Anda bayar saat Anda menyediakan node komputasi sesuai permintaan. Untuk informasi selengkapnya, lihat [Membeli node cadangan Amazon Redshift](#).

Membuat snapshot cluster

Snapshot adalah point-in-time backup dari sebuah cluster. Ada dua jenis snapshot: otomatis dan manual. Amazon Redshift menyimpan snapshot ini secara internal di Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) dengan menggunakan koneksi Secure Sockets Layer (SSL) terenkripsi. Jika Anda perlu memulihkan dari snapshot, Amazon Redshift membuat kluster baru dan mengimpor data dari snapshot yang Anda tentukan. Untuk informasi selengkapnya tentang snapshot, lihat [Cuplikan dan cadangan Amazon Redshift](#).

Akses dan keamanan kluster

Ada beberapa fitur yang terkait dengan akses cluster dan keamanan di Amazon Redshift. Fitur-fitur ini membantu Anda mengontrol akses ke cluster Anda, menentukan aturan konektivitas, dan mengenkripsi data dan koneksi. Fitur-fitur ini merupakan tambahan fitur yang terkait dengan akses database dan keamanan di Amazon Redshift. Untuk informasi selengkapnya tentang keamanan database, lihat [Mengelola Keamanan Database](#) di Panduan Pengembang Database Amazon Redshift.

AWS akun dan kredensi IAM

Secara default, cluster Amazon Redshift hanya dapat diakses oleh AWS akun yang membuat cluster. Cluster dikunci sehingga tidak ada orang lain yang memiliki akses. Dalam AWS akun Anda, Anda menggunakan layanan AWS Identity and Access Management (IAM) untuk membuat akun pengguna dan mengelola izin untuk akun tersebut untuk mengontrol operasi kluster. Untuk informasi selengkapnya, lihat [Keamanan di Amazon Redshift](#). Untuk informasi selengkapnya tentang mengelola identitas IAM, termasuk panduan dan praktik terbaik untuk peran IAM, lihat [Manajemen identitas dan akses di Amazon Redshift](#)

Grup keamanan

Secara default, cluster apa pun yang Anda buat ditutup untuk semua orang. Kredensi IAM hanya mengontrol akses ke sumber daya terkait Amazon Redshift API: konsol Amazon Redshift, antarmuka

baris perintah (CLI), API, dan SDK. Untuk mengaktifkan akses ke cluster dari alat klien SQL melalui JDBC atau ODBC, Anda menggunakan grup keamanan:

- Jika Anda menggunakan platform EC2-VPC untuk cluster Amazon Redshift Anda, Anda harus menggunakan grup keamanan VPC. Kami menyarankan Anda meluncurkan cluster Anda di platform EC2-VPC.

Anda tidak dapat memindahkan cluster ke VPC setelah diluncurkan dengan EC2-Classic. Namun, Anda dapat memulihkan snapshot EC2-Classic ke cluster EC2-VPC menggunakan konsol Amazon Redshift. Untuk informasi selengkapnya, lihat [Memulihkan cluster dari snapshot](#).

- Jika Anda menggunakan platform EC2-Classic untuk cluster Amazon Redshift Anda, Anda harus menggunakan grup keamanan Amazon Redshift.

Dalam kedua kasus tersebut, Anda menambahkan aturan ke grup keamanan untuk memberikan akses masuk eksplisit ke rentang alamat CIDR/IP tertentu atau ke grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) jika klien SQL Anda berjalan pada instans Amazon EC2. Untuk informasi selengkapnya, lihat [Grup keamanan klaster Amazon Redshift](#).

Selain aturan akses masuk, Anda membuat pengguna database untuk memberikan kredensi untuk mengautentikasi ke database dalam cluster itu sendiri. Untuk informasi lebih lanjut, lihat [Basis Data](#) di topik ini.

Enkripsi

Saat Anda menyediakan klaster, Anda dapat memilih untuk mengenkripsi klaster untuk keamanan tambahan. Saat Anda mengaktifkan enkripsi, Amazon Redshift menyimpan semua data dalam tabel yang dibuat pengguna dalam format terenkripsi. Anda dapat menggunakan AWS Key Management Service (AWS KMS) untuk mengelola kunci enkripsi Amazon Redshift Anda.

Enkripsi adalah properti abadi dari cluster. Satu-satunya cara untuk beralih dari cluster terenkripsi ke cluster yang tidak dienkripsi adalah dengan membongkar data dan memuatnya kembali ke cluster baru. Enkripsi berlaku untuk cluster dan cadangan apa pun. Saat Anda memulihkan cluster dari snapshot terenkripsi, cluster baru juga dienkripsi.

Untuk informasi selengkapnya tentang enkripsi, kunci, dan modul keamanan perangkat keras, lihat [Enkripsi basis data Amazon Redshift](#).

Koneksi SSL

Anda dapat menggunakan enkripsi Secure Sockets Layer (SSL) untuk mengenkripsi koneksi antara klien SQL dan cluster Anda. Untuk informasi selengkapnya, lihat [Mengkonfigurasi opsi keamanan untuk koneksi](#).

Cluster pemantauan

Ada beberapa fitur yang terkait dengan pemantauan di Amazon Redshift. Anda dapat menggunakan pencatatan audit database untuk menghasilkan log aktivitas, mengonfigurasi peristiwa, dan langganan notifikasi untuk melacak informasi yang diminati. Gunakan metrik di Amazon Redshift dan CloudWatch Amazon untuk mempelajari kesehatan dan kinerja cluster dan database Anda.

Pencatatan audit basis data

Anda dapat menggunakan fitur pencatatan audit database untuk melacak informasi tentang upaya otentikasi, koneksi, pemutusan, perubahan definisi pengguna database, dan kueri yang dijalankan dalam database. Informasi ini berguna untuk tujuan keamanan dan pemecahan masalah di Amazon Redshift. Log disimpan dalam ember Amazon S3. Untuk informasi selengkapnya, lihat [Pencatatan audit basis data](#).

Peristiwa dan notifikasi

Amazon Redshift melacak peristiwa dan menyimpan informasi tentangnya selama beberapa minggu di akun Anda. AWS Untuk setiap peristiwa, Amazon Redshift melaporkan informasi seperti tanggal peristiwa terjadi, deskripsi, sumber peristiwa (misalnya, cluster, grup parameter, atau snapshot), dan ID sumber. Anda dapat membuat langganan notifikasi acara Amazon Redshift yang menentukan satu set filter peristiwa. Saat terjadi peristiwa yang sesuai dengan kriteria filter, Amazon Redshift menggunakan Layanan Pemberitahuan Sederhana Amazon untuk memberi tahu Anda bahwa peristiwa tersebut telah terjadi. Untuk informasi selengkapnya tentang acara dan notifikasi, lihat [Acara Amazon Redshift](#).

Kinerja

Amazon Redshift menyediakan metrik kinerja dan data sehingga Anda dapat melacak kesehatan dan kinerja cluster dan database Anda. Amazon Redshift menggunakan CloudWatch metrik Amazon untuk memantau aspek fisik cluster, seperti pemanfaatan CPU, latensi, dan throughput. Amazon Redshift juga menyediakan kueri dan memuat data performa untuk membantu Anda memantau aktivitas database di klaster. Untuk informasi selengkapnya tentang metrik dan pemantauan kinerja, lihat [Memantau kinerja klaster Amazon Redshift](#).

Basis Data

Amazon Redshift membuat satu database saat Anda menyediakan kluster. Ini adalah database yang Anda gunakan untuk memuat data dan menjalankan kueri pada data Anda. Anda dapat membuat database tambahan sesuai kebutuhan dengan menjalankan perintah SQL. Untuk informasi selengkapnya tentang membuat database tambahan, buka [Langkah 1: Buat database](#) di Panduan Pengembang Database Amazon Redshift.

Saat Anda menyediakan kluster, Anda menentukan pengguna admin yang memiliki akses ke semua database yang dibuat di dalam kluster. Pengguna admin ini adalah pengguna super yang merupakan satu-satunya pengguna dengan akses ke database pada awalnya, meskipun pengguna ini dapat membuat pengguna super dan pengguna tambahan. Untuk informasi selengkapnya, buka [Superusers dan Users](#) di Amazon Redshift Database Developer Guide.

Amazon Redshift menggunakan grup parameter untuk menentukan perilaku semua database dalam kluster, seperti gaya presentasi tanggal dan presisi floating-point. Jika Anda tidak menentukan grup parameter saat menyediakan kluster, Amazon Redshift akan mengaitkan grup parameter default dengan kluster. Untuk informasi selengkapnya, lihat [Grup parameter Amazon Redshift](#).

Untuk informasi selengkapnya tentang database di Amazon Redshift, buka Panduan Pengembang Database [Amazon Redshift](#).

Membandingkan Amazon Redshift Tanpa Server dengan gudang data yang disediakan Amazon Redshift

Untuk Amazon Redshift Tanpa Server, beberapa konsep dan fitur berbeda dari fitur yang sesuai untuk gudang data yang disediakan Amazon Redshift. Misalnya, satu perbandingan yang kontras adalah bahwa Amazon Redshift Serverless tidak memiliki konsep cluster atau node. Tabel berikut menjelaskan fitur dan perilaku di Amazon Redshift Tanpa Server dan menjelaskan perbedaannya dari fitur yang setara di gudang data yang disediakan.

Fitur	Deskripsi	Nirserver	Disediakan
Workgroup dan Namespace	Untuk mengisolasi beban kerja dan	Namespace adalah kumpulan objek	Cluster yang disediakan adalah kumpulan node komputasi dan node pemimpin, yang Anda kelola secara langsung. Untuk informasi selengkapnya, lihat Cluster yang disediakan Amazon Redshift .

Fitur	Deskripsi	Nirserver	Disediakan
	mengelola sumber daya yang berbeda di Amazon Redshift Tanpa Server, Anda dapat membuat ruang nama dan grup kerja untuk mengelola penyimpanan dan menghitung sumber daya secara terpisah.	database dan pengguna. Workgroup adalah kumpulan sumber daya komputasi . Untuk informasi selengkapnya, lihat Amazon Redshift Tanpa Server untuk memahami desain Amazon Redshift Serverless.	

Fitur	Deskripsi	Nirserver	Disediakan
Jenis simpul	Saat Anda bekerja dengan Amazon Redshift Serverless, Anda tidak memilih jenis node atau menentukan jumlah node seperti yang Anda lakukan dengan cluster Amazon Redshift yang disediakan.	Amazon Redshift Serverless secara otomatis menyediakan dan mengelola kapasitas untuk Anda. Anda dapat secara opsional menentukan kapasitas gudang data dasar untuk memilih saldo harga/kinerja yang tepat untuk beban kerja Anda. Anda juga dapat menentukan jam RPU maksimum untuk mengatur kontrol	Anda membangun klaster dengan tipe node yang memenuhi spesifikasi biaya dan kinerja Anda. Untuk informasi selengkapnya, lihat Cluster yang disediakan Amazon Redshift .

Fitur	Deskripsi	Nirserver	Disediakan
		biaya untuk memastikan bahwa biaya dapat diprediksi. Untuk informasi selengkapnya, lihat Memahami kapasitas Amazon Redshift Tanpa Server.	

Fitur	Deskripsi	Nirserver	Disediakan
Manajemen beban kerja dan penskalaan konkurensi	Amazon Redshift dapat menskalakan untuk periode beban berat. Amazon Redshift Serverless juga dapat menskalakan untuk memenuhi periode beban tinggi yang terputus-putus.	Amazon Redshift Serverless secara otomatis mengelola sumber daya secara efisien dan menskalakan, berdasarkan beban kerja, dalam ambang batas kontrol biaya. Untuk informasi selengkapnya, lihat Penagihan untuk kapasitas komputasi .	Dengan gudang data yang disediakan, Anda mengaktifkan penskalaan konkurensi pada klaster Anda untuk menangani periode beban berat. Untuk informasi selengkapnya, lihat Penskalaan konkurensi .

Fitur	Deskripsi	Nirserver	Disediakan
Port	Nomor port yang Anda gunakan untuk menghubungkan.	Dengan Amazon Redshift Serverless, Anda dapat mengubah ke port lain dari rentang port 5431—5455 atau 8191—8215. Untuk informasi selengkapnya, lihat Menghubungkan ke Amazon Redshift Tanpa Server .	Dengan gudang data yang disediakan, Anda dapat memilih port apa pun untuk dihubungkan.

Fitur	Deskripsi	Nirserver	Disediakan
Mengubah ukuran	Menambah atau menghapus sumber daya komputasi untuk bekerja dengan baik untuk beban kerja.	Mengubah ukuran tidak berlaku di Amazon Redshift Tanpa Server. Namun Anda dapat mengubah kapasitas RPU gudang data dasar, berdasarkan persyaratan harga dan kinerja Anda. Untuk informasi selengkapnya, lihat Memahami kapasitas Amazon Redshift Tanpa Server .	Dengan kluster yang disediakan, Anda melakukan perubahan ukuran cluster untuk menambahkan node atau menghapus node. Untuk informasi selengkapnya, lihat Ikhtisar pengelolaan kluster di Amazon Redshift .

Fitur	Deskripsi	Nirserver	Disediakan
Menjeda dan melanjutkan	Anda dapat menjeda klaster yang disediakan saat Anda tidak memiliki beban kerja untuk dijalankan, untuk menghemat biaya.	Dengan Amazon Redshift Serverless, Anda hanya membayar saat kueri berjalan, jadi tidak perlu menjeda atau melanjutkan. Untuk informasi selengkapnya, lihat Penagihan untuk kapasitas komputasi .	Anda menjeda dan melanjutkan cluster secara manual, berdasarkan penilaian beban kerja Anda di berbagai waktu. Untuk informasi selengkapnya, lihat Ikhtisar pengelolaan klaster di Amazon Redshift .

Fitur	Deskripsi	Nirserver	Disediakan
Menanyakan data eksternal dengan kueri Spectrum	Anda dapat menanyakan data di bucket Amazon S3, dalam berbagai format, seperti JSON.	Penagihan bertambah saat menghitung sumber daya memproses beban kerja. Juga, penagihan bertambah ketika data Redshift Spectrum eksternal ditanyakan, seperti transaksi lainnya. Untuk informasi selengkapnya, lihat Penagihan untuk kapasitas komputasi .	Dengan gudang data yang disediakan, kapasitas Amazon Redshift Spectrum ada di server terpisah yang ditanyakan dari cluster Amazon Redshift. Untuk informasi selengkapnya, lihat Menanyakan data eksternal menggunakan Amazon Redshift Spectrum .

Fitur	Deskripsi	Nirserver	Disediakan
Tagihan sumber daya komputasi	Bagaimana penagihan bertambah untuk Amazon Redshift vs Amazon Redshift Tanpa Server.	Dengan Amazon Redshift Serverless, Anda membayar beban kerja yang Anda jalankan, dalam RPU-jam per detik, dengan biaya minimum 60 detik. Ini termasuk kueri yang mengakses data dalam format file terbuka di Amazon S3. Untuk informasi selengkapnya, lihat Penagihan untuk kapasitas komputasi .	Dengan kluster yang disediakan, penagihan terjadi per detik saat kluster tidak dijeda.

Fitur	Deskripsi	Nirserver	Disediakan
Jendela pemeliharaan	Cara kerja pemeliharaan server.	Dengan Amazon Redshift Serverless, tidak ada jendela pemeliharaan. Pembaruan ditangani dengan mulus. Untuk informasi lebih lanjut, lihat Apa itu Amazon Redshift Tanpa Server?	Dengan kluster yang disediakan, Anda menentukan jendela pemeliharaan saat penambalan terjadi. (Biasanya, Anda memilih waktu berulang saat penggunaan rendah.)

Fitur	Deskripsi	Nirserver	Disediakan
Enkripsi	Anda dapat mengaktifkan enkripsi basis data.	Amazon Redshift Serverless selalu dienkripsi dengan, dengan kunci terkelola atau AWS KMS dikelola pelanggan. AWS	Data dalam gudang data yang disediakan dapat dienkripsi dengan AWS KMS (dengan kunci yang AWS dikelola atau dikelola pelanggan), atau tidak dienkripsi. Lihat Enkripsi basis data Amazon Redshift .
Penagihan penyimpanan	Cara kerja penagihan untuk penyimpanan.	Untuk Amazon Redshift Tanpa Server. Tarif dihitung sesuai dengan GB per bulan. Lihat Penagihan untuk kapasitas komputasi .	Penyimpanan ditagih terpisah dari sumber daya komputasi untuk cluster yang disediakan dengan node RA3.

Fitur	Deskripsi	Nirserver	Disediakan
Manajemen pengguna	Bagaimana pengguna dikelola.	<p>Untuk Amazon Redshift Serverless, pengguna adalah pengguna IAM atau Redshift.</p> <p>Untuk informasi selengkapnya, lihat Manajemen identitas dan akses di Amazon Redshift Tanpa Server.</p> <p>Untuk informasi selengkapnya tentang mengelola identitas IAM, termasuk praktik terbaik untuk peran IAM, lihat.</p>	<p>Untuk gudang data yang disediakan, pengguna adalah pengguna IAM atau Redshift. Untuk informasi selengkapnya, lihat Mengelola keamanan database di Panduan Pengembang Database Amazon Redshift.</p> <p>Untuk informasi selengkapnya tentang mengelola identitas IAM, termasuk praktik terbaik untuk peran IAM, lihat. Manajemen identitas dan akses di Amazon Redshift</p>

Fitur	Deskripsi	Nirserver	Disediakan
		Manajemen identitas dan akses di Amazon Redshift	

Fitur	Deskripsi	Nirserver	Disediakan
Alat dan kompatibilitas JDBC dan ODBC	Bagaimana koneksi klien bekerja.	Amazon Redshift Serverless kompatibel dengan alat atau aplikasi klien yang sesuai dengan JDBC atau ODBC. Untuk informasi selengkapnya tentang driver, lihat Mengonfigurasi koneksi di Panduan Manajemen Amazon Redshift. Untuk informasi tentang menghubungkan ke Amazon Redshift Tanpa Server,	Amazon Redshift yang disediakan kompatibel dengan alat atau aplikasi klien yang sesuai dengan JDBC atau ODBC. Untuk informasi selengkapnya tentang driver, lihat Mengonfigurasi koneksi di Panduan Manajemen Amazon Redshift. Untuk informasi tentang menghubungkan ke cluster, lihat Menyambung ke gudang data Amazon Redshift menggunakan alat klien SQL .

Fitur	Deskripsi	Nirserver	Disediakan
		<p>lihat Menyambungkan ke Redshift Tanpa Server.</p>	
<p>Persyaratan untuk kredensial saat masuk</p>	<p>Bagaimana kredensial ditangani.</p>	<p>Untuk Amazon Redshift Tanpa Server, Anda tidak perlu memasukkan kredensial di setiap instans. Untuk informasi selengkapnya, lihat Menghubungkan ke Amazon Redshift Tanpa Server.</p>	<p>Akses ke Amazon Redshift memerlukan kredensial masuk dari pengguna yang terkait dengan peran IAM. Peran IAM memiliki izin khusus yang dilampirkan untuk gudang data yang disediakan. Setelah diautentikasi, pengguna dapat terhubung langsung ke database, ke konsol Redshift, dan ke editor kueri v2.</p>

Fitur	Deskripsi	Nirserver	Disediakan
Data API	Anda dapat mengakses data dari layanan web dan aplikasi lainnya.	Amazon Redshift Serverless mendukung Amazon Redshift Data API. Dengan Amazon Redshift Serverless, Anda menggunakan <code>workgroup-name</code> parameter alih-alih <code>parameter.cluster-identity</code> . Untuk informasi selengkapnya tentang memanggil Data API, lihat Menggunakan API Data Amazon Redshift .	Amazon Redshift yang disediakan mendukung Amazon Redshift Data API. Dengan cluster Amazon Redshift, Anda menggunakan parameter <code>cluster-identity</code> parameter <code>workgroup-name</code> . Untuk informasi selengkapnya tentang memanggil Data API, lihat Menggunakan API Data Amazon Redshift .

Fitur	Deskripsi	Nirserver	Disediakan
Cuplikan	Memberikan point-in-time pemulihan.	Amazon Redshift Serverless mendukung snapshot dan titik pemulihan . Untuk informasi selengkapnya tentang snapshot dan titik pemulihan untuk namespace , lihat. Bekerja dengan snapshot dan titik pemulihan	Cluster yang disediakan mendukung snapshot. Untuk informasi selengkapnya, lihat Mengelola snapshot menggunakan konsol .

Fitur	Deskripsi	Nirserver	Disediakan
Berbagi Data	Memberikan kemampuan untuk berbagi data antar database di akun yang sama atau di akun yang berbeda.	Amazon Redshift Serverless mendukung semua fitur berbagi data yang dilakukan oleh gudang data yang disediakan. Ini juga mendukung berbagi data antara Amazon Redshift Serverless dan gudang data, alat, atau aplikasi klien yang disediakan.	Cluster yang disediakan mendukung lintas basis data, lintas akun, Lintas wilayah, dan berbagi data. AWS Data Exchange Untuk informasi selengkapnya, lihat Berbagi data di seluruh cluster di Amazon Redshift .

Fitur	Deskripsi	Nirserver	Disediakan
Trek	Menyediakan jadwal untuk pembaruan perangkat lunak.	Amazon Redshift Serverless tidak memiliki konsep trek. Versi dan pembaruan ditangani oleh layanan. Untuk informasi selengkapnya tentang desain Amazon Redshift Serverless, lihat Bekerja dengan snapshot dan titik pemulihan	Cluster yang disediakan mendukung peralihan antara trek saat ini dan trailing.

Fitur	Deskripsi	Nirserver	Disediakan
Tabel dan tampilan sistem	Menyediakan cara untuk memantau sumber daya dan metadata sistem Anda.	Amazon Redshift Serverless mendukung tabel dan tampilan sistem baru. Untuk informasi selengkapnya tentang tabel sistem, lihat Pemantauan tampilan . Untuk informasi tentang cara memigrasikan kueri Anda dari menggunakan tabel dan tampilan sistem yang disediakan lebih lama ke tampilan baru, lihat	Gudang data yang disediakan mendukung kumpulan tabel dan tampilan sistem yang ada untuk pemantauan dan tugas lain yang memerlukan metadata sistem.

Fitur	Deskripsi	Nirserver	Disediakan
		Memigrasi ke tampilan pemantauan SYS.	
Grup parameter	Ini adalah sekelompok parameter yang berlaku untuk semua database yang dibuat dalam sebuah cluster. Parameter ini mengkonfigurasi pengaturan database seperti batas waktu kueri dan gaya tanggal.	Amazon Redshift Serverless tidak memiliki konsep grup parameter.	Gudang data yang disediakan mendukung kelompok parameter. Untuk informasi selengkapnya tentang grup parameter untuk klaster yang disediakan, lihat. Grup parameter Amazon Redshift

Fitur	Deskripsi	Nirserver	Disediakan
Pemantauan kueri	Menyediakan tampilan berbasis waktu dari kueri yang dijalankan.	Pemantauan kueri di Amazon Redshift Tanpa Server mengharuskan pengguna untuk terhubung ke database untuk menggunakan tabel sistem. Dengan demikian, pemantauan kueri dan tabel sistem sinkron. Kueri tabel sistem di Amazon Redshift Tanpa Server menggunakan pengguna database	Pemantauan kueri di kluster yang disediakan tidak menampilkan semua data dalam tabel sistem.

Fitur	Deskripsi	Nirserver	Disediakan
		yang dipetakan ke pengguna IAM untuk menggunakan pemantauan kueri. Untuk informasi selengkapnya tentang pemantauan kueri, lihat Memantau kueri dan beban kerja dengan Amazon Redshift Tanpa Server.	

Fitur	Deskripsi	Nirserver	Disediakan
Pencatatan audit	Memberikan informasi tentang koneksi dan aktivitas pengguna dalam database.	Dengan Amazon Redshift Serverless, CloudWatch adalah tujuan untuk log audit. Pengiriman log audit berbasis Amazon S3 tidak didukung untuk Amazon Redshift Tanpa Server. Untuk informasi selengkapnya, lihat Pencatatan audit untuk Amazon Redshift Tanpa Server .	Untuk kluster yang disediakan, pengiriman log audit berbasis Amazon S3 telah menjadi norma. Sekarang, pengiriman log audit ke CloudWatch diperluas untuk mencakup gudang data yang disediakan.

Fitur	Deskripsi	Nirserver	Disediakan
Pemberitahuan acara	Amazon EventBridge adalah layanan bus acara tanpa server yang dapat Anda gunakan untuk menghubungkan aplikasi Anda dengan data peristiwa dari berbagai sumber.	Amazon Redshift Serverless menggunakan Amazon EventBridge untuk mengelola pemberitahuan acara agar up-to-date. Anda tetap memperhatikan perubahan di gudang data Anda. Untuk informasi selengkapnya, lihat Pemberitahuan acara Amazon Redshift Tanpa Server dengan Amazon EventBridge .	Untuk kluster yang disediakan, Anda mengelola notifikasi peristiwa menggunakan konsol Amazon Redshift untuk membuat langganan acara. Untuk informasi selengkapnya, lihat Mengelola notifikasi acara kluster .

Menggunakan antarmuka manajemen Amazon Redshift untuk cluster yang disediakan

Note

Topik ini berfokus pada antarmuka manajemen Amazon Redshift untuk cluster yang disediakan. Ada antarmuka manajemen serupa untuk Amazon Redshift Serverless dan Amazon Redshift Data API.

Amazon Redshift mendukung beberapa antarmuka manajemen yang dapat Anda gunakan untuk membuat, mengelola, dan menghapus kluster Amazon Redshift: AWS SDK, () AWS Command Line Interface, AWS CLI dan API manajemen Amazon Redshift.

Amazon Redshift API — Anda dapat memanggil API manajemen Amazon Redshift ini dengan mengirimkan permintaan. Permintaan adalah permintaan HTTP atau HTTPS yang menggunakan kata kerja HTTP GET atau POST dengan parameter bernama `Action`. Memanggil Amazon Redshift API adalah cara paling langsung untuk mengakses layanan Amazon Redshift. Namun, aplikasi Anda harus menangani detail tingkat rendah seperti penanganan kesalahan dan menghasilkan hash untuk menandatangani permintaan.

- Untuk informasi tentang membuat dan menandatangani permintaan Amazon Redshift API, lihat [Menandatangani permintaan HTTP](#)
- Untuk informasi tentang tindakan Amazon Redshift API dan tipe data untuk Amazon Redshift, lihat referensi Amazon [Redshift](#) API.

AWS SDK — Anda dapat menggunakan AWS SDK untuk melakukan operasi terkait kluster Amazon Redshift. Beberapa pustaka SDK membungkus API Amazon Redshift yang mendasarinya. Mereka mengintegrasikan fungsionalitas API ke dalam bahasa pemrograman tertentu dan menangani banyak detail tingkat rendah, seperti menghitung tanda tangan, menangani percobaan ulang permintaan, dan penanganan kesalahan. Memanggil fungsi pembungkus di pustaka SDK dapat sangat menyederhanakan proses penulisan aplikasi untuk mengelola cluster Amazon Redshift.

- Amazon Redshift didukung oleh AWS SDK untuk Java, .NET, PHP, Python, Ruby, dan Node.js. Fungsi pembungkus untuk Amazon Redshift didokumentasikan dalam manual referensi untuk setiap SDK. Untuk daftar AWS SDK dan tautan ke dokumentasinya, lihat [Alat untuk Amazon Web Services](#).

- Panduan ini memberikan contoh bekerja dengan Amazon Redshift menggunakan Java SDK. Untuk contoh kode AWS SDK yang lebih umum, lihat [Contoh kode untuk Amazon Redshift menggunakan SDK AWS](#).

AWS CLICLI menyediakan seperangkat alat baris perintah yang dapat Anda gunakan untuk mengelola AWS layanan dari komputer Windows, Mac, dan Linux. AWS CLI Termasuk perintah berdasarkan tindakan Amazon Redshift API.

- Untuk informasi tentang menginstal dan menyiapkan Amazon Redshift CLI, lihat. [Menyiapkan Amazon Redshift CLI](#)
- [Untuk materi referensi tentang perintah Amazon Redshift CLI, lihat Amazon Redshift di Referensi.AWS CLI](#)

Menggunakan layanan ini dengan AWS SDK

AWS kit pengembangan perangkat lunak (SDK) tersedia untuk banyak bahasa pemrograman populer. Setiap SDK menyediakan API, contoh kode, dan dokumentasi yang memudahkan developer untuk membangun aplikasi dalam bahasa pilihan mereka.

Dokumentasi SDK	Contoh kode
AWS SDK for C++	AWS SDK for C++ contoh kode
AWS CLI	AWS CLI contoh kode
AWS SDK for Go	AWS SDK for Go contoh kode
AWS SDK for Java	AWS SDK for Java contoh kode
AWS SDK for JavaScript	AWS SDK for JavaScript contoh kode
AWS SDK for Kotlin	AWS SDK for Kotlin contoh kode
AWS SDK for .NET	AWS SDK for .NET contoh kode
AWS SDK for PHP	AWS SDK for PHP contoh kode
AWS Tools for PowerShell	Alat untuk contoh PowerShell kode

Dokumentasi SDK	Contoh kode
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) contoh kode
AWS SDK for Ruby	AWS SDK for Ruby contoh kode
AWS SDK for Rust	AWS SDK for Rust contoh kode
AWS SDK untuk SAP ABAP	AWS SDK untuk SAP ABAP contoh kode
AWS SDK for Swift	AWS SDK for Swift contoh kode

Ketersediaan contoh


Tidak dapat menemukan apa yang Anda butuhkan? Minta contoh kode menggunakan tautan Berikan umpan balik pada bagian bawah halaman ini.

Menandatangani permintaan HTTP

Amazon Redshift mengharuskan setiap permintaan yang Anda kirim ke API manajemen diautentikasi dengan tanda tangan. Topik ini menjelaskan cara menandatangani permintaan Anda.

Jika Anda menggunakan salah satu Kit Pengembangan Perangkat AWS Lunak (SDK) atau AWS Command Line Interface, penandatanganan permintaan ditangani secara otomatis, dan Anda dapat melewati bagian ini. Untuk informasi selengkapnya tentang menggunakan AWS SDK, lihat [Menggunakan antarmuka manajemen Amazon Redshift untuk cluster yang disediakan](#). Untuk informasi selengkapnya tentang penggunaan Antarmuka Baris Perintah Amazon Redshift, buka referensi baris perintah [Amazon Redshift](#).

Untuk menandatangani permintaan, Anda menghitung tanda tangan digital dengan menggunakan fungsi hash kriptografi. Hash kriptografi adalah fungsi yang mengembalikan nilai hash unik yang didasarkan pada input. Input ke fungsi hash mencakup teks permintaan Anda dan kunci akses rahasia Anda yang bisa Anda dapatkan dari kredensi sementara. Fungsi hash mengembalikan nilai hash yang Anda sertakan dalam permintaan sebagai tanda tangan Anda. Tanda tangan adalah bagian header `Authorization` dari permintaan Anda.

 Note

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. <ul style="list-style-type: none"> • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat otentikasi Pusat Identitas IAM di Panduan Referensi AWS SDK dan Alat.
IAM	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk dalam Menggunakan kredensial sementara dengan AWS sumber daya di Panduan Pengguna IAM.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Tidak direkomendasikan) Gunakan kredensial jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	<p>Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan.</p> <ul style="list-style-type: none"> • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensial pengguna IAM di Panduan Pengguna. AWS Command Line Interface • Untuk AWS SDK dan alat bantu, lihat Mengautentikasi menggunakan kredensial jangka panjang di Panduan Referensi AWS SDK dan Alat. • Untuk AWS API, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Setelah Amazon Redshift menerima permintaan Anda, itu menghitung ulang tanda tangan dengan menggunakan fungsi hash yang sama dan input yang Anda gunakan untuk menandatangani permintaan. Jika tanda tangan yang dihasilkan cocok dengan tanda tangan dalam permintaan, Amazon Redshift memproses permintaan; jika tidak, permintaan ditolak.

Amazon Redshift mendukung otentikasi menggunakan versi [AWS tanda tangan](#) 4. Proses untuk menghitung tanda tangan terdiri dari tiga tugas. Tugas-tugas ini diilustrasikan dalam contoh berikut.

- [Tugas 1: Buat permintaan kanonik](#)

Atur ulang permintaan HTTP Anda ke dalam bentuk kanonik. Menggunakan bentuk kanonik diperlukan karena Amazon Redshift menggunakan bentuk kanonik yang sama untuk menghitung tanda tangan yang dibandingkan dengan yang Anda kirim.

- [Tugas 2: Buat string untuk ditandatangani](#)

Buat string yang akan Anda gunakan sebagai salah satu nilai input untuk fungsi hash kriptografi Anda. String, yang disebut string to sign, adalah rangkaian dari nama algoritme hash, tanggal permintaan, string cakupan kredensial, dan permintaan kanonikalisasi dari tugas sebelumnya. String lingkup kredensi itu sendiri adalah rangkaian informasi tanggal, wilayah, dan layanan.

- [Tugas 3: Hitung tanda tangan](#)

Hitung tanda tangan untuk permintaan Anda dengan menggunakan fungsi hash kriptografi yang menerima dua string input, string Anda untuk ditandatangani dan kunci turunan. Kunci turunan dihitung dengan memulai dengan kunci akses rahasia Anda dan menggunakan string cakupan kredensi untuk membuat serangkaian kode otentikasi pesan berbasis hash (HMAC-SHA256).

Contoh perhitungan tanda tangan

Contoh berikut memandu Anda melalui detail pembuatan tanda tangan untuk [CreateCluster](#) permintaan. Anda dapat menggunakan contoh ini sebagai referensi untuk memeriksa metode perhitungan tanda tangan Anda sendiri. Perhitungan referensi lainnya disertakan dalam [bagian Minta contoh tanda tangan](#) pada Panduan Pengguna IAM.

Anda dapat menggunakan permintaan GET atau POST untuk mengirim permintaan ke Amazon Redshift. Perbedaan antara keduanya adalah bahwa untuk permintaan GET parameter Anda dikirim sebagai parameter string kueri. Untuk permintaan POST mereka termasuk dalam badan permintaan. Contoh di bawah ini menunjukkan permintaan POST.

Contoh tersebut mengasumsikan sebagai berikut:

- Stempel waktu permintaan adalah `Fri, 07 Dec 2012 00:00:00 GMT`.
- Titik akhirnya adalah Wilayah AS Timur (Virginia Utara), `us-east-1`.

Sintaks permintaan umum adalah:

```
https://redshift.us-east-1.amazonaws.com/  
?Action=CreateCluster
```

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

Bentuk kanonik permintaan yang dihitung untuk [Tugas 1: Membuat Permintaan Kanonik](#) adalah:

```
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
```

Baris terakhir dari permintaan kanonik adalah hash dari isi permintaan. Baris ketiga dalam permintaan kanonik kosong karena tidak ada parameter kueri untuk API ini.

String yang akan ditandatangani untuk [Tugas 2: Buat String untuk Ditandatangani](#) adalah:

```
AWS4-HMAC-SHA256
20121207T000000Z
20121207/us-east-1/redshift/aws4_request
06b6bef4f4f060a5558b60c627cc6c5b5b5a959b9902b5ac2187be80cbac0714
```

Baris pertama string to sign adalah algoritme, baris kedua adalah stempel waktu, baris ketiga adalah cakupan kredensial, dan baris terakhir adalah hash permintaan kanonik dari [Tugas 1: Membuat Permintaan Kanonik](#). Nama layanan untuk digunakan dalam cakupan kredensial adalah redshift.

Untuk [Tugas 3: Hitung Tanda Tangan](#), kunci turunan dapat direpresentasikan sebagai:

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

Kunci turunan dihitung sebagai rangkaian fungsi hash. Mulai dari pernyataan HMAC dalam rumus di atas, Anda menggabungkan frasa **AWS4** dengan kunci akses rahasia Anda dan menggunakan ini sebagai kunci untuk hash data "us-east-1". Hasil hash ini menjadi kunci untuk fungsi hash berikutnya.

Setelah Anda menghitung kunci turunan, Anda menggunakannya dalam fungsi hash yang menerima dua string input, string Anda untuk ditandatangani dan kunci turunan. Misalnya, jika Anda menggunakan kunci akses rahasia `wJa1rXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY` dan string untuk menandatangani yang diberikan sebelumnya, maka tanda tangan yang dihitung adalah sebagai berikut:

```
9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

Langkah terakhir adalah membangun header `Authorization`. Untuk access key demonstrasi `AKIAIOSFODNN7EXAMPLE`, header (dengan jeda baris yang ditambahkan untuk keterbacaan) adalah:

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

Menyiapkan Amazon Redshift CLI

Bagian ini menjelaskan cara mengatur dan menjalankan alat baris AWS CLI perintah untuk digunakan dalam mengelola Amazon Redshift. [Alat baris perintah Amazon Redshift berjalan di AWS Command Line Interface \(AWS CLI\), yang pada gilirannya menggunakan Python \(<https://www.python.org/>\)](#). Ini AWS CLI dapat dijalankan pada sistem operasi apa pun yang mendukung Python.

Petunjuk pemasangan

Untuk mulai menggunakan alat baris perintah Amazon Redshift, Anda terlebih dahulu mengatur AWS CLI, dan kemudian Anda menambahkan file konfigurasi yang menentukan opsi Amazon Redshift CLI.

Jika Anda telah menginstal dan mengkonfigurasi AWS CLI untuk AWS layanan lain, Anda dapat melewati prosedur ini.

Untuk menginstal AWS Command Line Interface

1. Pergi ke [Instal atau perbarui ke versi terbaru dari AWS CLI](#), dan kemudian ikuti petunjuk untuk menginstal AWS CLI.

Untuk akses CLI, Anda memerlukan ID kunci akses dan kunci akses rahasia. Gunakan kredensial sementara alih-alih kunci akses jangka panjang jika memungkinkan. Kredensial sementara mencakup ID kunci akses, kunci akses rahasia, dan token keamanan yang menunjukkan kapan kredensialnya kedaluwarsa. Untuk informasi selengkapnya, lihat [Menggunakan kredensial sementara dengan AWS sumber daya](#) di Panduan Pengguna IAM.

2. Buat file yang berisi informasi konfigurasi seperti kunci akses, wilayah default, dan format output perintah. Kemudian atur variabel `AWS_CONFIG_FILE` lingkungan untuk referensi file itu. Untuk instruksi terperinci, buka [Mengkonfigurasi antarmuka baris AWS perintah](#) di Panduan AWS Command Line Interface Pengguna.
3. Jalankan perintah uji untuk mengonfirmasi bahwa AWS CLI antarmuka berfungsi. Misalnya, perintah berikut harus menampilkan informasi bantuan untuk AWS CLI:

```
aws help
```

Perintah berikut akan menampilkan informasi bantuan untuk Amazon Redshift:

```
aws redshift help
```

[Untuk materi referensi tentang perintah Amazon Redshift CLI, buka Amazon Redshift di Referensi.](#)
AWS CLI

Amazon Redshift Tanpa Server

Amazon Redshift Serverless memudahkan Anda menjalankan dan menskalakan analitik tanpa harus menyediakan dan mengelola gudang data. Dengan Amazon Redshift Serverless, analis data, pengembang, dan ilmuwan data sekarang dapat menggunakan Amazon Redshift untuk mendapatkan wawasan dari data dalam hitungan detik dengan memuat data ke dalam dan menanyakan catatan dari gudang data. Amazon Redshift secara otomatis menyediakan dan menskalakan kapasitas gudang data untuk menghadirkan kinerja yang cepat untuk beban kerja yang berat dan tidak dapat diprediksi. Anda hanya membayar untuk kapasitas yang Anda gunakan. Anda bisa mendapatkan keuntungan dari kesederhanaan ini tanpa mengubah analitik dan aplikasi intelijen bisnis yang ada.

Apa itu Amazon Redshift Tanpa Server?

Amazon Redshift Serverless secara otomatis menyediakan kapasitas gudang data dan secara cerdas menskalakan sumber daya yang mendasarinya. Amazon Redshift Serverless menyesuaikan kapasitas dalam hitungan detik untuk menghadirkan kinerja tinggi secara konsisten dan operasi yang disederhanakan bahkan untuk beban kerja yang paling menuntut dan mudah berubah sekalipun.

Dengan Amazon Redshift Serverless, Anda bisa mendapatkan keuntungan dari fitur-fitur berikut:

- Akses dan analisis data tanpa perlu menyiapkan, menyetel, dan mengelola kluster yang disediakan Amazon Redshift.
- Gunakan kapabilitas Amazon Redshift SQL yang unggul, kinerja terdepan di industri, dan integrasi data-lake untuk melakukan kueri secara mulus di seluruh gudang data, data lake, dan sumber data operasional.
- Memberikan kinerja tinggi secara konsisten dan operasi yang disederhanakan untuk beban kerja yang paling menuntut dan mudah berubah dengan penskalaan cerdas dan otomatis.
- Gunakan workgroup dan namespace untuk mengatur sumber daya komputasi dan data dengan kontrol biaya granular.
- Bayar hanya ketika gudang data sedang digunakan.

Dengan Amazon Redshift Serverless, Anda menggunakan antarmuka konsol untuk menjangkau gudang data tanpa server atau API untuk membangun aplikasi. Melalui gudang data, Anda dapat mengakses penyimpanan terkelola Amazon Redshift dan data lake Amazon S3 Anda.

Video ini menunjukkan kepada Anda bagaimana Amazon Redshift Serverless memudahkan menjalankan dan menskalakan analitik tanpa harus mengelola infrastruktur gudang data:

Konsol Tanpa Server Amazon Redshift

Untuk memulai menggunakan konsol Amazon Redshift Serverless, tonton video berikut: [Memulai Amazon Redshift Tanpa Server](#).

Dasbor tanpa server

Pada halaman dasbor Tanpa Server, Anda dapat melihat ringkasan sumber daya dan grafik penggunaan Anda.

- Gambaran umum Namespace - Bagian ini menunjukkan jumlah snapshot dan datashares dalam namespace Anda.
- Workgroups - Bagian ini menampilkan semua workgroup dalam Amazon Redshift Serverless.
- Metrik kueri — Bagian ini menunjukkan aktivitas kueri selama satu jam terakhir.
- Kapasitas RPU yang digunakan - Bagian ini menunjukkan kapasitas yang digunakan selama satu jam terakhir.
- Uji coba gratis - Bagian ini menunjukkan kredit uji coba gratis yang tersisa di AWS akun Anda. Ini mencakup semua penggunaan sumber daya dan operasi Amazon Redshift Tanpa Server, termasuk snapshot, penyimpanan, workgroup, dan sebagainya, di bawah akun yang sama.
- Alarm - Bagian ini menunjukkan alarm yang Anda konfigurasi di Amazon Redshift Tanpa Server.

Pencadangan data

Pada tab Pencadangan data Anda dapat bekerja dengan yang berikut:

- Snapshots - Anda dapat membuat, menghapus, dan mengelola snapshot data Amazon Redshift Tanpa Server Anda. Periode retensi default adalah *indefinitely*, tetapi Anda dapat mengonfigurasi periode retensi menjadi nilai apa pun antara 1 dan 3653 hari. Anda dapat mengotorisasi Akun AWS untuk memulihkan ruang nama dari snapshot.
- Poin pemulihan - Menampilkan titik pemulihan yang dibuat secara otomatis sehingga Anda dapat pulih dari penulisan atau penghapusan yang tidak disengaja dalam 24 jam terakhir. Untuk memulihkan data, Anda dapat memulihkan titik pemulihan ke namespace yang tersedia. Anda dapat membuat snapshot dari titik pemulihan jika Anda ingin mempertahankan titik pemulihan

untuk jangka waktu yang lebih lama. Periode retensi default adalah *indefinitely*, tetapi Anda dapat mengonfigurasi periode retensi menjadi nilai apa pun antara 1 dan 3653 hari.

Akses data

Pada tab Akses data Anda dapat bekerja dengan yang berikut:

- Pengaturan jaringan dan keamanan - Anda dapat melihat nilai terkait VPC, nilai AWS KMS enkripsi, dan nilai pencatatan audit. Anda hanya dapat memperbarui pencatatan audit. Untuk informasi selengkapnya tentang pengaturan jaringan dan keamanan menggunakan konsol, lihat [Mengelola batas penggunaan, batas kueri, dan tugas administratif lainnya](#).
- AWS KMS key— AWS KMS key Digunakan untuk mengenkripsi sumber daya di Amazon Redshift Serverless.
- Izin — Anda dapat mengelola peran IAM yang dapat diasumsikan oleh Amazon Redshift Serverless untuk menggunakan sumber daya atas nama Anda. Untuk informasi selengkapnya, lihat [Manajemen identitas dan akses di Amazon Redshift Tanpa Server](#).
- Titik akhir VPC yang dikelola RedShift — Anda dapat mengakses instans Amazon Redshift Tanpa Server dari VPC atau subnet lain. Untuk informasi selengkapnya, lihat [Menghubungkan ke Amazon Redshift Tanpa Server dari titik akhir VPC lainnya](#).

Batas

Pada tab Limits, Anda dapat bekerja dengan yang berikut:

- Kapasitas dasar dalam pengaturan unit pemrosesan Redshift (RPU) - Anda dapat mengatur kapasitas dasar yang digunakan untuk memproses beban kerja Anda. Untuk meningkatkan kinerja kueri, tingkatkan nilai RPU Anda.
- Batas penggunaan — Sumber daya komputasi maksimum yang dapat digunakan instans Amazon Redshift Tanpa Server dalam periode waktu sebelum tindakan dimulai. Anda membatasi jumlah sumber daya yang digunakan Amazon Redshift Serverless untuk menjalankan beban kerja Anda. Penggunaan diukur dalam jam Redshift Processing Unit (RPU). Jam RPU adalah jumlah RPU yang digunakan dalam satu jam. Anda menentukan tindakan yang akan terjadi ketika Anda mencapai batas yang Anda tetapkan, sebagai berikut:
 - Kirim peringatan.
 - Log entri ke tabel sistem.
 - Matikan kueri pengguna.

Anda dapat mengatur hingga empat batas.

- Batas kueri — Anda dapat menambahkan batas untuk memantau kinerja dan batas. Untuk informasi selengkapnya tentang batas pemantauan kueri, lihat aturan [pemantauan kueri WLM](#).

Untuk informasi selengkapnya, lihat [Memahami kapasitas Amazon Redshift Tanpa Server](#).

Datashares

Pada tab Datashares Anda dapat bekerja dengan yang berikut:

- Datashares dibuat di pengaturan namespace saya — Anda dapat membuat datashare dan membagikannya dengan namespace lain dan. Akun AWS
- Datashares dari namespace lain dan Akun AWS — Anda dapat membuat database dari datashare dari namespace lain dan. Akun AWS

Untuk informasi selengkapnya tentang berbagi data, lihat [Berbagi data di Amazon Redshift Tanpa Server](#).

Pemantauan kueri dan basis data

Pada halaman Query dan pemantauan database, Anda dapat melihat grafik riwayat Query dan kinerja Database Anda.

Pada tab Query history, Anda melihat grafik berikut (Anda dapat memilih antara daftar Query dan Resource metrics):

- Query runtime — Grafik ini menunjukkan kueri mana yang berjalan dalam jangka waktu yang sama. Pilih bilah dalam grafik untuk melihat detail eksekusi kueri lainnya.
- Kueri dan beban - Bagian ini mencantumkan kueri dan beban berdasarkan Query ID.
- Kapasitas RPU yang digunakan - Grafik ini menunjukkan kapasitas keseluruhan dalam Unit Pemrosesan Redshift (RPU).
- Koneksi database - Grafik ini menunjukkan jumlah koneksi database aktif.

Kinerja basis data

Pada tab Kinerja Database, Anda melihat grafik berikut:

- Kueri selesai per detik — Grafik ini menunjukkan jumlah rata-rata kueri yang diselesaikan per detik.
- Durasi kueri — Grafik ini menunjukkan jumlah waktu rata-rata untuk menyelesaikan kueri.
- Koneksi database - Grafik ini menunjukkan jumlah koneksi database aktif.
- Menjalankan kueri — Grafik ini menunjukkan jumlah total kueri yang berjalan pada waktu tertentu.
- Kueri antrian — Grafik ini menunjukkan jumlah total kueri yang diantrian pada waktu tertentu.
- Perincian waktu proses kueri — Grafik ini menunjukkan total waktu kueri yang dihabiskan untuk dijalankan berdasarkan jenis kueri.

Pemantauan sumber daya

Pada halaman Pemantauan sumber daya, Anda dapat melihat grafik sumber daya yang Anda konsumsi. Anda dapat memfilter data berdasarkan beberapa aspek.

- Filter metrik - Anda dapat menggunakan filter metrik untuk memilih filter untuk grup kerja tertentu, serta memilih rentang waktu dan interval waktu.
- Kapasitas RPU yang digunakan — Grafik ini menunjukkan kapasitas keseluruhan dalam unit pemrosesan Redshift (RPU).
- Penggunaan komputasi - Grafik ini menunjukkan penggunaan jam RPU berdasarkan periode untuk rentang waktu yang dipilih. Untuk rentang waktu kurang dari 6 jam, jam RPU ditampilkan dalam waktu yang tepat. Untuk rentang waktu 6 jam atau lebih, jam RPU ditampilkan sebagai rata-rata.

Di halaman Datashares, Anda dapat mengelola datashares Di akun saya dan Dari akun lain. Untuk informasi selengkapnya tentang berbagi data, lihat [Berbagi data di Amazon Redshift Tanpa Server](#).

Pertimbangan saat menggunakan Amazon Redshift Serverless

Untuk daftar Wilayah AWS tempat Amazon Redshift Serverless tersedia, lihat titik akhir yang terdaftar untuk [Redshift](#) Serverless API di. Referensi Umum Amazon Web Services

Beberapa sumber daya yang digunakan oleh Amazon Redshift Serverless tunduk pada kuota. Untuk informasi selengkapnya, lihat [Kuota untuk objek Amazon Redshift Tanpa Server](#).

[Saat Anda MENDEKLARASIKAN kursor, spesifikasi ukuran set hasil untuk Amazon Redshift Serverless ditentukan dalam DECLARE.](#)

Jendela pemeliharaan - Tidak ada jendela pemeliharaan dengan Amazon Redshift Serverless. Pembaruan versi perangkat lunak diterapkan secara otomatis. Tidak ada gangguan untuk koneksi

atau eksekusi kueri yang ada saat Amazon Redshift beralih versi. Koneksi baru akan selalu terhubung dan bekerja dengan Amazon Redshift Serverless secara instan.

ID Availability Zone — Saat mengonfigurasi instans Amazon Redshift Tanpa Server, buka [Pertimbangan tambahan](#), dan pastikan ID subnet yang disediakan di Subnet berisi setidaknya tiga ID Availability Zone yang didukung. Untuk melihat subnet ke pemetaan ID Availability Zone, buka konsol VPC dan pilih Subnet untuk melihat daftar ID subnet dengan ID Availability Zone mereka. Verifikasi bahwa subnet Anda dipetakan ke ID Availability Zone yang didukung. Untuk membuat subnet, lihat [Membuat subnet di VPC Anda di Panduan Pengguna](#) Amazon VPC.

Tiga subnet — Anda harus memiliki setidaknya tiga subnet, dan mereka harus menjangkau tiga Availability Zone. Misalnya, Anda dapat menggunakan tiga subnet yang memetakan ke Availability Zones us-east-1a, us-east-1b, dan us-east-1c. Pengecualian untuk ini adalah Wilayah AS Barat (California N.). Ini membutuhkan tiga subnet, dengan cara yang sama seperti wilayah lain, tetapi ini harus mencakup hanya dua Availability Zone. Syaratnya adalah bahwa salah satu Availability Zone yang direntang harus berisi dua subnet.

Persyaratan alamat IP gratis - Anda harus memiliki alamat IP gratis yang tersedia saat membuat grup kerja Amazon Redshift Tanpa Server. Jumlah minimum alamat IP berskala lebih tinggi karena jumlah Redshift Processing Units (RPU) untuk kelompok kerja meningkat. Secara khusus, setiap subnet di VPC workgroup Anda memerlukan jumlah minimum alamat IP. Untuk informasi selengkapnya tentang mengalokasikan alamat IP, lihat [Pengalaman IP di Panduan](#) Pengguna Amazon VPC.

Jumlah alamat IP gratis minimum yang diperlukan saat membuat workgroup adalah sebagai berikut:

Jumlah alamat IP gratis yang diperlukan untuk setiap subnet

Unit Pemrosesan Pergeseran Merah (RPU)	Diperlukan alamat IP gratis	Ukuran CIDR minimum
8	9	/27
16	15	/27
32	13	/27
64	21	/27
128	37	/26
256	69	/25

Unit Pemrosesan Pergeseran Merah (RPU)	Diperlukan alamat IP gratis	Ukuran CIDR minimum
512	133	/24

Anda juga memerlukan alamat IP gratis saat memperbarui workgroup Anda untuk menggunakan lebih banyak RPU. Jumlah alamat IP gratis yang diperlukan saat memperbarui subnet untuk workgroup adalah sebagai berikut:

Jumlah alamat IP gratis yang diperlukan saat memperbarui subnet

Unit Pemrosesan Pergeseran Merah (RPU)	Unit Pemrosesan Redshift (RPU) yang Diperbarui	Diperlukan alamat IP gratis
8	16	10
16	32	13
32	64	16
64	128	28
128	256	52
256	512	100

Ruang penyimpanan setelah migrasi — Saat memigrasikan cluster kecil yang disediakan Amazon Redshift ke Amazon Redshift Tanpa Server, Anda mungkin melihat peningkatan alokasi ruang penyimpanan setelah migrasi. Ini adalah hasil dari alokasi ruang penyimpanan yang dioptimalkan, menghasilkan ruang penyimpanan yang telah dialokasikan sebelumnya. Ruang ini digunakan selama periode waktu tertentu karena data tumbuh di Amazon Redshift Tanpa Server.

Datasharing antara Amazon Redshift Serverless dan Amazon Redshift yang disediakan cluster — Saat datasharing di mana Amazon Redshift Serverless adalah produsen dan cluster yang disediakan adalah konsumen, cluster yang disediakan harus memiliki versi cluster lebih lambat dari 1.0.38214. Jika Anda menggunakan versi cluster lebih awal dari ini, kesalahan terjadi saat Anda menjalankan kueri. Anda dapat melihat versi cluster di konsol Amazon Redshift di tab Maintenance. Anda juga bisa lari `SELECT version();`.

Waktu eksekusi kueri maksimum - Waktu eksekusi yang berlalu untuk kueri, dalam hitungan detik. Waktu eksekusi tidak termasuk waktu yang dihabiskan menunggu dalam antrian. Jika kueri melebihi waktu eksekusi yang ditetapkan, Amazon Redshift Serverless menghentikan kueri. Nilai yang valid adalah 0—86.399.

Migrasi untuk tabel dengan kunci pengurutan yang disisipkan — Saat memigrasikan klaster yang disediakan Amazon Redshift ke Amazon Redshift Tanpa Server, Redshift mengonversi tabel dengan tombol pengurutan interleaved dan DISTSTYLE KEY menjadi kunci pengurutan majemuk. DISTSTYLE tidak berubah. Untuk informasi selengkapnya tentang gaya distribusi, lihat [Bekerja dengan gaya distribusi data](#) di Panduan Pengembang Amazon Redshift. Untuk informasi selengkapnya tentang kunci sortir, lihat [Bekerja dengan kunci sortir](#).

Berbagi VPC - Anda dapat membuat grup kerja Amazon Redshift Tanpa Server di VPC bersama. Jika Anda melakukannya, kami menyarankan agar Anda tidak menghapus pembagian sumber daya karena dapat mengakibatkan workgroup menjadi tidak tersedia.

Kapasitas komputasi untuk Amazon Redshift Serverless

Memahami kapasitas Amazon Redshift Tanpa Server

RPU

Amazon Redshift Serverless mengukur kapasitas gudang data di Redshift Processing Units (RPU). RPU adalah sumber daya yang digunakan untuk menangani beban kerja.

Kapasitas dasar

Setelan ini menentukan kapasitas gudang data dasar yang digunakan Amazon Redshift untuk menyajikan kueri. Kapasitas dasar ditentukan dalam RPU. Anda dapat mengatur kapasitas dasar di Redshift Processing Units (RPU). Satu RPU menyediakan memori 16 GB. Menetapkan kapasitas dasar yang lebih tinggi meningkatkan kinerja kueri, terutama untuk pekerjaan pemrosesan data yang menghabiskan banyak sumber daya. Kapasitas dasar default untuk Amazon Redshift Serverless adalah 128 RPU. Anda dapat menyesuaikan pengaturan kapasitas Basis dari 8 RPU ke 512 RPU dalam unit 8 (8,16,24... 512), menggunakan AWS konsol, operasi UpdateWorkgroup API, atau operasi di `update-workgroup` AWS CLI

Dengan kapasitas minimum 8 RPU, Anda sekarang memiliki lebih banyak fleksibilitas untuk menjalankan beban kerja yang lebih sederhana hingga lebih kompleks berdasarkan persyaratan

kinerja. Kapasitas RPU dasar RPU 8, 16, dan 24 ditargetkan untuk beban kerja yang membutuhkan kurang dari 128TB data. Jika kebutuhan data Anda lebih besar dari 128 TB, Anda harus menggunakan minimal 32 RPU. Untuk beban kerja yang memiliki tabel dengan kolom angka besar dan konkurensi yang lebih tinggi, sebaiknya gunakan 32 RPU atau lebih.

Pertimbangan dan batasan untuk kapasitas Amazon Redshift Tanpa Server

Berikut ini adalah pertimbangan dan batasan untuk kapasitas Amazon Redshift Serverless.

- Konfigurasi 8 atau 16 RPU mendukung kapasitas penyimpanan terkelola Redshift hingga 128 TB. Jika Anda menggunakan lebih dari 128 TB penyimpanan terkelola, Anda tidak dapat menurunkan versi ke kurang dari 32 RPU.
- Mengedit kapasitas dasar grup kerja Anda mungkin membatalkan beberapa kueri yang berjalan di workgroup Anda.

Penskalaan dan pengoptimalan berbasis AI (pratinjau)

Ini adalah dokumentasi prarilis untuk penskalaan dan pengoptimalan berbasis AI di Amazon Redshift Serverless, yang ada dalam rilis pratinjau. Dokumentasi dan fitur dapat berubah. Sebaiknya gunakan fitur ini hanya dalam lingkungan pengujian, bukan dalam lingkungan produksi. Untuk syarat dan ketentuan pratinjau, lihat Beta dan Pratinjau dalam [Persyaratan Layanan AWS](#).

Pratinjau ini tersedia sebagai berikut Wilayah AWS:

- AS Timur (Ohio) (us-east-2)
- US East (N. Virginia) (us-east-1)
- US West (Oregon) (us-west-2)
- Asia Pacific (Tokyo) (ap-northeast-1)
- Europe (Ireland) (eu-west-1)
- Eropa (Stockholm) (eu-north-1)

Anda dapat membuat workgroup pratinjau untuk menguji fitur baru Amazon Redshift Serverless. Anda tidak dapat menggunakan fitur tersebut dalam produksi memindahkan workgroup Anda ke workgroup lain. Untuk syarat dan ketentuan pratinjau, lihat Beta dan Pratinjau di [Ketentuan AWS](#)

[Layanan](#). Untuk petunjuk tentang cara membuat grup kerja pratinjau, lihat [Membuat grup kerja pratinjau](#).

Anda juga dapat menetapkan target harga-kinerja untuk grup kerja Anda, sehingga Redshift dapat secara otomatis membuat pengoptimalan berbasis AI ke sumber daya Anda. Dengan cara itu, Anda dapat memenuhi target harga-kinerja Anda sambil mengoptimalkan biaya. Optimalisasi harga-kinerja otomatis ini sangat membantu jika Anda tidak tahu kapasitas dasar apa yang harus ditetapkan untuk beban kerja Anda, atau jika beberapa bagian dari beban kerja Anda mungkin mendapat manfaat dari lebih banyak sumber daya yang dialokasikan.

Misalnya, jika organisasi Anda biasanya menjalankan beban kerja yang hanya memerlukan 32 RPU tetapi tiba-tiba memperkenalkan kueri yang lebih kompleks, Anda mungkin tidak mengetahui jumlah kapasitas dasar yang sesuai. Menetapkan kapasitas dasar yang lebih tinggi menghasilkan kinerja harga yang lebih baik tetapi juga menimbulkan biaya yang lebih tinggi, sehingga biayanya mungkin tidak sesuai dengan harapan Anda. Menggunakan penskalaan berbasis AI dan pengoptimalan sumber daya, Amazon Redshift Serverless secara otomatis menyesuaikan RPU untuk memenuhi target kinerja harga Anda sambil menjaga biaya dioptimalkan untuk organisasi Anda. Optimalisasi otomatis ini berguna terlepas dari ukuran beban kerja. Pengoptimalan otomatis dapat membantu Anda memenuhi target kinerja harga organisasi Anda jika Anda memiliki sejumlah kueri kompleks.

Target harga-kinerja adalah pengaturan khusus kelompok kerja. Kelompok kerja yang berbeda dapat memiliki target harga-kinerja yang berbeda.

Agar biaya tetap dapat diprediksi, tetapkan batas kapasitas maksimum yang diizinkan untuk dialokasikan oleh Amazon Redshift Serverless ke beban kerja Anda.

Untuk mengonfigurasi target harga-kinerja, gunakan konsol. AWS Secara default, target harga-kinerja diaktifkan saat Anda membuat grup kerja baru dan disetel ke Balanced. Untuk menetapkan target harga-kinerja yang berbeda atau menentukan kapasitas dasar untuk grup kerja Anda, gunakan pengaturan yang disesuaikan saat membuat grup kerja. Untuk informasi selengkapnya tentang membuat workgroup, lihat [Membuat workgroup dengan](#) namespace.

Untuk mengedit target harga-kinerja untuk grup kerja Anda:

1. Di konsol Amazon Redshift Tanpa Server, pilih konfigurasi Workgroup.
2. Pilih workgroup yang ingin Anda edit target harga-kinerja. Pilih tab Performance, lalu pilih Edit.
3. Pilih target Price-performance, dan sesuaikan slider sesuai dengan target yang ingin Anda atur workgroup.

4. Pilih Simpan perubahan.

Untuk memperbarui jumlah maksimum RPU yang dapat dialokasikan Amazon Redshift Serverless ke beban kerja Anda, buka tab Batas konfigurasi workgroup.

Untuk mempelajari lebih lanjut tentang pengoptimalan berbasis AI dan penskalaan sumber daya, tonton video berikut.

Penagihan untuk Amazon Redshift Tanpa Server

Harga

Untuk informasi harga, lihat harga [Amazon Redshift](#).

Penagihan untuk kapasitas komputasi

Kapasitas dasar dan pengaruhnya terhadap penagihan

Saat kueri berjalan, Anda ditagih sesuai dengan kapasitas yang digunakan dalam durasi tertentu, dalam jam RPU per detik. Saat tidak ada kueri yang berjalan, Anda tidak ditagih untuk kapasitas komputasi. Anda juga dikenakan biaya untuk Redshift Managed Storage (RMS), berdasarkan jumlah data yang disimpan.

Saat Anda membuat workgroup, Anda memiliki opsi untuk mengatur kapasitas Basis untuk komputasi. Untuk memenuhi persyaratan harga/kinerja beban kerja Anda di tingkat kelompok kerja, sesuaikan kapasitas dasar yang lebih tinggi atau lebih rendah untuk kelompok kerja yang ada. Pilih workgroup dari konfigurasi Workgroup dan pilih tab Limits untuk mengubah kapasitas dasar menggunakan konsol.

Seiring bertambahnya jumlah kueri, Amazon Redshift Tanpa Server menskalakan secara otomatis untuk memberikan kinerja yang konsisten.

Batas penggunaan jam RPU maksimum

Agar biaya dapat diprediksi untuk Amazon Redshift Serverless, Anda dapat mengatur jam RPU Maksimum yang digunakan per hari, per minggu, atau per bulan. Anda dapat mengaturnya menggunakan konsol atau dengan API. Ketika batas tercapai, Anda dapat menentukan bahwa entri log ditulis ke tabel sistem, atau Anda menerima peringatan, atau kueri pengguna dimatikan. Mengatur

jam RPU maksimum membantu menjaga biaya Anda tetap terkendali. Pengaturan untuk jam RPU maksimum berlaku untuk grup kerja untuk kueri yang mengakses data di gudang data dan kueri yang mengakses data eksternal, seperti di tabel eksternal di Amazon S3.

Berikut ini adalah contohnya:

Asumsikan Anda menetapkan batas untuk 100 jam untuk setiap minggu. Untuk melakukan ini di konsol, Anda melakukan hal berikut:

1. Pilih grup kerja Anda, lalu pilih Kelola batas penggunaan di bawah tab Batas.
2. Tambahkan batas penggunaan, pilih frekuensi Mingguan, durasi 100 jam, dan pengaturan tindakan untuk Matikan kueri pengguna.

Dalam contoh ini, jika Anda mencapai batas 100 jam RPU selama seminggu, kueri dimatikan.

Menyetel jam RPU maksimum untuk grup kerja tidak membatasi kinerja atau sumber daya komputasi untuk grup kerja. Anda dapat menyesuaikan pengaturan kapan saja tanpa mempengaruhi pemrosesan kueri. Tujuan untuk menetapkan jam RPU maksimum adalah untuk membantu Anda memenuhi persyaratan harga dan kinerja Anda. [Untuk informasi selengkapnya tentang penagihan tanpa server, lihat harga Amazon Redshift.](#)

Cara lain untuk menjaga biaya Amazon Redshift Serverless dapat diprediksi adalah dengan menggunakan [Deteksi Anomali AWS Biaya](#) untuk mengurangi kemungkinan kejutan penagihan dan memberikan kontrol lebih besar.

Note

[Kalkulator harga Amazon Redshift](#) sangat membantu untuk memperkirakan harga. Anda memasukkan sumber daya komputasi yang Anda butuhkan dan menyediakan pratinjau biaya.

Menetapkan kapasitas Maks untuk mengontrol biaya untuk sumber daya komputasi

Pengaturan kapasitas Max berfungsi sebagai plafon RPU yang dapat ditingkatkan oleh Amazon Redshift Serverless. Ini membantu mengontrol biaya Anda untuk sumber daya komputasi. Dengan cara yang mirip dengan bagaimana kapasitas dasar menetapkan jumlah minimum sumber daya komputasi yang tersedia, kapasitas Max menetapkan batas atas penggunaan RPU. Dengan begitu,

ini membantu pengeluaran Anda mematuhi rencana Anda. Kapasitas maksimum berlaku khusus untuk setiap kelompok kerja dan membatasi penggunaan komputasi setiap saat.

Bagaimana kapasitas Max berbeda dari batas penggunaan jam RPU

Tujuan dari batas jam RPU maksimum dan pengaturan kapasitas Max adalah untuk mengontrol biaya. Tetapi mereka mencapai ini melalui cara yang berbeda. Poin-poin berikut menjelaskan perbedaannya:

- Kapasitas maksimum - Pengaturan ini menetapkan jumlah RPU tertinggi yang digunakan Amazon Redshift Serverless untuk tujuan penskalaan. Ketika penskalaan komputasi otomatis diperlukan, memiliki nilai yang lebih tinggi untuk kapasitas Max dapat meningkatkan throughput kueri. Ketika batas kapasitas Max tercapai, kelompok kerja tidak meningkatkan sumber daya lebih jauh.
- Batas penggunaan jam RPU maksimum - Tidak seperti kapasitas Max, pengaturan ini tidak menetapkan batas kapasitas. Tapi itu melakukan tindakan lain untuk membantu Anda membatasi biaya. Ini termasuk menambahkan entri ke log, memberi tahu Anda, atau menghentikan kueri agar tidak berjalan, jika Anda mau.

Anda dapat menggunakan kapasitas Max secara eksklusif, atau Anda dapat memujinya dengan tindakan dari batas penggunaan jam RPU maksimum.

Kasus penggunaan kapasitas Maks

Setiap workgroup dapat memiliki pengaturan kapasitas Max yang berbeda. Ini membantu Anda menegakkan persyaratan anggaran. Untuk mengilustrasikan cara kerjanya, asumsikan hal berikut:

- Anda memiliki workgroup dengan kapasitas dasar yang disetel ke 256 RPU. Anda memiliki beban kerja yang stabil di lebih dari 256 RPU hampir sepanjang bulan.
- Kapasitas maks diatur ke 512 RPU.

Asumsikan Anda memiliki penggunaan tinggi yang tidak terduga selama periode tiga hari untuk menghasilkan laporan statistik ad-hoc. Dalam hal ini, Anda memiliki kapasitas Max yang disetel untuk menghindari biaya komputasi di luar biaya untuk 512 RPU. Ketika Anda melakukan ini, Anda dapat yakin bahwa kapasitas komputasi tidak akan melebihi batas atas ini.

Catatan penggunaan untuk kapasitas Max

Catatan ini dapat membantu Anda mengatur kapasitas Max dengan tepat:

- Setiap workgroup Amazon Redshift Tanpa Server dapat memiliki pengaturan kapasitas Maks yang berbeda.
- Jika Anda memiliki periode penggunaan sumber daya yang sangat tinggi dan kapasitas Max diatur ke tingkat RPU rendah, itu dapat menunda pemrosesan beban kerja dan menghasilkan pengalaman pengguna yang tidak optimal.
- Mengkonfigurasi pengaturan kapasitas Max tidak mengganggu kueri yang sedang berjalan, bahkan selama masa penggunaan RPU tinggi. Itu tidak berfungsi seperti batas penggunaan, yang dapat menghentikan kueri agar tidak berjalan. Ini hanya membatasi sumber daya komputasi yang tersedia untuk workgroup. Anda dapat melihat kapasitas yang digunakan selama periode waktu tertentu di dasbor Amazon Redshift Tanpa Server. Untuk informasi selengkapnya tentang melihat data ringkasan, lihat [Memeriksa data ringkasan Amazon Redshift Tanpa Server menggunakan dasbor](#).
- Pengaturan kapasitas Max teratas adalah 5632 RPU.

Cara mengatur kapasitas Max

Anda dapat mengatur kapasitas Max di konsol. Untuk workgroup yang ada, Anda dapat mengubah pengaturan di bawah konfigurasi Workgroup. Anda juga dapat menggunakan CLI untuk mengaturnya dengan menggunakan perintah seperti contoh berikut:

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

Ini menetapkan pengaturan kapasitas Max untuk workgroup dengan nama yang diberikan. Setelah mengaturnya, Anda dapat memeriksa nilai pada konsol untuk memverifikasinya. Anda juga dapat memeriksa nilai menggunakan CLI dengan menjalankan perintah. `get-workgroup`

Anda dapat mematikan pengaturan kapasitas Max dengan menyetelnya -1, seperti berikut ini:

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

Memantau penggunaan dan biaya Amazon Redshift Tanpa Server

Ada beberapa cara Anda dapat memperkirakan penggunaan dan penagihan untuk Amazon Redshift Serverless. Tampilan sistem dapat membantu karena metadata sistem, termasuk kueri dan data penggunaan, tepat waktu dan Anda tidak perlu melakukan pengaturan apa pun untuk menanyakannya. CloudWatch juga dapat berguna untuk memantau penggunaan instans Amazon

Redshift Tanpa Server Anda, dan memiliki fitur tambahan untuk memberikan wawasan dan menetapkan tindakan.

Memvisualisasikan penggunaan dengan menanyakan tampilan sistem

Kueri tabel sistem SYS_SERVERLESS_USAGE untuk melacak penggunaan dan mendapatkan biaya untuk kueri:

```
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
```

Kueri ini memberikan biaya per hari yang dikeluarkan untuk Amazon Redshift Tanpa Server, berdasarkan penggunaan.

Catatan penggunaan untuk menentukan penggunaan dan biaya

- Anda membayar beban kerja yang Anda jalankan dalam RPU-jam per detik, dengan biaya minimum 60 detik.
- Catatan dari tabel sistem sys_serverless_usage menunjukkan biaya yang dikeluarkan dalam interval waktu 1 menit. Memahami kolom berikut ini penting:

Kolom charged_seconds:

- Menyediakan unit komputasi (RPU) detik yang diisi selama interval waktu. Hasilnya termasuk biaya minimum apa pun di Amazon Redshift Tanpa Server.
- Memiliki informasi tentang penggunaan sumber daya komputasi setelah transaksi selesai. Dengan demikian, nilai kolom ini mungkin 0 jika transaksi belum selesai.

Kolom compute_seconds:

- Menyediakan informasi penggunaan komputasi waktu nyata. Ini tidak termasuk biaya minimum apa pun di Amazon Redshift Serverless. Dengan demikian dapat berbeda sampai tingkat tertentu dari detik yang dibebankan yang ditagih selama interval.
- Menampilkan informasi penggunaan selama setiap transaksi (bahkan jika transaksi belum berakhir), dan karenanya data yang diberikan adalah real-time.
- Ada situasi di mana compute_seconds adalah 0 tetapi charged_seconds lebih besar dari 0, atau sebaliknya. Ini adalah perilaku normal yang dihasilkan dari cara data direkam dalam tampilan

sistem. Untuk representasi detail penggunaan tanpa server yang lebih akurat, kami sarankan untuk menggabungkan data dalam `SYS_SERVERLESS_USAGE`.

Untuk informasi selengkapnya tentang memantau tabel dan tampilan, lihat [Memantau kueri dan beban kerja dengan Amazon Redshift Tanpa Server](#).

Memvisualisasikan penggunaan dengan CloudWatch

Anda dapat menggunakan metrik yang tersedia CloudWatch untuk melacak penggunaan. Metrik yang dihasilkan CloudWatch adalah `ComputeSeconds`, menunjukkan total detik RPU yang digunakan pada menit saat ini dan `ComputeCapacity`, menunjukkan total kapasitas komputasi untuk menit itu. Metrik penggunaan juga dapat ditemukan di konsol Redshift di dasbor Redshift Serverless. Untuk informasi selengkapnya CloudWatch, lihat [Apa itu Amazon CloudWatch?](#)

Penagihan untuk penyimpanan

Kapasitas penyimpanan primer ditagih sebagai Redshift Managed Storage (RMS). Penyimpanan ditagih oleh GB/bulan. Penagihan penyimpanan terpisah dari penagihan untuk kapasitas komputasi. Penyimpanan yang digunakan untuk snapshot pengguna ditagih dengan tarif penagihan cadangan standar, tergantung pada tingkat penggunaan Anda.

Biaya transfer data dan biaya pembelajaran mesin (ML) berlaku secara terpisah, sama seperti cluster yang disediakan. Replikasi snapshot dan berbagi data di seluruh AWS Wilayah ditagih dengan tarif transfer yang diuraikan pada halaman harga. Untuk informasi selengkapnya, lihat [harga Amazon Redshift](#).

Memvisualisasikan penggunaan tagihan dengan CloudWatch

`MetricSnapshotStorage`, yang melacak penggunaan penyimpanan snapshot, dibuat dan dikirim ke CloudWatch. Untuk informasi selengkapnya CloudWatch, lihat [Apa itu Amazon CloudWatch?](#)

Menggunakan uji coba gratis Amazon Redshift Serverless

Amazon Redshift Serverless menawarkan uji coba gratis. Jika Anda berpartisipasi dalam uji coba gratis, Anda dapat melihat saldo kredit uji coba gratis di konsol Redshift, dan memeriksa penggunaan uji coba gratis di tampilan [sistem SYS_SERVERLESS_USAGE](#). Perhatikan bahwa detail penagihan untuk penggunaan uji coba gratis tidak muncul di konsol penagihan. Anda hanya dapat melihat penggunaan di konsol penagihan setelah uji coba gratis berakhir. [Untuk informasi lebih lanjut tentang uji coba gratis Amazon Redshift Serverless, lihat uji coba gratis Amazon Redshift Serverless.](#)

Catatan penggunaan penagihan

- Penggunaan rekaman - Permintaan atau transaksi hanya diukur dan dicatat setelah transaksi selesai, digulung kembali, atau dihentikan. Misalnya, jika transaksi berjalan selama dua hari, penggunaan RPU dicatat setelah selesai. Anda dapat memantau penggunaan yang sedang berlangsung secara real time dengan melakukan `querysys_serverless_usage`. Pencatatan transaksi dapat mencerminkan variasi penggunaan RPU dan biaya efek untuk jam tertentu dan untuk penggunaan sehari-hari.
- Menulis transaksi eksplisit - Ini penting sebagai praktik terbaik untuk mengakhiri transaksi. Jika Anda tidak mengakhiri atau mengembalikan transaksi terbuka, Amazon Redshift Serverless terus menggunakan RPU. Misalnya, jika Anda menulis eksplisit `BEGIN TRAN`, penting untuk memiliki korespondensi `COMMIT` dan `ROLLBACK` pernyataan.
- Kueri yang dibatalkan - Jika Anda menjalankan kueri dan membatalkannya sebelum selesai, Anda masih ditagih untuk waktu kueri dijalankan.
- Penskalaan - Instans Amazon Redshift Tanpa Server dapat memulai penskalaan untuk menangani periode pemuatan yang lebih tinggi, untuk mempertahankan kinerja yang konsisten. Penagihan Amazon Redshift Tanpa Server Anda mencakup komputasi dasar dan kapasitas skala pada tingkat RPU yang sama.
- Penskalaan - Amazon Redshift Serverless meningkatkan skala dari kapasitas RPU dasarnya untuk menangani periode beban yang lebih tinggi. Dalam beberapa kasus, kapasitas RPU dapat tetap pada pengaturan yang lebih tinggi untuk periode setelah beban kueri turun. Kami menyarankan Anda mengatur jam RPU maksimum di konsol untuk menjaga terhadap biaya yang tidak terduga.
- Tabel sistem - Saat Anda menanyakan tabel sistem, waktu kueri ditagih.
- Redshift Spectrum - Jika Anda memiliki Amazon Redshift Serverless, dan Anda menjalankan kueri, tidak ada biaya terpisah untuk kueri data-lake. Untuk kueri pada data yang disimpan di Amazon S3, biayanya sama, berdasarkan waktu transaksi, seperti kueri pada data lokal.
- Kueri federasi - Kueri federasi dibebankan dalam hal RPU yang digunakan selama interval waktu tertentu, dengan cara yang sama seperti kueri di gudang data atau data lake.
- Penyimpanan - Penyimpanan ditagih secara terpisah, berdasarkan GB/bulan.
- Biaya minimum - Biaya minimum adalah untuk 60 detik penggunaan sumber daya, diukur berdasarkan per detik.
- Penagihan snapshot - Penagihan snapshot tidak berubah. Ini dibebankan sesuai dengan penyimpanan, ditagih dengan tarif GB/bulan. Anda dapat mengembalikan gudang data Anda

ke titik-titik tertentu dalam 24 jam terakhir dengan perincian 30 menit, gratis. Untuk informasi selengkapnya, lihat [harga Amazon Redshift](#).

Praktik terbaik Amazon Redshift Tanpa Server untuk menjaga penagihan tetap dapat diprediksi

Berikut ini adalah praktik terbaik dan pengaturan bawaan yang membantu menjaga penagihan Anda tetap konsisten.

- Pastikan untuk mengakhiri setiap transaksi. Ketika Anda menggunakan BEGIN untuk memulai transaksi, penting untuk END itu juga.
- Gunakan penanganan kesalahan praktik terbaik untuk merespons kesalahan dengan anggun dan mengakhiri setiap transaksi. Meminimalkan transaksi terbuka membantu menghindari penggunaan RPU yang tidak perlu.
- Gunakan SESSION TIMEOUT untuk membantu mengakhiri transaksi terbuka dan sesi idle. Ini menyebabkan sesi apa pun tetap diam atau tidak aktif selama lebih dari 3600 detik (1 jam) untuk waktu habis. Ini menyebabkan setiap transaksi tetap terbuka dan tidak aktif selama lebih dari 21600 detik (6 jam) hingga time out. Pengaturan batas waktu ini dapat diubah secara eksplisit untuk pengguna tertentu, seperti saat Anda ingin membuka sesi untuk kueri yang berjalan lama. Topik [CREATE USER](#) menunjukkan cara menyesuaikan SESSION TIMEOUT untuk pengguna.
- Dalam kebanyakan kasus, kami menyarankan Anda untuk tidak memperpanjang SESSION TIMEOUT nilainya, kecuali jika Anda memiliki kasus penggunaan yang mengharuskannya secara khusus. Jika sesi tetap menganggur, dengan transaksi terbuka, itu dapat mengakibatkan kasus di mana RPU digunakan sampai sesi ditutup. Ini akan menghasilkan biaya yang tidak perlu.
- Amazon Redshift Serverless memiliki waktu maksimum 86.399 detik (24 jam) untuk kueri yang berjalan. Periode maksimum tidak aktif untuk transaksi terbuka adalah enam jam sebelum Amazon Redshift Serverless mengakhiri sesi yang terkait dengan transaksi. Untuk informasi selengkapnya, lihat [Kuota untuk objek Amazon Redshift Tanpa Server](#).

Menghubungkan ke Amazon Redshift Tanpa Server

Setelah menyiapkan instans Amazon Redshift Tanpa Server, Anda dapat menghubungkannya dengan berbagai metode, yang diuraikan di bawah ini. Jika Anda memiliki beberapa tim atau proyek dan ingin mengelola biaya secara terpisah, Anda dapat menggunakan terpisah Akun AWS.

Untuk daftar Wilayah AWS tempat Amazon Redshift Serverless tersedia, lihat titik akhir yang terdaftar untuk [Redshift](#) Serverless API di. Referensi Umum Amazon Web Services

Amazon Redshift Tanpa Server terhubung ke lingkungan tanpa server di lingkungan Anda saat ini. Akun AWS Wilayah AWS Amazon Redshift Serverless berjalan dalam VPC dalam rentang port 5431-5455 dan 8191-8215. Defaultnya adalah 5439. Saat ini, Anda hanya dapat mengubah port dengan operasi API UpdateWorkgroup dan AWS CLI operasiupdate-workgroup.

Menghubungkan ke Amazon Redshift Tanpa Server

Anda dapat terhubung ke database (bernamadev) di Amazon Redshift Serverless dengan sintaks berikut.

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

Misalnya, string koneksi berikut menentukan Region us-east-1.

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

Menghubungkan ke Amazon Redshift Tanpa Server melalui driver JDBC

Anda dapat menggunakan salah satu metode berikut untuk terhubung ke Amazon Redshift Tanpa Server dengan klien SQL pilihan Anda menggunakan driver JDBC versi 2 yang disediakan Amazon RedShift.

Untuk terhubung dengan kredensi login untuk otentikasi database menggunakan driver JDBC versi 2.1.x atau yang lebih baru, gunakan sintaks berikut. Nomor port adalah opsional; jika tidak disertakan, Amazon Redshift Serverless default ke nomor port 5439. Anda dapat mengubah ke port lain dari rentang port 5431-5455 atau 8191-8215. Untuk mengubah port default untuk titik akhir tanpa server, gunakan API Amazon AWS CLI Redshift dan Amazon.

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

Misalnya, string koneksi berikut menentukan default workgroup, ID akun 123456789012, dan Region us-east-2.

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

Untuk terhubung dengan IAM menggunakan driver JDBC versi 2.1.x atau yang lebih baru, gunakan sintaks berikut. Nomor port adalah opsional; jika tidak disertakan, Amazon Redshift Serverless default ke nomor port 5439. Anda dapat mengubah ke port lain dari rentang port 5431-5455 atau 8191-8215. Untuk mengubah port default untuk titik akhir tanpa server, gunakan API Amazon AWS CLI Redshift dan Amazon.

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

Misalnya, string koneksi berikut menentukan default workgroup, ID akun 123456789012, dan Region us-east-2.

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

Untuk ODBC, gunakan sintaks berikut.

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

Jika Anda menggunakan versi driver JDBC sebelum 2.1.0.9 dan terhubung dengan IAM, Anda harus menggunakan sintaks berikut.

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

Misalnya, string koneksi berikut menentukan workgroup default dan Wilayah AWS us-east-1.

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

Untuk informasi lebih lanjut tentang driver, lihat [Mengonfigurasi koneksi di Amazon Redshift](#).

Menemukan string koneksi JDBC dan ODBC Anda

Untuk terhubung ke workgroup Anda dengan alat klien SQL Anda, Anda harus memiliki string koneksi JDBC atau ODBC. Anda dapat menemukan string koneksi di konsol Amazon Redshift Tanpa Server, di halaman detail grup kerja.

Untuk menemukan string koneksi untuk workgroup

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Redshift Serverless.
3. Pada menu navigasi, pilih konfigurasi Workgroup, lalu pilih nama workgroup dari daftar untuk membuka detailnya.
4. String koneksi URL JDBC dan URL ODBC tersedia, bersama dengan detail tambahan, di bagian Informasi umum. Setiap string didasarkan pada AWS Wilayah tempat workgroup berjalan. Pilih ikon di sebelah string koneksi yang sesuai untuk menyalin string koneksi.

Menghubungkan ke Amazon Redshift Tanpa Server dengan API Data

Anda juga dapat menggunakan Amazon Redshift Data API untuk terhubung ke Amazon Redshift Tanpa Server. Gunakan `workgroup-name` parameter alih-alih `cluster-identifier` parameter dalam AWS CLI panggilan Anda.

Untuk informasi selengkapnya tentang API Data, lihat [Menggunakan API Data Amazon Redshift](#). Misalnya kode yang memanggil Data API dengan Python dan contoh lainnya, lihat [Memulai dengan Redshift Data API](#) dan lihat di folder dan `quick-start`. `use-cases` GitHub

Menghubungkan dengan SSL ke Amazon Redshift Tanpa Server

Mengonfigurasi koneksi aman ke Amazon Redshift Tanpa Server

Untuk mendukung koneksi SSL, Redshift Serverless membuat dan menginstal sertifikat SSL ([ACM](#)) [AWS Certificate Manager yang dikeluarkan untuk](#) setiap workgroup. Sertifikat ACM dipercaya publik oleh sebagian besar sistem operasi, browser web, dan klien. Anda mungkin perlu mengunduh bundel sertifikat jika klien atau aplikasi SQL Anda terhubung ke Redshift Tanpa Server menggunakan SSL dengan opsi koneksi disetel `sslmode ke,,` atau `require verify-ca verify-full`. Jika klien Anda membutuhkan sertifikat, Redshift Serverless menyediakan sertifikat bundel sebagai berikut:

- Unduh bundel dari [https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle .crt](https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt).
- Nomor checksum MD5 yang diharapkan adalah `418dea9b6d5d5de7a8f1ac42e164cdcf`.
- Nomor checksum sha256 adalah `36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550`.

Jangan gunakan bundel sertifikat sebelumnya yang berada di <https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt>.

- Di China Wilayah AWS, unduh bundel dari <https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt>.
 - Nomor checksum MD5 yang diharapkan adalah 418dea9b6d5d5de7a8f1ac42e164cdf.
 - Nomor checksum sha256 adalah 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

Jangan gunakan bundel sertifikat sebelumnya yang berada di <https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt> dan <https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem>

Important

Redshift Serverless telah mengubah cara sertifikat SSL dikelola. Anda mungkin perlu memperbarui sertifikat CA root kepercayaan Anda saat ini untuk terus terhubung ke grup kerja menggunakan SSL. Untuk informasi selengkapnya tentang sertifikat ACM untuk koneksi SSL, lihat [Transisi ke sertifikat ACM untuk koneksi SSL](#)

Secara default, database workgroup menerima koneksi apakah menggunakan SSL atau tidak.

Untuk membuat workgroup baru yang hanya menerima koneksi SSL, gunakan `create-workgroup` perintah dan atur parameternya `require_ssl`. `true` Untuk menggunakan contoh berikut, ganti *yourNamespaceName* dengan nama namespace Anda dan ganti *yourWorkgroupName* dengan nama workgroup Anda.

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

Untuk memperbarui workgroup yang ada agar hanya menerima koneksi SSL, gunakan `update-workgroup` perintah dan atur `require_ssl` parameternya ke `true`. Perhatikan bahwa Redshift

Serverless akan memulai ulang workgroup Anda saat Anda memperbarui parameter. `require_ssl` Untuk menggunakan contoh berikut, ganti *yourWorkgroupName* dengan nama workgroup Anda.

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

Amazon Redshift mendukung protokol perjanjian kunci Elliptic Curve Diffie—Hellman Ephemeral (ECDHE). Dengan ECDHE, klien dan server masing-masing memiliki elliptic curve public-private key pair yang digunakan untuk membangun rahasia bersama melalui saluran yang tidak aman. Anda tidak perlu mengonfigurasi apa pun di Amazon Redshift untuk mengaktifkan ECDHE. Jika Anda terhubung dari alat klien SQL yang menggunakan ECDHE untuk mengenkripsi komunikasi antara klien dan server, Amazon Redshift menggunakan daftar sandi yang disediakan untuk membuat koneksi yang sesuai. [Untuk informasi lebih lanjut, lihat Elliptic curve diffie—hellman di Wikipedia dan Ciphers di situs web OpenSSL.](#)

Mengonfigurasi koneksi SSL yang sesuai dengan FIPS ke Amazon Redshift Tanpa Server

Untuk membuat workgroup baru yang menggunakan koneksi SSL yang sesuai dengan FIPS, gunakan `create-workgroup` perintah dan atur parameternya. `use_fips_ssl true` Untuk menggunakan contoh berikut, ganti *yourNamespaceName* dengan nama namespace Anda dan ganti *yourWorkgroupName* dengan nama workgroup Anda.

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

Untuk memperbarui workgroup yang ada agar menggunakan koneksi SSL yang sesuai dengan FIPS, gunakan `update-workgroup` perintah dan atur parameternya ke. `use_fips_ssl true` Perhatikan bahwa Redshift Serverless akan memulai ulang workgroup Anda saat Anda memperbarui parameter. `use_fips_ssl` Untuk menggunakan contoh berikut, ganti *yourWorkgroupName* dengan nama workgroup Anda.

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

[Untuk informasi selengkapnya tentang mengonfigurasi Redshift Tanpa Server untuk menggunakan koneksi yang sesuai dengan FIPS, lihat `use_fips_ssl` di Panduan Pengembang Database Amazon Redshift.](#)

Menghubungkan ke Amazon Redshift Tanpa Server dari titik akhir VPC yang dikelola Amazon Redshift

Menghubungkan ke Amazon Redshift Tanpa Server dari titik akhir VPC lainnya

[Untuk informasi tentang menyiapkan atau mengonfigurasi titik akhir VPC terkelola untuk grup kerja Amazon Redshift Tanpa Server, lihat `Bekerja dengan titik akhir VPC yang dikelola RedShift`.](#)

Menghubungkan ke Amazon Redshift Tanpa Server dari titik akhir VPC Redshift di akun atau wilayah lain

Menghubungkan ke Amazon Redshift Tanpa Server dari titik akhir VPC silang

Amazon Redshift Serverless disediakan dalam VPC. Anda dapat memberikan akses ke VPC di akun lain untuk mengakses Amazon Redshift Tanpa Server di akun Anda. Ini mirip dengan koneksi dari titik akhir VPC yang dikelola, tetapi dalam hal ini koneksi berasal, misalnya, dari klien database di akun lain. Ada beberapa operasi yang dapat Anda lakukan:

- Pemilik database dapat memberikan akses ke VPC yang berisi Amazon Redshift Tanpa Server ke akun lain di Wilayah yang sama.
- Pemilik database dapat mencabut akses Amazon Redshift Tanpa Server.

Manfaat utama dari akses lintas akun adalah memungkinkan kolaborasi database yang lebih mudah. Pengguna tidak harus disediakan di akun yang berisi database untuk mengaksesnya, yang mengurangi langkah konfigurasi dan menghemat waktu.

Izin yang diperlukan untuk memberikan akses ke VPC di akun lain

Untuk memberikan akses atau mengubah akses yang diizinkan, pemberi memerlukan kebijakan izin yang ditetapkan dengan izin berikut:

- `redshift-tanpa server: PutResourcePolicy`
- `redshift-tanpa server: GetResourcePolicy`
- `redshift-tanpa server: DeleteResourcePolicy`

- EC2: CreateVpcEndpoint
- EC2: ModifyVpcEndpoint

Anda mungkin memerlukan izin lain yang ditentukan dalam kebijakan AWS AmazonRedshiftFullAccessterkelola. Untuk informasi selengkapnya, lihat [Memberikan izin ke Amazon Redshift Tanpa Server](#).

Penerima hibah memerlukan kebijakan izin yang ditetapkan dengan izin berikut:

- redshift-tanpa server: ListWorkgroups
- redshift-tanpa server: CreateEndpointAccess
- redshift-tanpa server: UpdateEndpointAccess
- redshift-tanpa server: GetEndpointAccess
- redshift-tanpa server: ListEndpointAccess
- redshift-tanpa server: DeleteEndpointAccess

Sebagai praktik terbaik, kami menyarankan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).

Ini adalah contoh kebijakan sumber daya yang digunakan untuk mengonfigurasi akses lintas-VPC:

```
{
  "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"
        ]
      }
    }
  }
}

```

Prosedur yang mengikuti di bagian ini mengasumsikan bahwa pengguna yang melakukannya memiliki izin yang ditetapkan yang sesuai, misalnya, melalui peran IAM yang ditetapkan yang memiliki izin yang terdaftar. Prosedur juga mengasumsikan bahwa workgroup memiliki peran IAM yang dilampirkan dengan izin sumber daya yang sesuai.

Memberikan akses VPC ke akun lain, menggunakan konsol

Prosedur ini menunjukkan langkah-langkah untuk mengkonfigurasi akses database ketika Anda pemilik database, dan Anda ingin memberikan akses ke sana.

Memberikan akses dari akun pemilik

1. Di properti untuk workgroup Amazon Redshift Tanpa Server, pada tab Akses data, ada daftar yang disebut Akun yang diberikan. Ini menunjukkan akun dan VPC diberikan akses ke workgroup. Temukan daftar dan pilih Berikan akses untuk menambahkan akun ke daftar.
2. Sebuah jendela muncul di mana Anda dapat menambahkan informasi penerima hibah. Masukkan ID AWS akun, yang merupakan ID 12 digit dari akun yang ingin Anda berikan akses.
3. Berikan akses ke semua VPC untuk penerima hibah, atau ke VPC tertentu. Jika Anda memberikan akses hanya ke VPC tertentu, Anda dapat menambahkan ID untuk ini dengan memasukkan masing-masing dan memilih Tambahkan VPC.
4. Simpan perubahan saat Anda selesai.

Saat Anda menyimpan perubahan, akun akan muncul di daftar akun yang Diberikan. Entri menunjukkan ID Akun dan daftar akses yang diberikan VPC.

Pemilik database juga dapat mencabut akses ke akun. Pemilik dapat mencabut akses kapan saja.

Mencabut akses ke akun

1. Anda dapat mulai dari daftar akun yang diberikan. Pertama, pilih satu atau beberapa akun.
2. Pilih Cabut akses.

Setelah akses diberikan, administrator database untuk penerima hibah dapat memeriksa konsol untuk menentukan apakah mereka memiliki akses.

Menggunakan konsol untuk mengonfirmasi bahwa akses diberikan bagi Anda untuk mengakses akun lain

1. Di properti workgroup Amazon Redshift Tanpa Server, pada tab Akses data, ada daftar yang disebut Akun resmi. Ini menunjukkan akun yang dapat diakses dari workgroup ini. Penerima hibah tidak dapat menggunakan URL titik akhir grup kerja untuk mengakses grup kerja secara langsung. Untuk mengakses workgroup, Anda sebagai penerima hibah pergi ke bagian endpoint dan memilih buat endpoint.
2. Kemudian, sebagai penerima hibah, Anda memberikan nama titik akhir dan VPC untuk mengakses workgroup.
3. Setelah endpoint berhasil dibuat, itu muncul di bagian endpoint dan ada URL endpoint untuk itu. Anda dapat menggunakan URL endpoint ini untuk mengakses workgroup.

Memberikan akses ke akun lain, menggunakan perintah CLI

Akun yang memberikan akses harus terlebih dahulu memberikan akses ke akun lain untuk terhubung dengan menggunakan `put-resource-policy`. Pemilik database dapat memanggil `put-resource-policy` untuk mengotorisasi akun lain untuk membuat koneksi ke workgroup. Akun penerima hibah kemudian dapat digunakan `create-endpoint-authorization` untuk membuat koneksi ke grup kerja melalui VPC yang diizinkan.

Berikut ini menunjukkan properti untuk `put-resource-policy`, yang dapat Anda panggil untuk memungkinkan akses ke akun dan VPC tertentu.

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

Setelah memanggil perintah, Anda dapat menelepon `get-resource-policy`, menentukan `resource-arn` untuk melihat akun dan VPC mana yang diizinkan untuk mengakses sumber daya.

Panggilan berikut dapat dilakukan oleh penerima hibah. Ini menunjukkan informasi tentang akses yang diberikan. Secara khusus, ia mengembalikan daftar yang berisi akses yang diberikan VPC.

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

Tujuannya adalah agar penerima hibah mendapatkan informasi dari akun pemberi tentang otorisasi titik akhir. `owner-account` ini adalah akun berbagi. Ketika Anda menjalankan ini, ia mengembalikan `CrossAccountVpcs` untuk setiap workgroup, yang merupakan daftar VPC yang diizinkan. Sebagai referensi, berikut ini menunjukkan semua properti yang tersedia untuk workgroup:

```
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

Sebagai pengingat, [relokasi cluster](#) bukanlah prasyarat untuk mengonfigurasi fitur jaringan Redshift tambahan. Anda juga tidak perlu mengaktifkannya untuk mengaktifkan yang berikut:

- Menghubungkan dari VPC lintas akun atau lintas wilayah ke Redshift — Anda dapat terhubung dari satu AWS virtual private cloud (VPC) ke yang lain yang berisi database Redshift, seperti yang dijelaskan di bagian ini.

- Menyiapkan nama domain khusus — Anda dapat membuat nama domain khusus, juga dikenal sebagai URL khusus, untuk klaster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server, untuk membuat nama titik akhir lebih mudah diingat dan sederhana. Untuk informasi selengkapnya, lihat [Menggunakan nama domain khusus untuk koneksi klien](#).

Mengonfigurasi pengaturan lalu lintas jaringan yang sesuai untuk Amazon Redshift Serverless

Connect ke Amazon Redshift Serverless saat dapat diakses publik

Petunjuk untuk mengatur pengaturan lalu lintas jaringan Anda tersedia di [Aksesibilitas publik dengan konfigurasi grup keamanan default atau kustom](#). Ini termasuk kasus penggunaan di mana cluster dapat diakses publik.

Connect ke Amazon Redshift Serverless saat tidak dapat diakses publik

Petunjuk untuk mengatur pengaturan lalu lintas jaringan Anda tersedia di [Aksesibilitas pribadi dengan konfigurasi grup keamanan default atau kustom](#). Ini termasuk kasus penggunaan di mana cluster tidak tersedia untuk internet.

Mendefinisikan peran database yang akan diberikan kepada pengguna federasi di Amazon Redshift Tanpa Server

Anda dapat menentukan peran di organisasi yang menentukan peran database mana yang akan diberikan di Amazon Redshift Tanpa Server. Untuk informasi selengkapnya, lihat [Mendefinisikan peran database yang akan diberikan kepada pengguna federasi di Amazon Redshift Tanpa Server](#).

Sumber daya tambahan

Untuk informasi selengkapnya tentang koneksi aman ke Amazon Redshift Tanpa Server, termasuk pemberian izin, otorisasi akses ke layanan tambahan, dan membuat peran IAM, lihat [Manajemen identitas dan akses di Amazon Redshift Tanpa Server](#)

Mendefinisikan peran database yang akan diberikan kepada pengguna federasi di Amazon Redshift Tanpa Server

Ketika Anda menjadi bagian dari organisasi, Anda memiliki kumpulan peran terkait. Misalnya, Anda memiliki peran untuk fungsi pekerjaan Anda, seperti programmer dan manajer. Peran Anda menentukan aplikasi dan data mana yang dapat Anda akses. Sebagian besar organisasi menggunakan penyedia identitas, seperti Microsoft Active Directory, untuk menetapkan peran kepada pengguna dan grup. Penggunaan peran untuk mengontrol akses sumber daya telah berkembang, karena organisasi tidak harus melakukan banyak manajemen pengguna individu.

Baru-baru ini, kontrol akses berbasis peran diperkenalkan di Amazon Redshift Serverless. Menggunakan peran database, Anda dapat mengamankan akses ke data dan objek, seperti skema atau tabel, misalnya. Atau Anda dapat menggunakan peran untuk menentukan sekumpulan izin yang ditinggikan, seperti untuk monitor sistem atau administrator database. Namun setelah Anda memberikan izin sumber daya ke peran database, ada langkah tambahan, yaitu menghubungkan peran pengguna dari organisasi ke peran database. Anda dapat menetapkan setiap pengguna ke peran database mereka saat masuk awal dengan menjalankan pernyataan SQL, tetapi itu banyak usaha. Cara yang lebih mudah adalah dengan menentukan peran database yang akan diberikan dan meneruskannya ke Amazon Redshift Tanpa Server. Ini memiliki keuntungan menyederhanakan proses masuk awal.

Anda dapat meneruskan peran ke Amazon Redshift Serverless menggunakan `GetCredentials`. Saat pengguna masuk untuk pertama kalinya ke database Amazon Redshift Tanpa Server, pengguna database terkait dibuat dan dipetakan ke peran database yang cocok. Topik ini merinci mekanisme untuk meneruskan peran ke Amazon Redshift Tanpa Server.

Melewati peran database memiliki beberapa kasus penggunaan utama:

- Ketika pengguna masuk melalui penyedia identitas pihak ketiga, biasanya dengan federasi yang dikonfigurasi, dan meneruskan peran melalui tag sesi.
- Ketika pengguna masuk melalui kredensial masuk IAM, dan peran mereka diteruskan melalui kunci tag dan nilai.

Untuk informasi selengkapnya tentang kontrol akses berbasis peran, lihat [Kontrol akses berbasis peran \(RBAC\)](#).

Mengkonfigurasi peran basis data

Sebelum Anda dapat meneruskan peran ke Amazon Redshift Serverless, Anda harus mengonfigurasi peran database dalam database Anda dan memberi mereka izin yang sesuai pada sumber daya database. Misalnya, dalam skenario sederhana, Anda dapat membuat peran database bernama penjualan dan memberikannya akses ke tabel kueri dengan data penjualan. Untuk informasi selengkapnya tentang cara membuat peran database dan memberikan izin, lihat [MEMBUAT PERAN](#) dan [PEMBERIAN](#).

Kasus penggunaan untuk mendefinisikan peran basis data yang akan diberikan kepada pengguna federasi

Bagian ini menguraikan beberapa kasus penggunaan di mana meneruskan peran database ke Amazon Redshift Tanpa Server dapat menyederhanakan akses ke sumber daya database.

Masuk menggunakan penyedia identitas

Kasus penggunaan pertama mengasumsikan bahwa organisasi Anda memiliki identitas pengguna dalam layanan manajemen identitas dan akses. Layanan ini dapat berbasis cloud, misalnya JumpCloud atau Okta, atau lokal, seperti Microsoft Active Directory. Tujuannya adalah untuk secara otomatis memetakan peran pengguna dari penyedia identitas ke peran database Anda ketika mereka masuk ke klien seperti Query editor V2, misalnya, atau dengan klien JDBC. Untuk mengatur ini, Anda harus menyelesaikan beberapa tugas konfigurasi. Sumber daya yang dimaksud meliputi:

1. Konfigurasi integrasi gabungan dengan penyedia identitas (iDP) Anda menggunakan hubungan kepercayaan. Ini adalah prasyarat. Saat Anda mengatur ini, penyedia identitas bertanggung jawab untuk mengautentikasi pengguna melalui pernyataan SAML dan memberikan kredensi masuk. Untuk informasi selengkapnya, lihat [Mengintegrasikan penyedia solusi SAMP pihak ketiga](#) dengan AWS. Anda juga dapat menemukan informasi lebih lanjut di [akses Federate ke editor kueri Amazon Redshift V2 dengan Layanan Federasi Direktori Aktif \(AD FS\) atau akses masuk tunggal Federasi ke editor kueri Amazon Redshift v2](#) dengan Okta.
2. Pengguna harus memiliki izin kebijakan berikut:
 - `GetCredentials`— Memberikan kredensi untuk otorisasi sementara untuk masuk ke Amazon Redshift Tanpa Server.
 - `sts:AssumeRoleWithSAML` Menyediakan mekanisme untuk mengikat toko identitas perusahaan atau direktori ke akses berbasis peran AWS .
 - `sts:TagSession`— Izin untuk tindakan tag-session, pada prinsipal penyedia identitas.

Dalam hal ini, `AssumeRoleWithSAML` mengembalikan satu set kredensi keamanan untuk pengguna yang telah diautentikasi melalui respons SAFL yang diautentikasi. Operasi ini menyediakan mekanisme untuk mengikat penyimpanan identitas atau direktori ke AWS akses berbasis peran tanpa kredensi khusus pengguna. Untuk pengguna dengan izin `AssumeRoleWithSAML`, penyedia identitas bertanggung jawab untuk mengelola pernyataan SAFL yang digunakan untuk meneruskan informasi peran.

Sebagai praktik terbaik, kami menyarankan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).

3. Anda mengonfigurasi tag `RedshiftDbRoles` dengan nilai peran yang dipisahkan titik dua, dalam format `role1:role2`. Misalnya, `manager:engineer`. Ini dapat diambil dari implementasi tag sesi yang dikonfigurasi di penyedia identitas Anda. Permintaan otentikasi SAML melewati peran secara terprogram. Untuk informasi selengkapnya tentang meneruskan tag sesi, lihat [Melewati tag sesi AWS STS](#).

Dalam kasus di mana Anda meneruskan nama peran yang tidak ada dalam database, itu diabaikan.

Dalam kasus penggunaan ini, ketika pengguna masuk menggunakan identitas federasi, peran mereka diteruskan dalam permintaan otorisasi melalui kunci tag sesi dan nilai. Selanjutnya, setelah otorisasi, `GetCredentials` meneruskan peran ke database. Setelah koneksi berhasil, peran database dipetakan dan pengguna dapat melakukan tugas-tugas database yang sesuai dengan peran mereka. Bagian penting dari operasi adalah bahwa tag `RedshiftDbRoles` sesi diberi peran dalam permintaan otorisasi awal. Untuk informasi selengkapnya tentang meneruskan tag sesi, lihat [Melewati tag sesi menggunakan AssumeRoleWith SAMP](#).

Masuk menggunakan kredensi IAM

Dalam kasus penggunaan kedua, peran dapat diteruskan untuk pengguna dan mereka dapat mengakses aplikasi klien database melalui kredensi IAM.

1. Pengguna yang masuk dalam kasus ini harus diberi izin kebijakan untuk tindakan berikut:
 - `tag:GetResources`— Mengembalikan sumber daya yang ditandai terkait dengan tag tertentu.
 - `tag:GetTagKeys`— Mengembalikan kunci tag yang saat ini digunakan.

Sebagai praktik terbaik, kami menyarankan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).

2. Izinkan izin juga diperlukan untuk mengakses layanan database, seperti Amazon Redshift Tanpa Server.
3. Untuk kasus penggunaan ini, konfigurasi nilai tag untuk peran Anda AWS Identity and Access Management. Anda dapat memilih untuk mengedit tag dan membuat kunci tag yang dipanggil RedshiftDbRoles dengan string nilai tag yang menyertainya yang berisi peran. Misalnya, manajer:insinyur.

Ketika pengguna log in, peran mereka ditambahkan ke permintaan otorisasi dan diteruskan ke database. Hal ini dipetakan ke peran database yang ada.

Sumber daya tambahan

Seperti yang disebutkan dalam kasus penggunaan, Anda dapat mengonfigurasi hubungan kepercayaan antara IDP dan AWS. Untuk informasi selengkapnya, lihat [Mengonfigurasi IDP SAMP 2.0 Anda dengan mengandalkan kepercayaan pihak](#) dan menambahkan klaim.

Manajemen identitas dan akses di Amazon Redshift Tanpa Server

Akses ke Amazon Redshift memerlukan kredensial yang AWS dapat digunakan untuk mengautentikasi permintaan Anda. Kredensial tersebut harus memiliki izin untuk mengakses AWS sumber daya, seperti Amazon Redshift Tanpa Server.

Bagian berikut memberikan detail tentang bagaimana Anda dapat menggunakan AWS Identity and Access Management (IAM) dan Amazon Redshift untuk membantu mengamankan sumber daya Anda dengan mengontrol siapa yang dapat mengaksesnya. Untuk informasi selengkapnya, lihat [Manajemen identitas dan akses di Amazon Redshift](#).

Memberikan izin ke Amazon Redshift Tanpa Server

Untuk mengakses AWS layanan lain, Amazon Redshift Serverless memerlukan izin.

Mengotorisasi Amazon Redshift Tanpa Server untuk mengakses layanan lain untuk Anda AWS

Beberapa fitur Amazon Redshift memerlukan Amazon Redshift untuk mengakses layanan AWS lain atas nama Anda. Agar instans Amazon Redshift Tanpa Server Anda bertindak untuk Anda, berikan kredensi keamanan padanya. Metode yang lebih disukai untuk menyediakan kredensial keamanan adalah dengan menentukan peran AWS Identity and Access Management (IAM). Anda juga dapat membuat peran IAM melalui konsol Amazon Redshift dan mengaturnya sebagai default. Untuk informasi selengkapnya, lihat [Membuat peran IAM sebagai default untuk Amazon Redshift](#).

Untuk mengakses AWS layanan lain, buat peran IAM dengan izin yang sesuai. Anda juga perlu mengaitkan peran tersebut dengan Amazon Redshift Serverless. Selain itu, tentukan Nama Sumber Daya Amazon (ARN) peran saat Anda menjalankan perintah Amazon Redshift atau tentukan kata kunci. default

Saat mengubah hubungan kepercayaan untuk peran IAM di <https://console.aws.amazon.com/iam/>, pastikan itu berisi `redshift-serverless.amazonaws.com` dan `redshift.amazonaws.com` sebagai nama layanan utama. Untuk informasi tentang cara mengelola peran IAM untuk mengakses AWS layanan lain atas nama Anda, lihat [Mengotorisasi Amazon Redshift untuk mengakses layanan AWS lain atas nama Anda](#).

Membuat peran IAM sebagai default untuk Amazon Redshift

Saat Anda membuat peran IAM melalui konsol Amazon Redshift, Amazon Redshift secara terprogram membuat peran di dalam Anda. Akun AWS Amazon Redshift juga secara otomatis melampirkan kebijakan AWS terkelola yang ada padanya. Pendekatan ini berarti Anda dapat tetap berada di dalam konsol Amazon Redshift dan tidak perlu beralih ke konsol IAM untuk pembuatan peran.

Peran IAM yang Anda buat melalui konsol untuk klaster Anda memiliki kebijakan `AmazonRedshiftAllCommandsFullAccess` terkelola yang dilampirkan secara otomatis. Peran IAM ini memungkinkan Amazon Redshift untuk menyalin, membongkar, menanyakan, dan menganalisis data AWS untuk sumber daya di akun IAM Anda. Perintah terkait termasuk COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL, dan CREATE LIBRARY. Untuk informasi selengkapnya tentang cara membuat peran IAM sebagai default untuk Amazon Redshift, lihat. [Membuat peran IAM sebagai default untuk Amazon Redshift](#)

Untuk mulai membuat peran IAM sebagai default untuk Amazon Redshift, buka AWS Management Console, pilih konsol Amazon Redshift, lalu pilih Redshift Serverless di menu. Dari dasbor Tanpa Server Anda dapat membuat grup kerja baru. Langkah-langkah pembuatan memandu Anda memilih peran IAM atau mengonfigurasi peran IAM baru.

Bila Anda memiliki workgroup Amazon Redshift Serverless yang sudah ada dan Anda ingin mengonfigurasi peran IAM untuk itu, buka AWS Management Console. Pilih konsol Amazon Redshift, lalu pilih Redshift Serverless. Di konsol Amazon Redshift Tanpa Server, pilih konfigurasi Namespace untuk grup kerja yang ada. Di bawah Keamanan dan enkripsi, Anda dapat mengedit izin.

Menetapkan peran IAM ke namespace

Setiap peran IAM adalah AWS identitas dengan kebijakan izin yang menentukan tindakan apa yang dapat dilakukan setiap peran. AWS Peran ini dimaksudkan untuk diasumsikan oleh siapa saja yang membutuhkannya. Selain itu, setiap namespace adalah kumpulan objek, seperti tabel dan skema, dan pengguna. Saat menggunakan Amazon Redshift Tanpa Server, Anda dapat mengaitkan beberapa peran IAM dengan namespace Anda. Ini membuatnya lebih mudah untuk menyusun izin Anda dengan tepat untuk kumpulan objek database, sehingga peran dapat melakukan tindakan pada data internal dan eksternal. Misalnya, Anda dapat menjalankan COPY perintah dalam database Amazon Redshift untuk mengambil data dari Amazon S3 dan mengisi tabel Redshift.

Anda dapat mengaitkan beberapa peran ke namespace menggunakan konsol, seperti yang dijelaskan sebelumnya di bagian ini. Anda juga dapat menggunakan perintah `API createNamespace`, atau perintah CLI `create-namespace`. Dengan perintah API atau CLI, Anda dapat menetapkan peran IAM ke namespace dengan mengisi `IAMRoles` satu atau beberapa peran. Secara khusus, Anda menambahkan ARN untuk peran tertentu ke koleksi.

Mengelola namespace terkait peran IAM

Di bagian AWS Management Console Anda dapat mengelola kebijakan izin untuk peran. AWS Identity and Access Management Anda dapat mengelola peran IAM untuk namespace, menggunakan pengaturan yang tersedia di bawah konfigurasi Namespace. Untuk informasi selengkapnya tentang ruang nama dan penggunaannya di Amazon Redshift Tanpa Server, lihat [Ikhtisar grup kerja dan ruang nama Amazon Redshift Tanpa Server](#)

Memulai dengan kredensi IAM untuk Amazon Redshift

Saat Anda masuk ke konsol Amazon Redshift untuk pertama kalinya dan pertama kali mencoba Amazon Redshift Tanpa Server, kami sarankan Anda masuk sebagai pengguna dengan peran IAM

terlampir yang memiliki kebijakan yang diperlukan. Setelah Anda mulai membuat instance Amazon Redshift Tanpa Server, Amazon Redshift merekam nama peran IAM yang Anda gunakan untuk masuk. Anda dapat menggunakan kredensial yang sama untuk masuk ke konsol Amazon Redshift dan konsol Amazon Redshift Tanpa Server.

Saat membuat instance Amazon Redshift Tanpa Server, Anda dapat membuat database. Gunakan editor kueri v2 untuk terhubung ke database dengan opsi kredensial sementara.

Untuk menambahkan nama pengguna admin baru dan kata sandi yang tetap ada untuk database, pilih Sesuaikan kredensial pengguna admin dan masukkan nama pengguna admin baru dan kata sandi pengguna admin.

Untuk mulai menggunakan Amazon Redshift Serverless dan membuat workgroup dan namespace di konsol untuk pertama kalinya, gunakan peran IAM dengan kebijakan izin yang dilampirkan. Pastikan bahwa peran ini memiliki izin administrator `arn:aws:iam::aws:policy/AdministratorAccess` atau izin Amazon Redshift lengkap yang `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess` dilampirkan pada kebijakan IAM.

Skenario berikut menguraikan bagaimana kredensial IAM Anda digunakan oleh Amazon Redshift Tanpa Server saat Anda memulai konsol Amazon Redshift Tanpa Server:

- Jika Anda memilih Gunakan pengaturan default — Amazon Redshift Serverless menerjemahkan identitas IAM Anda saat ini ke superuser database. Anda dapat menggunakan identitas IAM yang sama dengan konsol Amazon Redshift Tanpa Server untuk melakukan tindakan pengguna super di database Anda di Amazon Redshift Serverless.
- Jika Anda memilih Sesuaikan setelan tanpa menentukan nama pengguna Admin dan kata sandi Amazon Redshift Tanpa Server, kredensial IAM Anda saat ini akan digunakan sebagai kredensial pengguna admin default Anda.
- Jika Anda memilih Sesuaikan setelan dan tentukan nama pengguna dan kata sandi Admin Amazon Redshift Tanpa Server — Amazon Redshift Tanpa Server menerjemahkan identitas IAM Anda saat ini ke superuser database. Amazon Redshift Serverless juga membuat nama pengguna login jangka panjang dan pasangan kata sandi juga sebagai pengguna super. Anda dapat menggunakan identitas IAM Anda saat ini atau pasangan nama pengguna dan kata sandi yang dibuat untuk masuk ke database Anda sebagai pengguna super.

Mengelola akses ke objek database Amazon Redshift Tanpa Server dengan izin peran basis data

Prosedur ini menunjukkan cara memberikan izin untuk menanyakan tabel melalui peran [database Amazon Redshift](#). Peran ditetapkan melalui tag yang dilampirkan ke pengguna di IAM dan diteruskan ke Amazon Redshift saat mereka masuk. Ini adalah penjelasan dengan contoh konsep dalam [Mendefinisikan peran database untuk diberikan kepada pengguna federasi di Amazon Redshift Tanpa Server](#). Manfaat menyelesaikan langkah-langkah ini adalah Anda dapat mengaitkan pengguna dengan peran database dan menghindari pengaturan izin mereka untuk setiap objek database. Ini menyederhanakan mengelola kemampuan pengguna untuk query, memodifikasi, atau menambahkan data ke tabel dan untuk melakukan tindakan lain.

Prosedur ini mengasumsikan Anda telah menyiapkan database Amazon Redshift Tanpa Server dan Anda memiliki kemampuan untuk memberikan izin dalam database. Ini juga mengasumsikan Anda memiliki izin untuk membuat pengguna IAM di AWS konsol, untuk membuat peran IAM, dan menetapkan izin kebijakan.

1. Buat pengguna IAM, menggunakan konsol IAM. Nanti, Anda akan terhubung ke database dengan pengguna ini.
2. Buat peran database Redshift, menggunakan editor kueri v2 atau klien SQL lainnya. Untuk informasi selengkapnya tentang membuat peran database, lihat [MEMBUAT PERAN](#).

```
CREATE ROLE urban_planning;
```

Kueri tampilan sistem [SVV_ROLES](#) untuk memeriksa apakah peran Anda dibuat. Ini juga mengembalikan peran sistem.

```
SELECT * from SVV_ROLES;
```

3. Berikan peran database yang Anda buat izin untuk memilih dari tabel. (Pengguna IAM yang Anda buat pada akhirnya akan masuk dan memilih catatan dari tabel melalui peran database.) Nama peran dan nama tabel dalam contoh kode berikut adalah sampel. Di sini, izin diberikan untuk memilih dari tabel bernama `cities`.

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

4. Gunakan AWS Identity and Access Management konsol untuk membuat peran IAM. Peran ini memberikan izin untuk menggunakan editor kueri v2. Buat peran IAM baru dan, untuk jenis entitas tepercaya, pilih AWS akun. Kemudian pilih Akun ini. Berikan peran izin kebijakan berikut:
 - `AmazonRedshiftReadOnlyAccess`
 - `tag:GetResources`
 - `tag:GetTagKeys`
 - Semua tindakan untuk `sqlworkbench`, termasuk `sqlworkbench:ListDatabases` dan `sqlworkbench:UpdateConnection`
5. Di konsol IAM, tambahkan tag dengan Kunci `RedshiftDbRoles` ke pengguna IAM yang Anda buat sebelumnya. Nilai tag harus sesuai dengan peran database yang Anda buat pada langkah pertama. Itu ada `urban_planning` di sampel.

Setelah Anda menyelesaikan langkah-langkah ini, tetapkan peran IAM ke pengguna yang Anda buat di konsol IAM. Saat pengguna masuk ke database dengan editor kueri v2, nama peran database mereka di tag diteruskan ke Amazon Redshift dan dikaitkan dengannya. Dengan demikian, mereka dapat menanyakan tabel yang sesuai dengan peran database. Untuk mengilustrasikan, pengguna dalam sampel ini dapat melakukan query `cities` tabel melalui peran `urban_planning` database.

Memigrasi kluster yang disediakan ke Amazon Redshift Tanpa Server

Untuk bermigrasi dari kluster yang disediakan ke Amazon Redshift Tanpa Server, lihat langkah-langkah berikut.

Membuat snapshot dari kluster yang Anda sediakan

Untuk mentransfer data dari cluster yang disediakan ke Amazon Redshift Serverless, buat snapshot kluster yang disediakan, lalu pulihkan snapshot di Amazon Redshift Serverless. Amazon Redshift secara otomatis mengonversi kunci interleaved menjadi kunci majemuk saat Anda memulihkan snapshot kluster yang disediakan ke namespace tanpa server.

Note

Sebelum memigrasikan data ke grup kerja tanpa server, pastikan kebutuhan kluster yang disediakan kompatibel dengan jumlah RPU yang Anda pilih di Amazon Redshift Tanpa Server.

Untuk membuat snapshot dari kluster yang telah disediakan

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Clusters, Snapshots, dan kemudian pilih Create snapshot.
3. Masukkan properti definisi snapshot, lalu pilih Buat snapshot. Mungkin perlu beberapa waktu agar snapshot tersedia.

Untuk memulihkan snapshot kluster yang disediakan ke namespace tanpa server:

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Mulai di konsol cluster yang disediakan Amazon Redshift dan navigasikan ke halaman Cluster, Snapshots.
3. Pilih snapshot untuk digunakan.
4. Pilih Pulihkan snapshot, Pulihkan ke namespace tanpa server.
5. Pilih namespace untuk mengembalikan snapshot Anda.
6. Konfirmasikan bahwa Anda ingin memulihkan dari snapshot Anda. Tindakan ini menggantikan semua database di titik akhir tanpa server Anda dengan data dari kluster yang disediakan. Pilih Pulihkan.

[Untuk informasi selengkapnya tentang snapshot kluster yang disediakan, lihat snapshot Amazon Redshift.](#)

Menghubungkan ke Amazon Redshift Tanpa Server menggunakan driver

Untuk terhubung ke Amazon Redshift Tanpa Server dengan klien SQL pilihan Anda, Anda dapat menggunakan driver driver JDBC versi 2 yang disediakan Amazon Redshift. Kami merekomendasikan menghubungkan menggunakan driver JDBC versi 2.1.x atau yang lebih baru.

Nomor port adalah opsional. Jika Anda tidak menyertakannya, Amazon Redshift Serverless default ke nomor port 5439. Anda dapat mengubah ke port lain dari rentang port 5431-5455 atau 8191-8215. Untuk mengubah port default untuk titik akhir tanpa server, gunakan API Amazon AWS CLI Redshift dan Amazon.

Untuk menemukan titik akhir yang tepat untuk digunakan untuk driver JDBC, ODBC, atau Python, lihat Konfigurasi Workgroup di Amazon Redshift Serverless. Anda juga dapat menggunakan operasi Amazon Redshift Serverless API `GetWorkgroup` atau AWS CLI operasi `get-workgroups` untuk mengembalikan informasi tentang workgroup Anda, lalu menyambung.

Menghubungkan menggunakan otentikasi berbasis kata sandi

Untuk terhubung menggunakan otentikasi berbasis kata sandi, gunakan sintaks berikut.

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

Untuk terhubung menggunakan driver Amazon Redshift Python, gunakan sintaks berikut.

```
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
```

Menghubungkan menggunakan IAM

Jika Anda lebih suka masuk dengan IAM, gunakan endpoint driver berikut. Endpoint driver ini memungkinkan Anda terhubung ke database tertentu dan menggunakan operasi API Tanpa [GetCredentials](#) Server Amazon Redshift.

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

Titik akhir driver ini tidak mendukung penyesuaian `dbUser`, `dbGroup` dan `auto-create`. Secara default, driver secara otomatis membuat pengguna database saat login dan menetapkannya ke grup

sesuai dengan grup yang Anda tentukan di IAM. Catatan: Nama grup yang Anda tentukan dalam IAM harus berisi hanya huruf kecil, angka, garis bawah ('_'), tanda plus ('+'), titik (titik), pada simbol (@), atau tanda hubung ('-'). Jika tidak, pengemudi mungkin tidak terhubung ke dbGroup.

Pastikan AWS identitas Anda memiliki kebijakan IAM yang benar untuk RedshiftServerlessGetCredentials tindakan tersebut. Berikut ini adalah contoh kebijakan IAM yang memberikan izin yang benar ke AWS identitas untuk terhubung ke Amazon Redshift Tanpa Server. Untuk informasi selengkapnya tentang izin IAM, lihat [Menambahkan Izin Identitas IAM](#).

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

Menghubungkan menggunakan IAM dengan DbUser dan dbGroups

Jika Anda ingin menggunakan opsi koneksi DBuser dan dbGroups kustom, gunakan endpoint driver berikut. Seperti endpoint driver Amazon Redshift Serverless lainnya, sintaks ini secara otomatis membuat pengguna database saat login. Endpoint driver ini menggunakan operasi API [GetCredentials](#) Tanpa Server Amazon Redshift. dbUser harus dimulai dengan huruf, harus berisi hanya karakter alfanumerik, garis bawah ('_'), tanda plus ('+'), titik ('.'), at ('@'), atau tanda hubung ('-'), dan harus kurang dari 128 karakter. dbGroups harus berisi hanya huruf kecil, angka, garis bawah ('_'), tanda plus ('+'), titik (titik), pada simbol (@), atau tanda hubung.

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

Untuk terhubung menggunakan driver Amazon Redshift Python, gunakan sintaks berikut.

```
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
```

Menghubungkan menggunakan ODBC

Untuk terhubung menggunakan ODBC, gunakan sintaks berikut.

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

Menggunakan Amazon Redshift Serverless SDK

Jika Anda menulis skrip manajemen apa pun menggunakan Amazon Redshift SDK, Anda harus menggunakan Amazon Redshift Serverless SDK baru untuk mengelola Amazon Redshift Tanpa Server dan sumber daya terkait. Untuk informasi selengkapnya tentang operasi API yang tersedia, lihat panduan Referensi API [Tanpa Server Amazon Redshift](#).

Ikhtisar grup kerja dan ruang nama Amazon Redshift Tanpa Server

Untuk mengisolasi beban kerja dan mengelola sumber daya yang berbeda di Amazon Redshift Tanpa Server, Anda dapat membuat ruang nama dan grup kerja serta mengelola penyimpanan dan menghitung sumber daya secara terpisah.

Ikhtisar grup kerja dan ruang nama Amazon Redshift Tanpa Server

Namespace adalah kumpulan objek database dan pengguna. Namespace terkait penyimpanan mengelompokkan skema, tabel, pengguna, atau AWS Key Management Service kunci untuk mengenkripsi data. Properti penyimpanan termasuk nama database dan kata sandi pengguna admin, izin, dan enkripsi dan keamanan. Sumber daya lain yang dikelompokkan di bawah ruang nama termasuk datashares, titik pemulihan, dan batas penggunaan. Anda dapat mengonfigurasi properti penyimpanan ini menggunakan konsol Amazon Redshift Serverless, the AWS Command Line Interface, atau Amazon Redshift Serverless API untuk sumber daya tertentu.

Workgroup adalah kumpulan sumber daya komputasi. Kelompok kerja terkait komputasi bersama-sama menghitung sumber daya seperti RPU, grup subnet VPC, dan grup keamanan. Properti untuk workgroup termasuk pengaturan jaringan dan keamanan. Sumber daya lain yang dikelompokkan

dalam kelompok kerja termasuk batas akses dan penggunaan. Anda dapat mengonfigurasi properti komputasi ini menggunakan konsol Amazon Redshift Serverless, AWS Command Line Interface the, atau Amazon Redshift Serverless API.

Anda dapat membuat satu atau lebih namespace dan workgroup. Setiap namespace hanya dapat memiliki satu workgroup yang terkait dengannya. Sebaliknya, setiap workgroup dapat dikaitkan dengan hanya satu namespace.

Memulai Amazon Redshift Serverless menggunakan konsol

Menyiapkan Amazon Redshift Serverless melibatkan berjalan melalui beberapa langkah konfigurasi. Bila Anda mengikuti langkah-langkah untuk mengatur Amazon Redshift Serverless, Anda membuat namespace dan workgroup, dan mengaitkannya satu sama lain. Untuk mulai menyetel konfigurasi Amazon Redshift Serverless menggunakan konsol Amazon Redshift Serverless, Anda dapat memilih Memulai Amazon Redshift Serverless untuk mengatur Amazon Redshift Serverless dan mulai berinteraksi dengannya. Anda dapat memilih lingkungan dengan pengaturan default, yang membuat penyiapan lebih cepat, atau secara eksplisit mengonfigurasi setelan sesuai kebutuhan organisasi Anda. Selama proses ini, Anda menentukan pengaturan untuk workgroup dan namespace Anda.

Setelah Anda mengatur lingkungan, [Properti Workgroup](#) dan [Properti namespace](#) membantu Anda membiasakan diri dengan pengaturan.

Mengelola grup kerja dan ruang nama menggunakan API Tanpa Server Amazon AWS Command Line Interface Redshift dan Amazon

Selain menggunakan AWS konsol, Anda juga dapat menggunakan API Tanpa Server Amazon Redshift AWS CLI atau Amazon Redshift untuk berinteraksi dengan grup kerja dan ruang nama. Tabel di bawah ini mencantumkan operasi API dan CLI yang dapat Anda gunakan untuk mengelola snapshot dan titik pemulihan.

Operasi API	Perintah CLI	Deskripsi
CreateNamespace	buat-namespace	Membuat namespace. Secara default, Amazon Redshift Serverless membuat ruang nama dengan AWS Key Management Service kunci default, tetapi Anda

Operasi API	Perintah CLI	Deskripsi
		dapat menentukan kunci lain untuk mengenkripsi data Anda. Anda juga dapat membuat namespace dengan memulihkan snapshot. Lihat Bekerja dengan snapshot dan titik pemulihan untuk informasi selengkapnya.
UpdateNamespace	perbaruan-namespace	Memperbarui namespace.
GetNamespace	dapatkan-namespace	Mengambil informasi tentang namespace
ListNamepaces	daftar-ruang nama	Mengambil informasi tentang daftar namespace.
DeleteNamespace	hapus-namespace	Menghapus namespace.
CreateWorkgroup	buat-workgroup	Membuat workgroup. Saat membuat workgroup, pastikan Anda memiliki namespace yang sudah ada yang dapat Anda kaitkan dengan workgroup. Saat membuat workgroup, Anda dapat menentukan sumber daya komputasi seperti subnet, grup keamanan, dan RPU.
UpdateWorkgroup	update-workgroup	Memperbarui grup kerja.
GetWorkgroup	dapatkan-kelompok kerja	Mengambil informasi tentang workgroup.
ListWorkgroups	daftar-kelompok kerja	Mengambil informasi tentang daftar kelompok kerja.

Operasi API	Perintah CLI	Deskripsi
DeleteWorkgroup	hapus-workgroup	Menghapus workgroup.

Mengelola Amazon Redshift Tanpa Server menggunakan konsol

Untuk membuat, mengedit, dan menghapus gudang data Amazon Redshift Tanpa Server, gunakan dasbor Tanpa Server di konsol Amazon Redshift. Akses ke pengaturan konsol individual bergantung pada peran IAM dan izin Anda.

Untuk informasi tentang cara menyiapkan Amazon Redshift Tanpa Server, lihat Menyiapkan [Amazon Redshift Tanpa Server untuk pertama kalinya](#). Untuk informasi tentang membuat dan mengonfigurasi grup kerja, lihat [Bekerja dengan kelompok kerja](#) Untuk informasi tentang mengonfigurasi ruang nama, lihat [Bekerja dengan ruang nama](#)

Menyiapkan Amazon Redshift Tanpa Server untuk pertama kalinya

Pertama kali Anda memilih dasbor Tanpa Server, itu memandu Anda melalui langkah-langkah untuk mengatur Amazon Redshift Tanpa Server. Di bawah Memulai pengalaman tanpa server, Anda dapat mengatur gudang data Amazon Redshift Tanpa Server, menggunakan kumpulan data sampel. Amazon Redshift Serverless secara otomatis memuat kumpulan data sampel selama proses pembuatan. Setelah gudang data dibuat, Anda dapat segera melakukan kueri data. [Untuk informasi selengkapnya tentang cara mengatur Amazon Redshift Serverless untuk pertama kalinya, lihat Redshift Tanpa Server.](#)

Bekerja dengan kelompok kerja

Untuk mengisolasi beban kerja dan mengelola sumber daya di Amazon Redshift Tanpa Server, Anda dapat membuat grup kerja dan ruang nama. Kelompok kerja terkait komputasi bersama-sama menghitung sumber daya seperti RPU dan grup subnet VPC. Jika Anda belum membuat workgroup dan namespace, dan Anda sedang mencari petunjuk yang menunjukkan cara memulai Amazon Redshift Serverless, lihat Menyiapkan Amazon Redshift Serverless untuk pertama [kalinya](#).

Membuat workgroup dengan namespace

Langkah-langkah ini mengasumsikan Anda telah menyelesaikan konfigurasi awal untuk Amazon Redshift Serverless. Jika Anda belum membuat workgroup dan namespace, dan Anda sedang

mencari petunjuk yang menunjukkan cara memulai Amazon Redshift Serverless, lihat [Menyiapkan Amazon Redshift Serverless untuk pertama kalinya](#).

Selesaikan langkah-langkah berikut untuk membuat workgroup:

1. Pilih dasbor Tanpa Server. Kemudian pilih Buat workgroup.
2. Masukkan nama workgroup.
3. Pilih Virtual Private Cloud (VPC) untuk Amazon Redshift Tanpa Server. Ini menetapkan workgroup ke jaringan virtual tertentu di lingkungan Anda AWS . Untuk informasi selengkapnya tentang VPC, lihat [Ikhtisar VPC dan subnet](#).
4. Pilih satu atau beberapa grup keamanan VPC. Untuk informasi selengkapnya, lihat [Mengontrol lalu lintas ke sumber daya menggunakan grup keamanan](#).
5. Di bawah Subnet, tentukan satu atau beberapa subnet untuk dikaitkan dengan database Anda. Subnet ini terdapat dalam VPC yang Anda pilih sebelumnya dan harus berada di tiga Availability Zone yang berbeda. Untuk informasi selengkapnya, lihat [Pertimbangan saat menggunakan Amazon Redshift Tanpa Server](#).
6. Pilih kapasitas RPU dasar yang sesuai dengan kebutuhan Anda.

Pilih namespace

1. Pilih salah satu Buat namespace baru, dan masukkan nama namespace, atau Tambahkan ke namespace yang ada, dan pilih namespace dari daftar drop-down.
2. Untuk nama dan kata sandi Database, tentukan nama database pertama. Anda juga dapat menentukan admin selain admin konsol default Anda, dengan mengedit kredensi pengguna Admin.
3. Untuk Izin, Anda memilih peran IAM Associate untuk mengaitkan peran IAM tertentu dengan namespace dan workgroup Anda. Untuk informasi selengkapnya tentang mengaitkan peran IAM dengan Amazon Redshift, [lihat Identitas dan manajemen akses di Amazon Redshift](#).
4. Anda dapat menyesuaikan pengaturan enkripsi Anda dengan membuat kunci baru atau memilih kunci selain default. Untuk pencatatan Audit, pilih log yang akan diekspor. Setiap jenis log menentukan metadata yang berbeda. Pilih Lanjutkan untuk meninjau pilihan Anda.

Tinjau pilihan workgroup

1. Tinjau pengaturan Anda di bawah Tinjau dan buat. Ini menunjukkan pengaturan yang Anda pilih di langkah sebelumnya.

2. Pilih Simpan.

Setelah Anda membuat workgroup, itu ditambahkan ke daftar Workgroups.

Membuat workgroup pratinjau

Untuk menguji fitur Amazon Redshift Serverless baru, buat workgroup Amazon Redshift Tanpa Server di Pratinjau. Anda tidak dapat menggunakan fitur tersebut dalam produksi atau memindahkan workgroup Preview ke workgroup produksi. Untuk syarat dan ketentuan pratinjau, lihat Beta dan Pratinjau di [Ketentuan AWS Layanan](#).

Fitur-fitur berikut saat ini tersedia di workgroup pratinjau:

- [Bekerja dengan integrasi nol-ETL](#)

Untuk membuat workgroup di Preview

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Dasbor Tanpa Server, dan pilih Konfigurasi Workgroup. Kelompok kerja untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap workgroup ditampilkan dalam kolom dalam daftar.
3. Spanduk di halaman konfigurasi Workgroup memperkenalkan workgroup pratinjau. Pilih tombolnya Buat workgroup pratinjau untuk membuka halaman buat workgroup.
4. Masukkan properti untuk grup kerja Anda. Kami merekomendasikan memasukkan nama untuk workgroup yang menunjukkan bahwa itu dalam pratinjau. Pilih opsi untuk grup kerja Anda, termasuk opsi berlabel -preview, untuk fitur yang ingin Anda uji. Lanjutkan melalui halaman untuk memasukkan opsi untuk workgroup dan namespace Anda. Untuk informasi umum tentang membuat grup kerja, lihat [the section called “Membuat workgroup dengan namespace”](#).
5. Pilih Buat untuk membuat grup kerja di pratinjau.
6. Bila workgroup pratinjau Anda tersedia, gunakan klien SQL Anda untuk memuat dan menanyakan data.

Untuk informasi tentang pratinjau di kluster yang disediakan, lihat [Membuat kluster pratinjau](#)

Melihat properti untuk grup kerja

Di Amazon Redshift Tanpa Server, workgroup adalah kumpulan sumber daya yang tersedia untuk digunakan. Saat memilih Amazon Redshift Tanpa Server, di AWS konsol, Anda dapat memilih konfigurasi Workgroup dari menu navigasi untuk melihat daftar. Anda dapat menggunakan kotak Pencarian untuk menemukan grup kerja yang memenuhi kriteria penelusuran Anda. Setiap entri workgroup memiliki beberapa properti yang ditampilkan:

- Workgroup - Nama workgroup. Anda dapat memilihnya untuk melihat dan mengedit properti workgroup.
- Status - Menunjukkan apakah workgroup tersedia.
- Namespace - Namespace yang terkait dengan workgroup. Setiap workgroup dikaitkan dengan satu namespace.
- Tanggal pembuatan - Tanggal workgroup dibuat.
- Tag - Tag yang terkait dengan workgroup.

Properti Workgroup

Anda dapat membuat daftar kelompok kerja dengan memilih konfigurasi Workgroup di menu sebelah kiri. Kemudian Anda dapat memilih workgroup dari daftar. Beberapa panel menunjukkan properti untuk workgroup. Anda juga dapat melakukan tindakan. Informasi umum menampilkan yang berikut:

- Workgroup - Nama workgroup.
- Namespace - Namespace yang terkait dengan workgroup. Anda dapat memilihnya untuk melihat propertinya. Workgroup dikaitkan dengan satu namespace.
- Tanggal dibuat - Saat workgroup dibuat.
- Status - Menunjukkan jika sumber daya workgroup tersedia. Jika tersedia, Anda dapat terhubung dengan klien ke instans Amazon Redshift Tanpa Server, untuk menanyakan data atau membuat sumber daya basis data, atau Anda dapat terhubung dengan editor kueri v2.
- Endpoint - URL.
- URL JDBC - URL untuk membangun koneksi klien JDBC. Anda dapat menggunakan URL ini untuk terhubung dengan driver JDBC untuk Amazon Redshift. Untuk informasi selengkapnya, lihat [Mengonfigurasi sambungan untuk driver JDBC versi 2.1 untuk Amazon Redshift](#).
- URL ODBC - URL untuk membuat koneksi klien ODBC. Ini berisi properti, seperti database dan ID pengguna, dan nilai-nilai mereka.

- Versi Workgroup dan versi Patch - Amazon Redshift Serverless secara teratur merilis versi dan tambalan baru. Anda dapat menggunakan versi workgroup dan nomor versi Patch untuk melacak pembaruan perangkat lunak ke grup kerja Amazon Redshift Serverless Anda. Untuk informasi selengkapnya tentang perubahan dan fitur di tambalan tertentu, lihat [Versi kluster untuk Amazon Redshift](#).

Tab Akses data berisi beberapa panel:

- Jaringan dan keamanan - Anda dapat melihat properti jaringan, seperti pengidentifikasi Virtual Private Cloud (VPC), daftar grup keamanan VPC, Perutean VPC yang Ditingkatkan, dan pengaturan yang dapat diakses publik. Jika Anda memilih Edit, Anda dapat mengubah pengaturan ini. Selain itu, Anda dapat memilih Aktifkan perutean VPC yang disempurnakan, yang merutekan lalu lintas jaringan antara database tanpa server dan repositori data Anda melalui VPC, untuk meningkatkan privasi dan keamanan. Anda juga dapat memilih Aktifkan Akses Publik, yang membuat database dapat diakses publik dari luar VPC, memungkinkan instance dan perangkat untuk terhubung.
- Titik akhir VPC terkelola Redshift - Anda dapat membuat titik akhir VPC terkelola untuk mengakses Amazon Redshift Tanpa Server dari VPC lain.

Tab Limits memiliki pengaturan untuk mengontrol kapasitas dan batas penggunaan untuk Amazon Redshift Serverless. Ini berisi panel berikut:

- Kapasitas dasar dalam unit pemrosesan Redshift (RPU) - Anda dapat mengatur kapasitas dasar sumber daya komputasi yang digunakan untuk memproses beban kerja Anda. Untuk informasi selengkapnya, lihat [Memahami kapasitas Amazon Redshift Tanpa Server](#).
- Batas penggunaan - Anda dapat mengatur hingga empat batas untuk sumber daya komputasi maksimum yang dapat digunakan instans Amazon Redshift Tanpa Server dalam jangka waktu tertentu, dan memilih tindakan untuk Amazon Redshift Tanpa Server untuk dilakukan saat mencapai batas tersebut. Misalnya, Anda dapat mengatur workgroup Anda untuk memiliki dua batas, satu dari 500 jam RPU dan satu dari 900 jam RPU. Anda dapat meminta Amazon Redshift Serverless mengirimkan Anda peringatan ketika mencapai batas pertama 500 jam RPU, lalu matikan kueri pengguna ketika mencapai batas kedua 900 jam. Batasan ini membantu mengendalikan biaya Anda dan membuatnya lebih dapat diprediksi.
- Batas kueri - Anda dapat menetapkan batas pada kueri, seperti pengaturan batas waktu. Batasan ini membantu Anda mengoptimalkan biaya dan kinerja.

Tab Tab memiliki panel Tag, yang menampilkan tag apa pun yang Anda buat untuk workgroup Anda. Untuk informasi selengkapnya tentang menandai sumber daya, lihat [Memberi tag pada sumber daya](#).

Menghapus workgroup

Anda dapat menghapus workgroup menggunakan konsol. Sebelum Anda melakukan ini, pastikan bahwa Anda memiliki data Anda dicadangkan dan snapshot di tempat. Sumber daya yang dihapus sebagai bagian dari grup kerja dalam banyak kasus tidak dapat diambil.

Selesaikan langkah-langkah berikut:

1. Pilih Amazon Redshift Tanpa Server, pilih konfigurasi Workgroup dan pilih Hapus instans Amazon Redshift Tanpa Server.
2. Dialog terbuka. Saat Anda memilih untuk menghapus grup kerja, semua batas penggunaan dihapus, semua titik akhir VPC dihapus, dan akses ke titik akhir VPC dihapus.

Ketik hapus dan pilih Hapus untuk mengonfirmasi.

Setelah Anda menyelesaikan langkah-langkahnya, status workgroup adalah Menghapus dan spanduk menunjukkan bahwa workgroup sedang dihapus. Saat proses penghapusan sedang berlangsung, beberapa fitur di bawah dasbor Tanpa Server dinonaktifkan. Tetapi Anda dapat mengonfigurasi cluster yang disediakan di dasbor kluster yang disediakan.

Setelah Anda menghapus workgroup, itu tidak muncul dengan namespace. Anda dapat memilih tombol Create workgroup untuk membuat yang baru.

Anda dapat menghapus workgroup yang ada dan mengaitkan workgroup baru dengan konfigurasi yang berbeda ke namespace yang sama. Saat membuat workgroup baru, pilih kapasitas dasar yang sesuai dengan ukuran data yang terkait dengan namespace.

Anda dapat mengaitkan workgroup dengan namespace yang dibuat dengan kunci yang dikelola pelanggan (CMK). Untuk informasi lebih lanjut tentang AWS KMS, lihat [AWS KMS konsep](#).

Bekerja dengan ruang nama

Di Amazon Redshift Tanpa Server, namespace mendefinisikan wadah logis untuk objek database. Ini dapat menampung tabel, kelompok kerja, dan sumber daya database lainnya. Jika Anda belum membuat workgroup dan namespace, dan Anda sedang mencari petunjuk tentang cara memulai Amazon Redshift Serverless, lihat [Menyiapkan Amazon Redshift Serverless untuk pertama kalinya](#).

Mencari namespace

Dari menu Amazon Redshift, Anda dapat memilih dari daftar Namespaces untuk melihat atau mengedit properti untuk namespace. Informasi di konsol mencakup nama namespace, nama admin, dan properti lainnya.

Pengaturan dan properti namespace ada di beberapa tab. Sumber daya yang dimaksud meliputi:

- Workgroup - Menunjukkan workgroup yang terkait dengan namespace.
- Data back up - Anda dapat mengkonfigurasi dan membuat snapshot, dan mengkonfigurasi titik pemulihan.
- Keamanan dan enkripsi - Anda dapat mengelola izin peran IAM dan melihat atau mengedit pengaturan keamanan dan enkripsi Anda. Ini termasuk status kunci enkripsi Anda dan pengaturan pencatatan audit Anda.
- Datashares - Menunjukkan datashares.

Properti namespace

Di Amazon Redshift Tanpa Server, namespace mendefinisikan wadah untuk objek database. Anda dapat memilih konfigurasi Namespace dari daftar navigasi, memilih namespace dari daftar, dan mengedit pengaturannya.

Informasi umum untuk namespace meliputi:

- Namespace - Nama.
- Namespace ID - Pengidentifikasi unik.
- ARN - Sebuah identifier unik yang digunakan untuk menentukan sumber daya di seluruh AWS. Ini berisi properti seperti wilayah dan layanan.
- Status - Status, seperti Tersedia.
- Tanggal dibuat - Tanggal namespace dibuat.
- Penyimpanan yang digunakan - Ruang penyimpanan yang digunakan oleh namespace dan semua objeknya.
- Nama pengguna admin - Akun admin. Ini biasanya akun yang digunakan untuk membuat namespace.
- Nama database - Nama database yang terkandung oleh namespace.

- Jumlah tabel total - Hitungan tabel di semua skema.

Pengaturan dan properti tambahan untuk namespace ada di beberapa tab. Sumber daya yang dimaksud meliputi:

- Workgroup - Menunjukkan workgroup yang terkait dengan namespace.
- Data back up - Pada panel ini, Anda dapat mengkonfigurasi dan membuat snapshot, dan mengkonfigurasi titik pemulihan.
- Keamanan dan enkripsi - Anda dapat mengelola izin peran IAM dan melihat atau mengedit pengaturan keamanan dan enkripsi Anda. Ini termasuk status kunci enkripsi Anda, dan pengaturan untuk mengaktifkan pencatatan audit. Untuk informasi selengkapnya tentang pencatatan audit untuk Amazon Redshift Tanpa Server, lihat Pencatatan [audit untuk Amazon Redshift](#) Tanpa Server.
- Datashares - Menunjukkan datashares. Dengan berbagi data, Anda dapat memberikan akses ke data tanpa perlu menyalin atau memindahkannya. Untuk informasi selengkapnya tentang berbagi data, lihat [Berbagi data di Amazon Redshift](#) Tanpa Server.

Mengedit keamanan dan enkripsi

Amazon Redshift Serverless diamankan dengan menggunakan enkripsi KMS. Anda dapat memperbarui pengaturan enkripsi melalui konsol:

1. Pilih konfigurasi Namespace dari menu utama di konsol, pilih namespace yang akan diedit, dan pilih Edit pada tab Keamanan dan enkripsi. Dialog muncul.
2. Anda dapat memilih Sesuaikan pengaturan enkripsi dan kemudian Pilih kunci yang dikelola AWS pelanggan untuk mengubah kunci yang digunakan untuk mengenkripsi sumber daya Anda.
3. Untuk pencatatan Audit, pilih log yang akan diekspor. Setiap jenis log menentukan metadata yang berbeda.
4. Untuk menyelesaikan pembaruan konfigurasi, pilih Simpan perubahan.

Mengubah AWS KMS kunci untuk namespace

Di Amazon Redshift, enkripsi melindungi data saat istirahat. Amazon Redshift Serverless menggunakan enkripsi AWS KMS kunci secara otomatis untuk mengenkripsi sumber daya dan snapshot Amazon Redshift Tanpa Server Anda. Sebagai praktik terbaik, sebagian besar organisasi meninjau jenis data yang mereka simpan dan memiliki rencana untuk memutar kunci enkripsi sesuai

jadwal. Frekuensi untuk memutar kunci dapat bervariasi, tergantung pada kebijakan Anda untuk keamanan data. Amazon Redshift Tanpa Server mendukung perubahan AWS KMS kunci untuk namespace sehingga Anda dapat mematuhi kebijakan keamanan organisasi Anda.

Ketika Anda mengubah AWS KMS kunci, data tetap tidak berubah.

Mengubah AWS KMS kunci menggunakan konsol

Di Amazon Redshift, enkripsi melindungi data saat istirahat. Amazon Redshift Serverless menggunakan enkripsi AWS KMS kunci secara otomatis untuk mengenkripsi Amazon Redshift Serverless dan snapshot. Sebagai praktik terbaik, sebagian besar organisasi meninjau jenis data yang mereka simpan dan memiliki rencana untuk memutar kunci enkripsi sesuai jadwal. Frekuensi untuk memutar kunci dapat bervariasi, tergantung pada kebijakan Anda untuk keamanan data. Amazon Redshift Tanpa Server mendukung perubahan AWS KMS kunci untuk namespace sehingga Anda dapat mematuhi kebijakan keamanan organisasi Anda.

Ketika Anda mengubah AWS KMS kunci, data tetap tidak berubah.

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih konfigurasi Namespace. Pilih namespace Anda dari daftar.
3. Dari tab Keamanan dan enkripsi, pilih Edit.
4. Pilih Sesuaikan pengaturan enkripsi dan kemudian pilih kunci untuk namespace. Anda dapat membuat kunci baru secara opsional.

Mengubah kunci AWS KMS enkripsi menggunakan AWS CLI

Gunakan `update-namespace` untuk mengubah AWS KMS kunci untuk namespace. Berikut ini menunjukkan sintaks untuk perintah:

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

Anda harus memiliki namespace yang dibuat atau perintah CLI menghasilkan kesalahan.

Waktu yang diperlukan untuk mengubah kunci tergantung pada jumlah data di Amazon Redshift Serverless. Ini biasanya memakan waktu lima belas menit per 8TB data yang disimpan.

Batasan

Anda tidak dapat mengubah dari KMS Key yang dikelola pelanggan menjadi AWS KMS kunci. Dalam hal ini, Anda harus membuat namespace baru.

Anda tidak dapat melakukan tindakan lain saat kuncinya sedang diubah.

Menghapus namespace

Jika Anda ingin menghapus namespace dengan workgroup terkait, Anda harus menghapus workgroup terlebih dahulu.

Di konsol Amazon Redshift Tanpa Server, selesaikan langkah-langkah berikut:

1. Pilih konfigurasi Namespace dari menu kiri dan kemudian pilih namespace yang ingin Anda hapus dari daftar.
2. Pilih Tindakan dan pilih Hapus namespace.
3. Kotak dialog terbuka. Anda dapat menyimpan data Anda dengan membuat snapshot manual sebelum menyelesaikan operasi penghapusan.

Ketik hapus dan pilih Hapus untuk mengonfirmasi.

Mengelola batas penggunaan, batas kueri, dan tugas administratif lainnya

Anda dapat mengonfigurasi pengaturan di konsol untuk mengontrol penggunaan dan membatasi biaya.

Mengelola batas penggunaan, termasuk menetapkan batas RPU

Di bawah tab Batas untuk grup kerja, Anda dapat menambahkan satu atau beberapa batas penggunaan untuk mengontrol RPU maksimum yang Anda gunakan dalam periode waktu tertentu, atau untuk menetapkan batas penggunaan berbagi data.

1. Pilih Kelola batas penggunaan. Bagian batas muncul di bagian bawah panel Compute use by period.
2. Tetapkan batas penggunaan dalam jumlah jam RPU.
3. Pilih Frekuensi, yaitu Harian, Mingguan, atau Bulanan. Ini menetapkan periode waktu untuk batas penggunaan. Memilih Harian dalam hal ini memberi Anda kontrol yang lebih rinci.

4. Tetapkan batas penggunaan, dalam jumlah jam.
5. Atur tindakan. Ini adalah sebagai berikut:
 - Masuk ke tabel sistem - Menambahkan catatan ke tampilan sistem [SYS_QUERY_HISTORY](#). Anda dapat menanyakan `usage_limit` kolom dalam tampilan ini untuk menentukan apakah kueri melebihi batas.
 - Peringatan - Menggunakan Amazon SNS untuk mengatur langganan notifikasi dan mengirim pemberitahuan jika batas dilanggar. Anda dapat memilih topik Amazon SNS yang ada atau membuat yang baru.
 - Matikan kueri pengguna - Menonaktifkan kueri untuk menghentikan penggunaan Amazon Redshift Tanpa Server. Ini juga mengirimkan pemberitahuan.

Dua tindakan pertama bersifat informasional, tetapi yang terakhir mematikan pemrosesan kueri.

6. Secara opsional, Anda dapat menetapkan batas penggunaan berbagi data Lintas Wilayah, yang membatasi jumlah data yang ditransfer dari Wilayah produsen ke Wilayah konsumen yang dapat ditanyakan konsumen. Untuk melakukan ini, pilih Tambahkan batas dan ikuti langkah-langkahnya.
7. Pilih Simpan perubahan di bagian bawah halaman untuk menyimpan batas.
8. Atur hingga 3 batas lagi seperlunya.

Untuk informasi konseptual selengkapnya tentang RPU dan penagihan, lihat [Penagihan Amazon Redshift](#) Tanpa Server.

Mengelola batas kueri

Di bawah tab Batas untuk grup kerja, Anda dapat menambahkan batas untuk memantau kinerja dan batas. Untuk informasi selengkapnya tentang batas pemantauan kueri, lihat aturan [pemantauan kueri WLM](#).

1. Pilih Kelola batas kueri. Pilih Tambahkan batas baru pada dialog Kelola batas kueri.
2. Pilih jenis batas yang ingin Anda tetapkan dan masukkan nilai untuk batas yang sesuai.
3. Pilih Simpan perubahan untuk menyimpan batas.

Ketika Anda mengubah batas kueri dan parameter konfigurasi, database Anda akan restart.

Memfilter kueri

Anda dapat menggunakan filter yang tersedia di dasbor tanpa server. Untuk memfilter kueri, lakukan langkah-langkah berikut.

1. Di sebelah kiri panel Ringkasan kueri, pilih daftar drop-down untuk memfilter berdasarkan kueri yang sudah selesai, kueri gagal, atau keduanya.
2. Di sebelah kanan panel ringkasan Kueri, pilih daftar drop-down untuk memfilter dengan menjalankan kueri, kueri antrian, atau keduanya.

Mengubah kata sandi admin

1. Pilih konfigurasi Namespace. Kemudian pilih Ubah kata sandi admin. Dialog muncul.
2. Anda dapat menentukan nama pengguna admin baru dan kata sandi pengguna admin baru.
3. Pilih Simpan.

Memeriksa data ringkasan Amazon Redshift Tanpa Server menggunakan dasbor

Dasbor Amazon Redshift Tanpa Server berisi kumpulan panel yang menampilkan at-a-glance metrik dan informasi tentang workgroup dan namespace Anda. Panel-panel ini meliputi:

- Ringkasan sumber daya - Menampilkan informasi tingkat tinggi tentang Amazon Redshift Tanpa Server, seperti penyimpanan yang digunakan dan metrik lainnya.
- Ringkasan kueri - Menampilkan informasi tentang kueri, termasuk kueri lengkap dan kueri yang sedang berjalan. Pilih Lihat detail untuk membuka layar yang memiliki filter tambahan.
- Kapasitas RPU yang digunakan - Menampilkan kapasitas keseluruhan yang digunakan selama periode waktu tertentu, seperti sepuluh jam sebelumnya, misalnya.
- Datashares - Menunjukkan jumlah datashares, yang digunakan untuk berbagi data antara, misalnya, akun. AWS Metrik menunjukkan datashares mana yang memerlukan otorisasi, dan informasi lainnya.
- Total penggunaan komputasi - Menunjukkan total jam RPU yang Anda konsumsi untuk grup kerja yang dipilih selama rentang waktu yang dipilih, hingga 7 hari terakhir.

Dari dasbor, Anda dapat dengan cepat menyelami metrik yang tersedia ini untuk memeriksa detail mengenai Amazon Redshift Tanpa Server, atau meninjau kueri, atau melacak item pekerjaan.

Memantau kueri dan beban kerja dengan Amazon Redshift Serverless

Memantau kueri dan beban kerja dengan Amazon Redshift Serverless

Anda dapat memantau kueri dan beban kerja Tanpa Server Amazon Redshift dengan tampilan sistem yang disediakan.

Memberikan akses untuk memonitor kueri

Superuser dapat memberikan akses ke pengguna yang bukan pengguna super sehingga mereka dapat melakukan pemantauan kueri untuk semua pengguna. Pertama, Anda menambahkan kebijakan untuk pengguna atau peran untuk menyediakan akses pemantauan kueri. Kemudian, Anda memberikan izin pemantauan kueri kepada pengguna atau peran.

Untuk menambahkan kebijakan pemantauan kueri

1. Pilih <https://console.aws.amazon.com/iam/>.
2. Di bagian Manajemen akses, pilih Kebijakan.
3. Pilih Buat Kebijakan.
4. Pilih JSON dan tempel definisi kebijakan berikut.

```
{
  "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. Pilih Tinjau kebijakan.
6. Untuk Nama, masukkan nama untuk kebijakan, seperti `query-monitoring`.
7. Pilih Buat kebijakan.

Setelah membuat kebijakan, Anda dapat memberikan izin yang sesuai.

Untuk memberikan akses, menambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

Buat rangkaian izin. Ikuti instruksi di [Buat rangkaian izin](#) di Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

Buat peran untuk federasi identitas. Ikuti instruksi dalam [Membuat peran untuk penyedia identitas pihak ketiga \(federasi\)](#) di Panduan Pengguna IAM.

- Pengguna IAM:

- Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam [Membuat peran untuk pengguna IAM](#) dalam Panduan Pengguna IAM.
- (Tidak disarankan) Pasang kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti instruksi dalam [Menambahkan izin ke pengguna \(konsol\)](#) dalam Panduan Pengguna IAM.

Untuk memberikan izin pemantauan kueri bagi pengguna

Pengguna dengan `sys:monitor` izin dapat melihat semua kueri. Selain itu, pengguna dengan `sys:operator` izin dapat membatalkan kueri, menganalisis riwayat kueri, dan melakukan operasi vakum.

1. Masukkan perintah berikut untuk menyediakan akses monitor sistem, di mana nama pengguna adalah nama pengguna yang ingin Anda berikan aksesnya.

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

2. (Opsional) Masukkan perintah berikut untuk menyediakan akses operator sistem, di mana nama pengguna adalah nama pengguna yang ingin Anda berikan aksesnya.

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

Untuk memberikan izin pemantauan kueri untuk peran

Pengguna dengan peran yang memiliki `sys:monitor` izin dapat melihat semua kueri. Selain itu, pengguna dengan peran yang memiliki `sys:operator` izin dapat membatalkan kueri, menganalisis riwayat kueri, dan melakukan operasi vakum.

1. Masukkan perintah berikut untuk menyediakan akses monitor sistem, di mana `role-name` adalah nama peran yang ingin Anda berikan aksesnya.

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

2. (Opsional) Masukkan perintah berikut untuk menyediakan akses operator sistem, di mana `role-name` adalah nama peran yang ingin Anda berikan aksesnya.

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

Pemantauan tampilan

Tampilan pemantauan adalah tampilan sistem di Amazon Redshift Tanpa Server yang digunakan untuk memantau penggunaan kueri dan beban kerja. Pandangan ini terletak di `pg_catalog` skema. Tampilan sistem yang tersedia telah dirancang untuk memberi Anda informasi yang diperlukan untuk memantau Amazon Redshift Tanpa Server, yang jauh lebih sederhana daripada yang diperlukan untuk cluster yang disediakan. Tampilan sistem SYS telah dirancang untuk bekerja dengan Amazon Redshift Serverless. Untuk menampilkan informasi yang disediakan oleh tampilan ini, jalankan pernyataan SQL `SELECT`.

Tampilan sistem didefinisikan untuk mendukung tujuan pemantauan berikut.

Pemantauan beban kerja

Anda dapat memantau aktivitas kueri Anda dari waktu ke waktu untuk:

- Memahami pola beban kerja, sehingga Anda tahu apa yang normal (baseline) dan apa yang ada dalam perjanjian tingkat layanan bisnis (SLA).

- Identifikasi penyimpangan dengan cepat dari normal, yang mungkin merupakan masalah sementara atau sesuatu yang menjamin tindakan lebih lanjut.

Pemantauan pemuatan dan bongkar data

Pergerakan data masuk dan keluar dari Amazon Redshift Serverless adalah fungsi penting. Anda menggunakan COPY dan UNLOAD untuk memuat atau membongkar data, dan Anda harus memantau kemajuan dengan cermat dalam hal byte/baris yang ditransfer dan file diselesaikan untuk melacak kepatuhan terhadap SLA bisnis. Hal ini biasanya dilakukan dengan menjalankan query tabel sistem sering (yaitu, setiap menit) untuk melacak kemajuan dan meningkatkan peringatan untuk penyelidikan/tindakan korektif jika penyimpangan signifikan terdeteksi.

Diagnostik kegagalan dan masalah

Ada kasus di mana Anda harus mengambil tindakan untuk kegagalan kueri atau runtime. Pengembang mengandalkan tabel sistem untuk mendiagnosis sendiri masalah dan menentukan solusi yang benar.

Penyempurnaan performa

Anda mungkin perlu menyetel kueri yang tidak memenuhi persyaratan SLA baik dari awal, atau telah menurun seiring waktu. Untuk menyetel, Anda harus memiliki detail runtime termasuk run plan, statistik, durasi, dan konsumsi sumber daya. Anda memerlukan data dasar untuk pertanyaan yang menyinggung untuk menentukan penyebab penyimpangan dan untuk memandu Anda cara meningkatkan kinerja.

Objek pengguna pemantauan acara

Anda perlu memantau tindakan dan aktivitas pada objek pengguna, seperti menyegarkan tampilan terwujud, menyedot debu, dan menganalisis. Ini termasuk peristiwa yang dikelola sistem seperti penyegaran otomatis untuk tampilan terwujud. Anda ingin memantau kapan suatu peristiwa berakhir jika itu dimulai pengguna, atau yang terakhir berhasil dijalankan jika sistem dimulai.

Pelacakan penggunaan untuk penagihan

Anda dapat memantau tren penggunaan Anda dari waktu ke waktu untuk:

- Menginformasikan perencanaan anggaran dan perkiraan ekspansi bisnis.
- Identifikasi peluang penghematan biaya potensial seperti menghapus data dingin.

Gunakan tampilan sistem SYS untuk memantau Amazon Redshift Tanpa Server;. Untuk informasi selengkapnya tentang tampilan pemantauan SYS, lihat tampilan [pemantauan SYS](#).

Pencatatan audit untuk Amazon Redshift Tanpa Server

Mengekspor log

Anda dapat mengonfigurasi Amazon Redshift Tanpa Server untuk mengekspor data log koneksi, pengguna, dan aktivitas pengguna ke grup log di Amazon Logs. CloudWatch Dengan Amazon CloudWatch Logs, Anda dapat melakukan analisis real-time dari data log dan menggunakannya CloudWatch untuk membuat alarm dan melihat metrik. Anda dapat menggunakan CloudWatch Log untuk menyimpan catatan log Anda dalam penyimpanan yang tahan lama.

Anda dapat membuat CloudWatch alarm untuk melacak metrik menggunakan konsol Amazon Redshift. Untuk informasi selengkapnya tentang membuat alarm, lihat [Mengelola alarm](#).

Untuk mengekspor data log yang dihasilkan ke Amazon CloudWatch Logs, masing-masing log harus dipilih untuk diekspor di setelan konfigurasi Amazon Redshift Tanpa Server, di konsol. Anda dapat melakukan ini dengan memilih pengaturan konfigurasi Namespace, di bawah Keamanan dan enkripsi.

Memantau peristiwa log di CloudWatch

Setelah memilih log Redshift mana yang akan diekspor, Anda dapat memantau peristiwa di Amazon CloudWatch Logs. Grup log baru secara otomatis dibuat untuk Amazon Redshift Serverless, yang `log_type` mewakili jenis log.

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

Saat Anda membuat workgroup dan namespace pertama Anda, default adalah nama namespace. Nama grup log bervariasi sesuai dengan apa yang Anda sebut namespace.

Misalnya, jika Anda mengekspor log koneksi, data log disimpan dalam grup log berikut.

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

Peristiwa log diekspor ke grup log menggunakan aliran log tanpa server. Perilaku tergantung pada kondisi berikut mana yang benar:

- Ada grup log dengan nama yang ditentukan. Redshift mengekspor data log menggunakan grup log yang ada. Untuk membuat grup log dengan periode penyimpanan log, filter metrik, dan akses pelanggan yang telah ditentukan sebelumnya, Anda dapat menggunakan konfigurasi otomatis, seperti yang disediakan oleh AWS CloudFormation

- Grup log dengan nama yang ditentukan tidak ada. Saat entri log yang cocok terdeteksi di log untuk instance, Amazon Redshift Serverless akan membuat grup log baru di Amazon Logs secara otomatis. CloudWatch Grup log menggunakan periode penyimpanan log default Never Exire. Untuk mengubah periode penyimpanan log, gunakan konsol Amazon CloudWatch Logs, API Amazon Logs AWS CLI, atau Amazon CloudWatch Logs. Untuk informasi selengkapnya tentang mengubah periode penyimpanan CloudWatch log di Log, lihat [Mengubah penyimpanan data log di Bekerja dengan grup log dan aliran log](#).

Untuk mencari informasi dalam peristiwa log, gunakan konsol Amazon CloudWatch Logs, API Amazon Logs AWS CLI, atau Amazon CloudWatch Logs. Untuk informasi selengkapnya tentang mencari dan memfilter data log, lihat [Menelusuri dan memfilter data log](#).

Metrik Tanpa Server Amazon Redshift

Amazon Redshift Metrik tanpa server dibagi menjadi metrik komputasi dan metrik data dan penyimpanan, masing-masing termasuk dalam kumpulan dimensi workgroup dan namespace. Untuk informasi selengkapnya tentang workgroup dan ruang nama, lihat [Ikhtisar grup kerja dan ruang nama Amazon Redshift Tanpa Server](#).

CloudWatch metrik komputasi adalah sebagai berikut:

CloudWatch menghitung metrik

Nama metrik	Unit	Deskripsi	Set dimensi
QueriesCompletedPerSecond	Jumlah kueri	Jumlah kueri yang diselesaikan setiap detik.	{Database LatencyRange,, Kelompok Kerja}, {LatencyRange, Kelompok Kerja}
QueryDuration	Mikrodetik	Jumlah rata-rata waktu untuk menyelesaikan kueri.	{Database LatencyRange,, Kelompok Kerja}, {LatencyRange, Kelompok Kerja}
QueriesRunning	Jumlah kueri	Jumlah query yang berjalan	{Database QueryType,,

Nama metrik	Unit	Deskripsi	Set dimensi
		pada suatu titik waktu.	Kelompok Kerja}, {QueryType, Kelompok Kerja}
QueriesQueued	Jumlah kueri	Jumlah kueri dalam antrian pada suatu titik waktu.	{Database QueryType,, Kelompok Kerja}, {QueryType, Kelompok Kerja}
DatabaseConnections	Jumlah koneksi	Jumlah koneksi ke database pada suatu titik waktu.	{Database, Kelompok Kerja}, {Kelompok Kerja}
QueryRuntimeBreakdown	Milidetik	Total waktu kueri dijalankan, berdasarkan tahap kueri.	{Database, Panggung, Kelompok Kerja}, {Tahap, Kelompok Kerja}
ComputeCapacity	RPU	Jumlah rata-rata unit komputasi yang dialokasikan selama 30 menit terakhir, dibulatkan ke bilangan bulat terdekat.	{Kelompok Kerja}
ComputeSeconds	RPU-detik	Akumulasi detik unit komputasi yang digunakan dalam 30 menit terakhir.	{Kelompok Kerja}

Nama metrik	Unit	Deskripsi	Set dimensi
QueriesSucceeded	Jumlah kueri	Jumlah query yang berhasil dalam 5 menit terakhir.	{Database QueryType,, Kelompok Kerja}, {QueryType, Kelompok Kerja}
QueriesFailed	Jumlah kueri	Jumlah kueri yang gagal dalam 5 menit terakhir.	{Database QueryType,, Kelompok Kerja}, {QueryType, Kelompok Kerja}

Nama metrik	Unit	Deskripsi	Set dimensi
UsageLimitAvailable	RPU-jam atau TBs	<p>Tergantung pada UsageType, UsageLimitAvailable mengembalikan yang berikut:</p> <ul style="list-style-type: none"> • Jika UsageType adalah SERVERLESS_COMPUTE, UsageLimitAvailable mengembalikan jumlah RPU-jam yang tersisa yang dapat ditanyakan oleh workgroup dalam batas yang diberikan. • Jika UsageType adalah CROSS_REGION_DATASHARING, UsageLimitAvailable mengembal 	{UsageLimitId, UsageType, Kelompok Kerja}

Nama metrik	Unit	Deskripsi	Set dimensi
		ikan sisa jumlah TB yang dapat dipindai pelanggan dalam batas yang diberikan.	

Nama metrik	Unit	Deskripsi	Set dimensi
UsageLimitConsumed	RPU-jam atau TBs	<p>Tergantung pada UsageType, UsageLimitConsumed mengembalikan yang berikut:</p> <ul style="list-style-type: none"> • Jika UsageType adalah SERVERLESS_COMPUTE, UsageLimitConsumed mengembalikan jumlah RPU-jam yang telah ditanyakan oleh workgroup dalam batas yang diberikan. • Jika UsageType adalah CROSS_REGION_DATASHARING, UsageLimitConsumed mengembalikan jumlah 	{UsageLimitId, UsageType, Kelompok Kerja}

Nama metrik	Unit	Deskripsi	Set dimensi
		TB yang telah digunakan pelanggan untuk memindai dalam batas yang diberikan.	

CloudWatch Metrik data dan penyimpanan adalah sebagai berikut:

CloudWatch metrik data dan penyimpanan

Nama metrik	Unit	Deskripsi	Set dimensi
TotalTableCount	Jumlah tabel	Jumlah tabel pengguna yang ada pada suatu titik waktu. Total ini tidak termasuk tabel Amazon Redshift Spectrum.	{Database, Ruang Nama}
DataStorage	Megabyte	Jumlah megabyte yang digunakan , dalam disk atau ruang penyimpanan, untuk data Redshift.	{Ruang nama}

SnapshotStorageMetriknya adalah namespace- dan workgroup-agnostik.

CloudWatchSnapshotStorage metrik adalah sebagai berikut:

CloudWatch SnapshotStorage metrik

Nama metrik	Unit	Deskripsi	Set dimensi
SnapshotStorage	Megabyte	Jumlah megabyte yang digunakan, dalam disk atau ruang penyimpanan, untuk Snapshots.	{}

Kumpulan dimensi adalah dimensi pengelompokan yang diterapkan pada metrik Anda. Anda dapat menggunakan grup dimensi ini untuk menentukan bagaimana statistik Anda diambil.

Tabel berikut merinci dimensi dan nilai dimensi untuk metrik tertentu:

CloudWatch dimensi dan nilai dimensi

Dimensi	Deskripsi dan nilai
DatabaseName	Nama basis data. Nilai khusus.
Latency	Kemungkinan nilainya adalah sebagai berikut: <ul style="list-style-type: none"> • Pendek - di bawah 10 detik • Sedang — antara 10 detik dan 10 menit • Panjang — lebih dari 10 menit
QueryType	Kemungkinan nilai adalah INSERT, DELETE, UPDATE, UNLOAD, LOAD, SELECT, CTAS, dan OTHER.
stage	Tahapan eksekusi untuk kueri. Kemungkinan nilainya adalah sebagai berikut:

Dimensi	Deskripsi dan nilai
	<ul style="list-style-type: none"> • QueryPlanning: Waktu yang dihabiskan mengurai dan mengoptimalkan pernyataan SQL. • QueryWaiting: Waktu yang dihabiskan menunggu di antrian WLM. • QueryExecutingRead: Waktu yang dihabiskan untuk mengeksekusi kueri baca. • QueryExecutingInsert: Waktu yang dihabiskan untuk mengeksekusi kueri sisipan. • QueryExecutingDelete: Waktu yang dihabiskan untuk mengeksekusi kueri hapus. • QueryExecutingUpdate: Waktu yang dihabiskan untuk mengeksekusi kueri pembaruan. • QueryExecutingCtas: Waktu yang dihabiskan untuk mengeksekusi membuat tabel sebagai kueri. • QueryExecutingUnload: Waktu yang dihabiskan untuk mengeksekusi kueri bongkar muat. • QueryExecutingCopy: Waktu yang dihabiskan untuk mengeksekusi kueri salinan. • QueryCommit: Waktu yang dihabiskan untuk berkomitmen.
Namespace	Nama namespace. Nilai khusus.
Workgroup	Nama workgroup. Nilai khusus.
UsageLimitId	Pengidentifikasi batas penggunaan.

Dimensi	Deskripsi dan nilai
UsageType	Fitur Amazon Redshift Tanpa Server dibatasi. Kemungkinan nilainya adalah sebagai berikut: <ul style="list-style-type: none">• SERVERLESS_COMPUTE• CROSS_REGION_DATASHARING

Bekerja dengan snapshot dan titik pemulihan

Cadangan di Amazon Redshift Serverless adalah point-in-time representasi objek dan data di namespace Anda. Ada dua jenis cadangan: snapshot yang dibuat secara manual dan titik pemulihan yang dibuat secara otomatis oleh Amazon Redshift Serverless untuk Anda. Poin pemulihan dibuat setiap 30 menit dan disimpan selama 24 jam.

Jika Anda menemukan bahwa Anda ingin mengambil data dalam snapshot atau titik pemulihan, Anda dapat memulihkan snapshot ke namespace tanpa server atau ke kluster yang disediakan. Ada tiga skenario di mana Anda dapat memulihkan snapshot:

- Kembalikan snapshot tanpa server ke namespace tanpa server.
- Kembalikan snapshot tanpa server ke cluster yang disediakan.
- Kembalikan snapshot cluster yang disediakan ke namespace tanpa server.

Saat mengembalikan snapshot tanpa server ke kluster yang disediakan, Anda harus memilih jenis node yang akan digunakan, seperti RA3, dan jumlah node, sehingga Anda dapat mengontrol pengaturan di tingkat cluster atau node.

Untuk memulihkan snapshot kluster yang disediakan ke namespace tanpa server, mulai dari konsol yang disediakan Redshift, pilih snapshot yang akan dipulihkan, lalu pilih Pulihkan dari snapshot, Pulihkan ke namespace tanpa server. Amazon Redshift mengonversi tabel dengan kunci interleaved menjadi kunci pengurutan majemuk saat Anda memulihkan snapshot kluster yang disediakan ke namespace tanpa server. Untuk informasi selengkapnya tentang kunci sortir, lihat [Bekerja dengan kunci sortir](#).

Jika Anda ingin menambahkan konteks tambahan, Anda dapat menandai snapshot dan titik pemulihan dengan pasangan nilai kunci yang menyediakan metadata dan informasi ke snapshot

dan titik pemulihan. Untuk informasi selengkapnya tentang menandai sumber daya, lihat Ringkasan sumber [daya penandaan](#).

Terakhir, Anda juga dapat berbagi snapshot dengan AWS akun lain, yang memungkinkan mereka mengakses data dalam snapshot dan menjalankan kueri.

Snapshot

Anda dapat memulihkan snapshot yang dibuat di konsol Amazon Redshift Tanpa Server ke namespace yang tersedia yang terkait dengan workgroup. Namespace tersedia setelah siap untuk query dan/atau modifikasi. Anda dapat memulihkan snapshot yang dienkripsi dengan kunci KMS AWS terkelola ke namespace tanpa server.

Untuk melihat daftar semua snapshot Anda, di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data.

Untuk membuat snapshot

1. Di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data.
2. Pilih Buat snapshot.
3. Pilih namespace untuk membuat snapshot dari.
4. Masukkan pengenalan snapshot.
5. (Opsional) Pilih periode retensi. Jika Anda memilih Nilai kustom, pilih jumlah hari. Jumlah yang Anda pilih harus antara 1-3653 hari, inklusif. Defaultnya dipertahankan tanpa batas waktu.
6. Pilih Buat.

Untuk membuat snapshot dari konfigurasi namespace

1. Di konsol Amazon Redshift Tanpa Server, pilih konfigurasi Namespace.
2. Pilih namespace untuk membuat snapshot dari. Anda hanya dapat membuat snapshot dari namespace yang terkait dengan workgroup dan yang statusnya Tersedia.
3. Pilih tab Pencadangan data.
4. Pilih Buat snapshot.
5. Masukkan pengenalan snapshot.
6. (Opsional) Pilih periode retensi. Jika Anda memilih Nilai kustom, pilih jumlah hari. Jumlah yang Anda pilih harus antara 1-3653 hari, inklusif.

7. Pilih Buat.

Untuk memperbarui periode retensi snapshot

1. Di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data.
2. Pilih snapshot untuk diperbarui.
3. Pilih Tindakan, Atur pengaturan snapshot manual.
4. Pilih periode retensi. Jika Anda memilih Nilai kustom, pilih jumlah hari.
5. Pilih Simpan perubahan.

Untuk menghapus snapshot

Note

Anda tidak dapat menghapus snapshot yang telah dibagikan dengan akun lain. Anda harus terlebih dahulu menghapus akses akun itu ke snapshot sebelum menghapus snapshot.

1. Di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data.
2. Pilih snapshot untuk dihapus.
3. Pilih Tindakan, Hapus.
4. Pilih Hapus.

Untuk membuat snapshot akhir dari semua data dalam namespace sebelum menghapus namespace.

1. Di konsol Amazon Redshift Tanpa Server, pilih konfigurasi Namespace.
2. Pilih namespace yang akan dihapus.
3. Pilih Tindakan, Hapus.
4. Pilih Buat snapshot akhir.
5. Masukkan nama untuk snapshot.
6. Masukkan hapus.
7. Pilih Hapus.

Untuk berbagi snapshot dengan AWS akun lain atau menghapus akses akun ke snapshot

1. Di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data.
2. Pilih snapshot untuk dibagikan.
3. Pilih Tindakan, Kelola akses.
4. Untuk berbagi snapshot dengan akun lain, masukkan Akun AWSID. Untuk menghapus akses dari akun, pilih Hapus.
5. Pilih Simpan perubahan.

Memulihkan snapshot

Memulihkan snapshot ke namespace tanpa server menggantikan database saat ini dengan database dalam snapshot.

Memulihkan snapshot ke namespace tanpa server diselesaikan dalam dua fase. Fase pertama selesai dalam beberapa menit, mengembalikan data ke namespace Anda, dan membuatnya tersedia untuk kueri. Tahap kedua restorasi adalah tempat database Anda disetel, yang dapat menyebabkan masalah kinerja kecil. Fase kedua ini dapat berlangsung dari beberapa jam hingga beberapa hari, dan dalam beberapa kasus, beberapa minggu. Jumlah waktu tergantung pada ukuran data, tetapi kinerja semakin meningkat saat database disetel. Pada akhir fase ini, namespace tanpa server Anda sepenuhnya disetel, dan Anda dapat mengirimkan kueri tanpa masalah kinerja.

Untuk mengembalikan snapshot ke namespace tanpa server

1. Di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data.
2. Pilih snapshot untuk dipulihkan. Anda hanya dapat memulihkan satu snapshot pada satu waktu.
3. Pilih Tindakan, Pulihkan ke namespace tanpa server.
4. Pilih namespace yang tersedia untuk dipulihkan. Anda hanya dapat mengembalikan ke ruang nama yang statusnya Tersedia.
5. Pilih Pulihkan.

Untuk memulihkan snapshot ke kluster yang disediakan

1. Di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data.
2. Pilih snapshot untuk dipulihkan.

3. Pilih Tindakan, Pulihkan ke klaster yang disediakan.
4. Masukkan pengidentifikasi cluster.
5. Pilih tipe Node. Jumlah node tergantung pada jenis node.
6. Ikuti petunjuk pada halaman di halaman konsol untuk memasukkan properti untuk konfigurasi Cluster. Lihat [Membuat klaster](#) untuk informasi selengkapnya.

[Untuk informasi selengkapnya tentang snapshot pada klaster yang disediakan, lihat snapshot dan cadangan Amazon Redshift.](#)

Poin pemulihan

Poin pemulihan di Amazon Redshift Tanpa Server dibuat kira-kira setiap 30 menit dan disimpan selama 24 jam.

Di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data untuk mengelola titik pemulihan. Anda dapat melakukan operasi berikut:

- Kembalikan titik pemulihan ke namespace tanpa server.
- Ubah titik pemulihan menjadi snapshot.

Untuk mengembalikan titik pemulihan ke namespace tanpa server

1. Di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data.
2. Di bawah Poin pemulihan, pilih waktu pembuatan titik pemulihan yang ingin Anda pulihkan.
3. Pilih Pulihkan. Anda hanya dapat mengembalikan ke ruang nama yang statusnya Tersedia.
4. Masukkan restore di bidang input teks dan pilih Restore.

Untuk mengonversi titik pemulihan menjadi snapshot

1. Di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data.
2. Di bawah Poin pemulihan, pilih waktu pembuatan titik pemulihan yang ingin Anda konversi ke snapshot.
3. Pilih Buat snapshot dari titik pemulihan.
4. Masukkan pengenalan Snapshot.
5. Pilih Buat.

Menjadwalkan snapshot

Untuk mengontrol secara tepat kapan harus mengambil snapshot, Anda dapat membuat jadwal snapshot untuk namespaces tertentu. Saat menjadwalkan pembuatan snapshot, Anda dapat membuat acara satu kali atau menggunakan ekspresi cron Unix untuk membuat jadwal berulang. Ekspresi cron mendukung tiga bidang dan dipisahkan oleh spasi putih.

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

Bidang	Nilai-nilai	Wildcard
Menit	0–59	, - * /
Jam	0–23	, - * /
Day-of-month	1–31	, - * ? / L W
Bulan	1–12 atau JAN-DEC	, - * /
Day-of-week	1–7 atau SUN-SAT	, - * ? L #
Tahun	1970–2199	, - * /

Wildcard

- Wildcard , (koma) mencakup nilai tambahan. Di Day-of-week lapangan, MON, WED, FRI akan mencakup Senin, Rabu, dan Jumat. Nilai total dibatasi hingga 24 per bidang.
- Wildcard - (tanda hubung) menentukan rentang. Di Hour lapangan, 1-15 akan mencakup jam 1 hingga 15 dari hari yang ditentukan.
- Wildcard * (bintang) mencakup semua nilai di bidang. Di kolom Hours, * akan mencakup setiap jam.
- Wildcard / (garis miring) menentukan tambahan. Di Hours lapangan, Anda bisa masuk **1/10** untuk menentukan setiap jam ke-10, mulai dari jam pertama hari itu (misalnya, 01:00, 11:00, dan 21:00).
- Wildcard ? (tanda tanya) menentukan satu atau yang lain. Di **Day-of-month** lapangan Anda bisa masuk 7, dan jika Anda tidak peduli hari apa dalam minggu ketujuh, Anda bisa masuk? di ay-of-week bidang D.

- Wildcard L di kolom Day-of-month atau Day-of-week menentukan hari terakhir pada bulan atau minggu.
- Wildcard W di kolom Day-of-month menentukan hari kerja. Di kolom Day-of-month, 3W menentukan hari kerja yang paling dekat dengan pekan ketiga di bulan itu.
- Wildcard # di ay-of-week bidang D menentukan contoh tertentu dari hari yang ditentukan dalam seminggu dalam sebulan. Sebagai contoh, 3#2 akan menjadi hari Selasa kedua setiap bulan: 3 mengacu pada hari Selasa karena itu adalah hari ketiga setiap minggu, dan 2 mengacu pada hari kedua dari jenis tersebut dalam bulan tersebut.

Note

Jika Anda menggunakan karakter '#', Anda hanya dapat menentukan satu ekspresi di day-of-week bidang. Misalnya, "3 #1 ,6 #3" tidak valid karena ditafsirkan sebagai dua ekspresi.

Batas

- Anda tidak dapat menentukan kolom Day-of-month dan Day-of-week dalam ekspresi cron yang sama. Jika Anda menentukan sebuah nilai di salah satu kolom, maka Anda harus menggunakan ? (tanda tanya) di kolom yang lain.
- Jadwal snapshot tidak mendukung frekuensi berikut:
 - Snapshot dijadwalkan lebih sering dari 1 per jam.
 - Snapshot dijadwalkan kurang dari 1 per hari (24 jam).

Jika Anda memiliki jadwal yang tumpang tindih yang menghasilkan penjadwalan snapshot dalam jendela 1 jam, kesalahan validasi akan terjadi.

Tabel berikut memiliki beberapa contoh string cron.

Menit	Jam	Hari dalam seminggu	Arti			
0	14-20/1	SELAM	Setiap jam antara jam 2 siang dan 8 malam pada hari Selasa.			

Menit	Jam	Hari dalam seminggu	Arti			
0	21	MON-FRI	Setiap malam jam 9 malam Senin-Jumat.			
30	0/6	SAT-MATAHARI	Setiap kenaikan 6 jam pada hari Sabtu dan Minggu dimulai pada 30 menit setelah tengah malam (00:30) hari itu. Ini menghasilkan snapshot pada [00:30, 06:30, 12:30, dan 18:30] setiap hari.			
30	12/4	*	Setiap kenaikan 4 jam mulai pukul 12:30 setiap hari. Ini memutuskan untuk [12:30, 16:30, 20:30].			

Contoh berikut menunjukkan cara membuat jadwal yang berjalan dalam kenaikan 2 jam mulai dari 15:15 setiap hari.

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

Saat ini, Anda hanya dapat menggunakan Amazon Redshift Serverless API atau AWS CLI untuk membuat jadwal snapshot. Untuk informasi selengkapnya tentang operasi tersebut, lihat [Menggunakan API Tanpa Server Amazon Redshift AWS CLI dan Amazon Redshift](#).

Menyalin cadangan ke yang lain Wilayah AWS

Anda dapat mengonfigurasi Amazon Redshift Tanpa Server untuk secara otomatis menyalin snapshot dan titik pemulihan ke yang lain. Wilayah AWS Saat Anda membuat snapshot di sumber Wilayah AWS, itu disalin ke Wilayah tujuan. Anda dapat mengonfigurasi namespace Anda

sehingga hanya menyalin snapshot dan titik pemulihan ke satu tujuan Wilayah AWS pada satu waktu. Untuk daftar Wilayah AWS tempat Amazon Redshift Serverless tersedia, lihat titik akhir yang terdaftar untuk [Redshift](#) Serverless API di. Referensi Umum Amazon Web Services

Saat mengonfigurasi penyalinan cadangan, Anda juga dapat menentukan periode retensi berapa lama Amazon Redshift Serverless harus menyimpan snapshot yang disalin. Anda tidak dapat mengubah periode retensi titik pemulihan, yang harus 1 hari. Periode retensi snapshot di Wilayah tujuan terpisah dari periode retensi snapshot di Wilayah sumber. Secara default, periode retensi adalah menyimpan snapshot tanpa batas waktu. Jika Anda memilih Nilai kustom pilih jumlah hari. Jumlah yang Anda pilih harus antara 1-3653 hari, inklusif.

Untuk mengubah Wilayah tujuan untuk menyalin snapshot, pertama nonaktifkan penyalinan cadangan, lalu tentukan Wilayah tujuan baru saat Anda mengaktifkan kembali penyalinan.

Setelah snapshot atau titik pemulihan disalin ke Wilayah tujuan, Anda dapat menggunakannya untuk memulihkan data ke Wilayah.

Secara default, data Anda dienkripsi dengan kunci yang AWS mengelola untuk Anda. Untuk menggunakan kunci yang berbeda, pilih kunci yang ingin Anda gunakan saat mengonfigurasi penyalinan cadangan di sumber Wilayah AWS, dan Amazon Redshift Tanpa Server secara otomatis membuat hibah, yang memungkinkan enkripsi snapshot di tujuan. Wilayah AWS

Untuk menyalin cadangan ke Wilayah lain, pastikan Anda memiliki izin IAM berikut:

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

Jika Anda menggunakan kunci KMS Anda sendiri untuk mengenkripsi cadangan Anda, Anda juga memerlukan izin berikut:

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

Untuk mengonfigurasi penyalinan snapshot atau titik pemulihan Anda ke yang lain Wilayah AWS

1. Di konsol Amazon Redshift Tanpa Server, pilih namespace yang ingin Anda konfigurasi menyalin snapshot atau titik pemulihan.

2. Pilih Tindakan, Konfigurasi cadangan Lintas wilayah.
3. Pilih tujuan Wilayah AWS untuk menyalin snapshot ke.
4. (Opsional) Pilih berapa lama untuk mempertahankan snapshot. Jika Anda memilih Nilai kustom pilih jumlah hari Jumlah yang Anda pilih harus antara 1-3653 hari, inklusif. Defaultnya adalah mempertahankan tanpa batas waktu.
5. (Opsional) Pilih AWS KMS kunci lain yang akan digunakan untuk mengenkripsi enkripsi di Wilayah tujuan.
6. Pilih Simpan konfigurasi.

Memulihkan tabel

Anda juga dapat memulihkan tabel tertentu dari snapshot atau titik pemulihan Saat melakukannya, Anda menentukan snapshot sumber atau titik pemulihan, database, skema, tabel, basis data target, skema, dan nama tabel baru. Tabel baru ini tidak dapat memiliki nama yang sama dengan tabel yang ada. Jika Anda ingin mengganti tabel yang ada dengan memulihkan tabel, Anda harus terlebih dahulu mengganti nama atau menjatuhkan tabel sebelum Anda mengembalikan tabel.

Tabel target dibuat menggunakan definisi kolom tabel sumber, atribut tabel, dan atribut kolom kecuali untuk kunci asing. Untuk mencegah konflik karena dependensi, tabel target tidak mewarisi kunci asing dari tabel sumber. Dependensi apa pun, seperti tampilan atau izin yang diberikan pada tabel sumber, tidak diterapkan ke tabel target.

Jika pemilik tabel sumber ada, maka pengguna tersebut adalah pemilik tabel yang dipulihkan, asalkan pengguna memiliki izin yang cukup untuk menjadi pemilik relasi dalam database dan skema yang ditentukan. Jika tidak, tabel yang dipulihkan dimiliki oleh pengguna admin yang dibuat saat cluster diluncurkan.

Tabel yang dipulihkan kembali ke keadaan semula pada saat cadangan diambil. Ini termasuk aturan visibilitas transaksi yang ditentukan oleh kepatuhan Amazon Redshift terhadap isolasi [serial](#), yang berarti bahwa data akan segera terlihat dalam transaksi penerbangan yang dimulai setelah pencadangan.

Anda dapat menggunakan konsol Amazon Redshift Tanpa Server untuk memulihkan tabel dari snapshot.

Memulihkan tabel dari cadangan data memiliki batasan berikut:

- Anda hanya dapat mengembalikan satu tabel pada satu waktu.

- Dependensi apa pun, seperti tampilan atau izin yang diberikan pada tabel sumber, tidak diterapkan ke tabel target.
- Jika keamanan tingkat baris diaktifkan untuk tabel dipulihkan, Amazon Redshift Serverless mengembalikan tabel dengan keamanan tingkat baris diaktifkan.

Untuk memulihkan tabel menggunakan konsol Amazon Redshift Serverless

1. Di konsol Amazon Redshift Tanpa Server, pilih Pencadangan data.
2. Pilih snapshot atau titik pemulihan yang memiliki tabel untuk dipulihkan.
3. Pilih Tindakan, Kembalikan tabel dari snapshot atau Pulihkan tabel dari titik pemulihan.
4. Masukkan informasi tentang snapshot sumber atau titik pemulihan dan tabel target, lalu pilih Pulihkan tabel.

Menggunakan API Tanpa AWS Command Line Interface Server Amazon Redshift dan Amazon

Selain menggunakan AWS konsol, Anda juga dapat menggunakan AWS CLI atau Amazon Redshift Serverless API untuk berinteraksi dengan snapshot dan titik pemulihan. Tabel di bawah ini mencantumkan operasi API dan CLI yang dapat Anda gunakan untuk mengelola snapshot dan titik pemulihan.

Operasi API	Perintah CLI	Deskripsi
CreateSnapshot	buat-snapshot	Membuat snapshot. Snapshot harus dikaitkan dengan namespace, jadi Anda harus menyertakan nama namespace dalam permintaan Anda. Secara default, Amazon Redshift Serverless menyimpan snapshot untuk jangka waktu yang tidak terbatas, tetapi Anda dapat menentukan periode retensi.

Operasi API	Perintah CLI	Deskripsi
RestoreFromSnapshot	restore-from-snapshot	Mengembalikan database dalam snapshot ke namespace Anda. Jika memulihkan snapshot dari Amazon Redshift Tanpa Server ke kluster yang disediakan, Anda harus menentukan snapshotArn snapshot yang sedang Anda pulihkan. Jika tidak, jika Anda memulihkan dari tanpa server ke tanpa server, Anda dapat menentukan snapshotArn atau snapshotName, tetapi tidak keduanya.
RestoreTableFromSnapshot	restore-table-from-snapshot	Mengembalikan tabel dari snapshot ke namespace Amazon Redshift Tanpa Server Anda. Anda tidak dapat menggunakan operasi ini untuk memulihkan tabel dengan kunci pengurutan yang disisipkan.
GetSnapshot	dapatkan-snapshot	Mengambil informasi tentang snapshot.
ListSnapshots	daftar-snapshot	Mengambil informasi tentang beberapa snapshot.
DeleteSnapshot	hapus-snapshot	Menghapus snapshot.
RestoreFromRecoveryPoint	restore-from-recovery-point	Mengembalikan data dalam titik pemulihan ke namespace Anda.

Operasi API	Perintah CLI	Deskripsi
RestoreTableFromRecoveryPoint	restore-table-from-recovery-point	Mengembalikan tabel dari titik pemulihan ke namespace Amazon Redshift Tanpa Server Anda. Anda tidak dapat menggunakan operasi ini untuk memulihkan tabel dengan kunci pengurutan yang disisipkan.
ConvertRecoveryPointToSnapshot	convert-recovery-point-to-snapshot	Mengonversi titik pemulihan ke snapshot.
GetRecoveryPoint	get-recovery-point	Mengambil informasi tentang titik pemulihan.
ListRecoveryPoints	list-recovery-points	Mengambil informasi tentang beberapa titik pemulihan.

Untuk menjadwalkan pembuatan snapshot, gunakan operasi API berikut.

Operasi API	Perintah CLI	Deskripsi
CreateScheduledAction	create-scheduled-action	Membuat tindakan terjadwal, yang berisi jadwal dan tindakan Amazon Redshift Tanpa Server. Misalnya, Anda dapat membuat jadwal kapan menjalankan operasi <code>CreateSnapshot</code> API.
DeleteScheduledAction	delete-scheduled-action	Menghapus tindakan terjadwal.
GetScheduledAction	get-scheduled-action	Mengambil informasi tentang tindakan terjadwal.

Operasi API	Perintah CLI	Deskripsi
ListScheduledActions	list-scheduled-actions	Mengambil informasi tentang daftar tindakan terjadwal.
UpdateScheduledAction	update-scheduled-action	Memperbarui tindakan terjadwal.

Berbagi data di Amazon Redshift Tanpa Server

Gunakan berbagi data untuk membagikan informasi yang paling konsisten up-to-date dan paling konsisten saat diperbarui di Amazon Redshift Tanpa Server.

Berbagi data di Amazon Redshift Tanpa Server

Dengan berbagi data, Anda memiliki akses langsung ke data sehingga pengguna dapat melihat informasi yang paling konsisten up-to-date dan paling konsisten saat diperbarui di Amazon Redshift Tanpa Server.

Memulai berbagi data di Amazon Redshift Serverless

Anda dapat membagikan data untuk tujuan pembacaan di berbagai instans Tanpa Server Amazon Redshift di dalam atau di seluruh Akun AWS

Anda dapat memulai berbagi data dengan menggunakan antarmuka SQL atau konsol Amazon Redshift. Untuk informasi selengkapnya, lihat [Memulai berbagi data menggunakan antarmuka SQL](#) atau [Memulai berbagi data menggunakan konsol di Panduan Pengembang](#) Database Amazon Redshift di Panduan Pengembang Database Amazon Redshift.

Dengan berbagi data, ruang nama Amazon Redshift Tanpa Server dan kluster yang disediakan dapat berbagi data langsung satu sama lain, baik di dalam seberang, atau di seberang. Akun AWS Akun AWS Wilayah AWS Untuk informasi selengkapnya, lihat [Wilayah tempat berbagi data tersedia](#).

Untuk mulai berbagi data dalam file Akun AWS, buka AWS Management Console, lalu pilih konsol Amazon Redshift. Pilih konfigurasi Namespace dan kemudian Datashares. Ikuti prosedur di [Memulai berbagi data menggunakan konsol di Panduan](#) Pengembang Database Amazon Redshift.

Untuk mulai berbagi data Akun AWS, buka AWS Management Console, lalu pilih konsol Amazon Redshift. Pilih Datashares. Ikuti prosedur di [Memulai berbagi data menggunakan konsol di Panduan Pengembang Database Amazon Redshift](#).

Untuk memulai kueri data dalam datashare, buat database di namespace yang memiliki workgroup yang terkait dengannya. Dari datashare tertentu, pilih namespace yang memiliki workgroup yang terkait dengannya dan buat database untuk kueri data. Ikuti prosedur di [Membuat database dari datashares](#).

Memberikan akses untuk melihat datashares menggunakan konsol

Superuser dapat memberikan akses ke pengguna yang bukan pengguna super sehingga mereka dapat melihat datashares yang dibuat oleh semua pengguna.

Untuk memberikan akses ke datashare bagi pengguna, gunakan perintah berikut untuk menyediakan akses datashare bagi pengguna, di mana `datashare_name` adalah nama datashare dan nama pengguna adalah nama pengguna yang ingin Anda berikan akses.

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

Untuk memberikan akses ke datashare untuk grup pengguna, pertama buat grup pengguna dengan pengguna. Untuk informasi tentang cara membuat grup pengguna, lihat [MEMBUAT GRUP](#). Kemudian, berikan akses datashare ke pengguna menggunakan perintah berikut, di mana `datashare_name` adalah nama datashare dan `user-group` adalah nama grup pengguna yang ingin Anda berikan akses.

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

Untuk informasi tentang cara menggunakan pernyataan GRANT, lihat [GRANT](#).

Pertimbangan berbagi data di Amazon Redshift Tanpa Server

Berikut ini adalah pertimbangan untuk bekerja dengan berbagi data di Amazon Redshift Serverless:

- Amazon Redshift hanya mendukung klaster yang disediakan dari tipe instans `ra3.16xlarge`, `ra3.4xlarge`, dan `ra3.xlplus`, serta titik akhir tanpa server sebagai produsen atau konsumen berbagi data.
- Amazon Redshift Tanpa Server dienkripsi secara default.

Untuk daftar batasan pembagian data, termasuk objek database yang didukung, persyaratan enkripsi, dan persyaratan sort-key, lihat [Pertimbangan saat menggunakan berbagi data di Amazon Redshift di Panduan Pengembang Database Amazon Redshift](#).

Memberi tag pada sumber daya

Dalam AWS, tag adalah label yang ditentukan pengguna yang terdiri dari pasangan nilai-kunci. Amazon Redshift Tanpa Server mendukung pemberian tag untuk menyediakan metadata tentang sumber daya secara sekilas.

Tag tidak diperlukan untuk sumber daya, tetapi mereka membantu menyediakan konteks. Anda mungkin ingin menandai sumber daya dengan metadata dengan informasi yang terkait dengan sumber daya. Sebagai contoh, Anda ingin melacak sumber daya mana yang termasuk dalam lingkungan pengujian dan lingkungan produksi. Anda dapat membuat lingkungan bernama kunci dan memberikan uji nilai atau produksi untuk mengidentifikasi sumber daya yang digunakan di setiap lingkungan. Jika Anda menggunakan penandaan di AWS layanan lain atau memiliki kategori standar untuk bisnis Anda, kami sarankan Anda membuat pasangan nilai kunci yang sama untuk sumber daya agar konsisten.

Jika Anda menghapus sebuah sumber daya, tag apa pun yang terkait dihapus. Anda dapat menggunakan konsol Amazon Redshift Serverless AWS CLI dan Amazon untuk menandai sumber daya tanpa server. Operasi API yang tersedia adalah `TagResource`, `UntagResource`, dan `ListTagsForResource`.

Setiap sumber daya memiliki satu set tag, yang merupakan kumpulan dari satu atau lebih tag yang ditugaskan ke sumber daya. Setiap sumber daya dapat memiliki hingga 50 tag dapat memiliki hingga 50 tag dapat diatur. Anda dapat menambahkan tag saat membuat sebuah sumber daya dan setelah sebuah sumber daya telah dibuat. Anda dapat menambahkan tag ke jenis sumber daya tanpa server berikut:

- Kelompok kerja
- Namespace
- Snapshot
- Poin pemulihan

Tag memiliki persyaratan sebagai berikut:

- Kunci tidak dapat diawali dengan `aws :`.

- Kunci dalam rangkaian tag harus unik.
- Kunci harus berkisar antara 1 sampai 128 karakter yang diizinkan.
- Nilai harus antara 0 dan 256 karakter yang diizinkan.
- Nilai tidak perlu bersifat unik untuk setiap tag tidak perlu unik.
- Karakter yang diizinkan untuk kunci dan nilai nilai Unicode adalah huruf Unicode, angka, white space, dan salah satu simbol berikut: `._:/= + - @`.
- Kunci dan nilai peka huruf besar dan kecil.

Mengelola tag sumber daya Amazon Redshift Tanpa Server

1. Di konsol Amazon Redshift Tanpa Server, pilih Kelola Tag.
2. Masukkan jenis sumber daya yang akan dicari dan pilih Cari sumber daya. Pilih sumber daya yang ingin Anda kelola, lalu pilih Kelola tanda yang ingin Anda kelola, lalu pilih Kelola tanda.
3. Tentukan kunci dan nilai opsional yang ingin Anda tambahkan ke sumber daya. Saat memodifikasi tag, Anda dapat mengubah nilai tag, tetapi bukan kuncinya.
4. Setelah selesai menambahkan, menghapus, atau memodifikasi tag, pilih Simpan perubahan, lalu pilih Terapkan untuk menyimpan perubahan.

Cluster yang disediakan Amazon Redshift

Di bagian berikut, Anda dapat mempelajari dasar-dasar membuat gudang data dengan meluncurkan satu set node komputasi, yang disebut cluster Amazon Redshift.

Topik

- [Ikhtisar Amazon Redshift](#)
- [Gunakan EC2-VPC saat Anda membuat cluster](#)
- [Alarm ruang disk default](#)
- [Status klaster](#)
- [Pertimbangan untuk menggunakan cluster yang disediakan Amazon Redshift](#)
- [Operasi cluster](#)
- [Mengkonfigurasi penyebaran Multi-AZ](#)
- [Mengelola cluster menggunakan konsol](#)
- [Mengelola cluster menggunakan API Amazon AWS CLI Redshift dan Amazon](#)
- [Mengelola cluster dalam VPC](#)
- [Riwayat versi cluster](#)

Ikhtisar Amazon Redshift

Gudang data Amazon Redshift adalah kumpulan sumber daya komputasi yang disebut node, yang diatur ke dalam grup yang disebut cluster. Setiap klaster menjalankan mesin Amazon Redshift dan berisi satu atau lebih database.

Note

Saat ini, mesin Amazon Redshift versi 1.0 tersedia. Namun, saat mesin diperbarui, beberapa versi mesin Amazon Redshift mungkin tersedia untuk dipilih.

Cluster dan node di Amazon Redshift

Cluster Amazon Redshift terdiri dari node. Setiap cluster memiliki node pemimpin dan satu atau lebih node komputasi. Node pemimpin menerima kueri dari aplikasi klien, mem-parsing kueri, dan

mengembangkan rencana eksekusi kueri. Node pemimpin kemudian mengoordinasikan eksekusi paralel dari rencana ini dengan node komputasi dan mengumpulkan hasil antara dari node ini. Kemudian akhirnya mengembalikan hasil kembali ke aplikasi klien.

Node komputasi menjalankan rencana eksekusi kueri dan mengirimkan data di antara mereka sendiri untuk melayani kueri ini. Hasil antara dikirim ke node pemimpin untuk agregasi sebelum dikirim kembali ke aplikasi klien. Untuk informasi selengkapnya tentang node pemimpin dan node komputasi, lihat [Arsitektur sistem gudang data di Panduan](#) Pengembang Database Amazon Redshift.

Note

Saat membuat klaster di konsol Amazon Redshift (<https://console.aws.amazon.com/redshiftv2/>), Anda bisa mendapatkan rekomendasi konfigurasi klaster berdasarkan ukuran data dan karakteristik kueri. Untuk menggunakan kalkulator ukuran ini, cari Bantu saya memilih di konsol di AWS Wilayah yang mendukung jenis simpul RA3. Untuk informasi selengkapnya, lihat [Membuat klaster](#).

Saat Anda meluncurkan cluster, salah satu opsi yang Anda tentukan adalah tipe node. Tipe node menentukan CPU, RAM, kapasitas penyimpanan, dan tipe drive penyimpanan untuk setiap node.

Amazon Redshift menawarkan berbagai jenis node untuk mengakomodasi beban kerja Anda, dan sebaiknya pilih RA3 atau DC2 tergantung pada kinerja yang diperlukan, ukuran data, dan pertumbuhan data yang diharapkan.

Node RA3 dengan penyimpanan terkelola memungkinkan Anda mengoptimalkan gudang data dengan menskalakan dan membayar komputasi dan penyimpanan terkelola secara independen. Dengan RA3, Anda memilih jumlah node berdasarkan persyaratan kinerja Anda dan hanya membayar penyimpanan terkelola yang Anda gunakan. Ukur cluster RA3 Anda berdasarkan jumlah data yang Anda proses setiap hari. Anda meluncurkan cluster yang menggunakan tipe node RA3 di virtual private cloud (VPC). Anda tidak dapat meluncurkan cluster RA3 di EC2-Classic. Untuk informasi selengkapnya, lihat [Membuat cluster di VPC](#).

Penyimpanan terkelola Amazon Redshift menggunakan SSD besar berkinerja tinggi di setiap node RA3 untuk penyimpanan lokal yang cepat dan Amazon S3 untuk penyimpanan tahan lama jangka panjang. Jika data dalam node tumbuh melampaui ukuran SSD lokal yang besar, penyimpanan terkelola Amazon Redshift secara otomatis membongkar data tersebut ke Amazon S3. Anda membayar tarif rendah yang sama untuk penyimpanan terkelola Amazon Redshift terlepas dari apakah data berada di SSD berkinerja tinggi atau Amazon S3. Untuk beban kerja yang membutuhkan

penyimpanan yang terus bertambah, penyimpanan terkelola memungkinkan Anda secara otomatis menskalakan kapasitas penyimpanan gudang data Anda terpisah dari node komputasi.

Node DC2 memungkinkan Anda memiliki gudang data intensif komputasi dengan penyimpanan SSD lokal yang disertakan. Anda memilih jumlah node yang Anda butuhkan berdasarkan ukuran data dan persyaratan kinerja. Node DC2 menyimpan data Anda secara lokal untuk kinerja tinggi, dan seiring bertambahnya ukuran data, Anda dapat menambahkan lebih banyak node komputasi untuk meningkatkan kapasitas penyimpanan cluster. Untuk kumpulan data di bawah 1 TB (terkompresi), kami merekomendasikan tipe node DC2 untuk kinerja terbaik dengan harga terendah. Jika Anda mengharapkan data Anda tumbuh, sebaiknya gunakan node RA3 sehingga Anda dapat mengukur komputasi dan penyimpanan secara independen untuk mencapai peningkatan harga dan kinerja. Anda meluncurkan cluster yang menggunakan tipe node DC2 di virtual private cloud (VPC). Anda tidak dapat meluncurkan cluster DC2 di EC2-Classic. Untuk informasi selengkapnya, lihat [Membuat cluster di VPC](#).

Jenis node tersedia dalam berbagai ukuran. Ukuran node dan jumlah node menentukan total penyimpanan untuk sebuah cluster. Untuk informasi selengkapnya, lihat [Rincian tipe simpul](#).

Beberapa jenis node memungkinkan satu node (single-node) atau dua atau lebih node (multi-node). Jumlah minimum node untuk cluster dari beberapa jenis node adalah dua node. Pada cluster simpul tunggal, node dibagikan untuk fungsionalitas pemimpin dan komputasi. Cluster simpul tunggal tidak direkomendasikan untuk menjalankan beban kerja produksi. Pada cluster multi-node, node pemimpin terpisah dari node komputasi. Node pemimpin adalah tipe node yang sama dengan node komputasi. Anda hanya membayar untuk node komputasi.

Amazon Redshift menerapkan kuota ke sumber daya untuk setiap AWS akun di setiap Wilayah. AWS Kuota membatasi jumlah sumber daya yang dapat dibuat akun Anda untuk jenis sumber daya tertentu, seperti node atau snapshot, di dalam Wilayah. AWS Untuk informasi selengkapnya tentang kuota default yang berlaku untuk resource Amazon Redshift, lihat Batas [Pergeseran Merah Amazon di](#). Referensi Umum Amazon Web Services Untuk meminta kenaikan, kirimkan Formulir [Peningkatan Batas Pergeseran Merah Amazon](#).

Biaya cluster Anda tergantung pada AWS Region, tipe node, jumlah node, dan apakah node dicadangkan terlebih dahulu. Untuk informasi selengkapnya tentang biaya node, lihat halaman [harga Amazon Redshift](#).

Rincian tipe simpul

Tabel berikut merangkum spesifikasi node untuk setiap jenis dan ukuran node. Judul dalam tabel memiliki arti ini:

- vCPU adalah jumlah CPU virtual untuk setiap node.
- RAM adalah jumlah memori dalam gibibytes (GiB) untuk setiap node.
- Irisan default per node adalah jumlah irisan di mana node komputasi dipartisi saat cluster dibuat atau diubah ukurannya dengan pengubahan ukuran klasik.

Jumlah irisan per node dapat berubah jika cluster diubah ukurannya menggunakan pengubahan ukuran elastis. Namun jumlah total irisan pada semua node komputasi di cluster tetap sama setelah mengubah ukuran elastis.

Saat Anda membuat cluster dengan operasi restore from snapshot, jumlah irisan cluster yang dihasilkan mungkin berubah dari cluster asli jika Anda mengubah jenis node.

- Penyimpanan adalah kapasitas dan jenis penyimpanan untuk setiap node.
- Rentang node adalah jumlah node minimum dan maksimum yang didukung Amazon Redshift untuk jenis dan ukuran node.

Note

Anda mungkin dibatasi untuk node yang lebih sedikit tergantung pada kuota yang diterapkan ke AWS akun Anda di AWS Wilayah yang dipilih. Untuk meminta kenaikan, kirimkan Formulir [Peningkatan Batas Pergeseran Merah Amazon](#).

- Kapasitas total adalah kapasitas penyimpanan total untuk cluster jika Anda menggunakan jumlah maksimum node yang ditentukan dalam rentang node.

Jenis simpul RA3

Jenis simpul	vCPU	RAM (GiB)	Irisan default per node	Batas penyimpanan terkelola per node ¹	Rentang node dengan create cluster	Total kapasitas penyimpanan terkelola ²
ra3.xlplu s (simpul tunggal)	4	32	2	4 TB	1	4 TB ³

Jenis simpul	vCPU	RAM (GiB)	Irisan default per node	Batas penyimpanan terkelola per node ¹	Rentang node dengan create cluster	Total kapasitas penyimpanan terkelola ²
ra3.xlplus (multi-node)	4	32	2	32 TB	2—16 ⁴	1024 TB ⁴
ra3.4xlarge	12	96	4	128 TB	2—32 ⁵	8192 TB ⁵
ra3.16xlarge	48	384	16	128 TB	2—128	16,384 TB

¹ Batas penyimpanan untuk penyimpanan terkelola Amazon Redshift. Ini adalah batas yang sulit.

² Total batas penyimpanan terkelola adalah jumlah maksimum node dikalikan batas penyimpanan terkelola per node.

³ Untuk mengubah ukuran cluster simpul tunggal menjadi multi-node, hanya pengubahan ukuran klasik yang didukung.

⁴ Anda dapat membuat cluster dengan tipe node ra3.xlplus (multi-node) yang memiliki hingga 16 node. Untuk cluster multi-node, Anda dapat mengubah ukuran dengan mengubah ukuran elastis hingga maksimum 32 node.

⁵ Anda dapat membuat cluster dengan tipe node ra3.4xlarge dengan hingga 32 node. Anda dapat mengubah ukurannya dengan mengubah ukuran elastis hingga maksimum 64 node.

Jenis node komputasi padat

Jenis simpul	vCPU	RAM (GiB)	Irisan default per node	Penyimpanan per node	Rentang simpul	Kapasitas total
dc2.large	2	15	2	160 GB NVME-SSD	1—32	5.12 TB

Jenis simpul	vCPU	RAM (GiB)	Irisan default per node	Penyimpanan per node	Rentang simpul	Kapasitas total
dc2.8xlarge	32	244	16	2,56 TB NVME-SSD	2—128	326 TB

Note

Jenis node penyimpanan padat (DS2) tidak lagi tersedia.

Nama tipe node sebelumnya

Dalam rilis Amazon Redshift sebelumnya, jenis node tertentu memiliki nama yang berbeda. Anda dapat menggunakan nama sebelumnya di Amazon Redshift API dan AWS CLI. Namun, kami menyarankan Anda memperbarui skrip apa pun yang mereferensikan nama-nama tersebut untuk menggunakan nama saat ini. Nama saat ini dan sebelumnya adalah sebagai berikut.

Nama saat ini	Nama sebelumnya
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

Menentukan jumlah node

Karena Amazon Redshift mendistribusikan dan menjalankan kueri secara paralel di semua node komputasi kluster, Anda dapat meningkatkan kinerja kueri dengan menambahkan node ke cluster

Anda. Ketika Anda menjalankan cluster dengan setidaknya dua node komputasi, data pada setiap node dicerminkan pada disk node lain untuk mengurangi risiko terjadinya kehilangan data.

Anda dapat memantau kinerja kueri di konsol Amazon Redshift dan dengan metrik Amazon CloudWatch . Anda juga dapat menambah atau menghapus node sesuai kebutuhan untuk mencapai keseimbangan antara harga dan kinerja untuk klaster Anda. Saat Anda meminta node tambahan, Amazon Redshift menangani semua detail penerapan, penyeimbangan beban, dan pemeliharaan data. Untuk informasi selengkapnya tentang kinerja klaster, lihat [Memantau kinerja klaster Amazon Redshift](#).

Node cadangan sesuai untuk beban kerja produksi kondisi mapan, dan menawarkan diskon signifikan atas node sesuai permintaan. Anda dapat membeli node cadangan setelah menjalankan eksperimen dan proof-of-concepts memvalidasi konfigurasi produksi Anda. Untuk informasi selengkapnya, lihat [Membeli node cadangan Amazon Redshift](#).

Saat menjeda klaster, Anda menanggihkan penagihan sesuai permintaan selama klaster dijeda. Selama waktu jeda ini, Anda hanya membayar untuk penyimpanan cadangan. Ini membebaskan Anda dari perencanaan dan pembelian kapasitas gudang data di depan kebutuhan Anda, dan memungkinkan Anda mengelola lingkungan secara hemat biaya untuk tujuan pengembangan atau pengujian.

Untuk informasi tentang harga node sesuai permintaan dan cadangan, lihat harga [Amazon Redshift](#).

Gunakan EC2-VPC saat Anda membuat cluster

Cluster Amazon Redshift berjalan di instans Amazon EC2 yang dikonfigurasi untuk jenis dan ukuran node Amazon Redshift yang Anda pilih. Buat cluster Anda menggunakan EC2-VPC. Jika Anda masih menggunakan EC2-Classic, kami sarankan Anda menggunakan EC2-VPC untuk mendapatkan peningkatan kinerja dan keamanan. Untuk informasi selengkapnya tentang platform jaringan ini, lihat [Platform yang Didukung](#) di Panduan Pengguna Amazon EC2. Pengaturan AWS akun Anda menentukan apakah EC2-VPC atau EC2-Classic tersedia untuk Anda.

Note

Untuk mencegah masalah koneksi antara alat klien SQL dan database Amazon Redshift, sebaiknya lakukan salah satu dari dua hal. Anda dapat mengonfigurasi aturan masuk yang memungkinkan host untuk menegosiasikan ukuran paket. Atau, Anda dapat menonaktifkan bingkai jumbo TCP/IP dengan mengatur unit transmisi maksimum (MTU) ke 1500 pada

antarmuka jaringan (NIC) instans Amazon EC2 Anda. Untuk informasi lebih lanjut tentang pendekatan ini, lihat [Kueri tampaknya hang dan terkadang gagal mencapai cluster](#).

EC2-VPC

Saat menggunakan EC2-VPC, cluster Anda berjalan di cloud pribadi virtual (VPC) yang secara logis diisolasi ke akun Anda. AWS Jika Anda menyediakan klaster di EC2-VPC, Anda mengontrol akses ke klaster dengan mengaitkan satu atau beberapa grup keamanan VPC dengan klaster. Untuk informasi selengkapnya, lihat [Grup Keamanan untuk VPC Anda](#) di Panduan Pengguna Amazon VPC.

Untuk membuat klaster di VPC, Anda harus terlebih dahulu membuat grup subnet klaster Amazon Redshift dengan memberikan informasi subnet VPC Anda, lalu berikan grup subnet saat meluncurkan cluster. Untuk informasi selengkapnya, lihat [Grup subnet klaster Amazon Redshift](#).

Untuk informasi selengkapnya tentang Amazon Virtual Private Cloud (Amazon VPC), lihat halaman detail [produk Amazon VPC](#).

Alarm ruang disk default

Saat membuat klaster Amazon Redshift, Anda dapat mengonfigurasi CloudWatch alarm Amazon secara opsional untuk memantau persentase rata-rata ruang disk yang digunakan di semua node di cluster Anda. Kami akan menyebut alarm ini sebagai alarm ruang disk default.

Tujuan dari alarm ruang disk default adalah untuk membantu Anda memantau kapasitas penyimpanan cluster Anda. Anda dapat mengonfigurasi alarm ini berdasarkan kebutuhan gudang data Anda. Misalnya, Anda dapat menggunakan peringatan sebagai indikator bahwa Anda mungkin perlu mengubah ukuran klaster Anda. Anda dapat mengubah ukuran ke jenis node yang berbeda atau menambahkan node, atau mungkin untuk membeli node cadangan untuk ekspansi masa depan.

Alarm ruang disk default dipicu ketika penggunaan disk mencapai atau melebihi persentase yang ditentukan untuk beberapa kali dan pada durasi tertentu. Secara default, alarm ini terpicu ketika persentase yang Anda tentukan tercapai, dan tetap pada atau di atas persentase itu selama lima menit atau lebih. Anda dapat mengedit nilai default setelah Anda meluncurkan cluster.

Saat CloudWatch alarm dipicu, Amazon Simple Notification Service (Amazon SNS) mengirimkan notifikasi ke penerima tertentu untuk memperingatkan mereka bahwa ambang batas persentase tercapai. Amazon SNS menggunakan topik untuk menentukan penerima dan pesan yang dikirim dalam pemberitahuan. Anda dapat menggunakan topik Amazon SNS yang ada; jika tidak, topik

dibuat berdasarkan pengaturan yang Anda tentukan saat meluncurkan kluster. Anda dapat mengedit topik untuk alarm ini setelah Anda meluncurkan cluster. Untuk informasi selengkapnya tentang membuat topik Amazon SNS, lihat [Memulai Layanan Pemberitahuan Sederhana Amazon](#).

Setelah Anda meluncurkan cluster, Anda dapat melihat dan mengedit alarm dari jendela Status cluster di bawah CloudWatch Alarm. **Namanya adalah `percentage-disk-space-used-default-< string >`**. Anda dapat membuka alarm untuk melihat topik Amazon SNS yang terkait dengannya dan mengedit pengaturan alarm. **Jika Anda tidak memilih topik Amazon SNS yang ada untuk digunakan, topik yang dibuat untuk Anda diberi nama `< clustername >-default-alarm (< receiver >)`; misalnya, `(notify@example.com). examplecluster-default-alarms`**

Untuk informasi selengkapnya tentang mengonfigurasi dan mengedit alarm ruang disk default, lihat [Membuat kluster](#) dan [Membuat atau mengedit alarm ruang disk](#).

Note

Jika Anda menghapus cluster Anda, alarm yang terkait dengan cluster tidak akan dihapus tetapi tidak akan memicu. Anda dapat menghapus alarm dari CloudWatch konsol jika Anda tidak lagi membutuhkannya.

Status kluster

Status cluster menampilkan status cluster saat ini. Tabel berikut memberikan deskripsi untuk setiap status cluster.

Status	Deskripsi
available	Cluster berjalan dan tersedia.
available, prep-for-resize	Cluster sedang dipersiapkan untuk mengubah ukuran elastis. Cluster berjalan dan tersedia untuk kueri baca dan tulis, tetapi operasi kluster, seperti membuat snapshot, tidak tersedia.
available, resize-cleanup	Operasi pengubahan ukuran elastis menyelesaikan transfer data ke node cluster baru. Cluster berjalan dan tersedia untuk kueri baca dan tulis, tetapi operasi kluster, seperti membuat snapshot, tidak tersedia.

Status	Deskripsi
cancelling-resize	Operasi perubahan ukuran sedang dibatalkan.
creating	Amazon Redshift membuat cluster. Untuk informasi selengkapnya, lihat Membuat klaster .
deleting	Amazon Redshift menghapus cluster. Untuk informasi selengkapnya, lihat Menghapus klaster .
final-snapshot	Amazon Redshift mengambil snapshot terakhir dari cluster sebelum menghapusnya. Untuk informasi selengkapnya, lihat Menghapus klaster .
hardware-failure	Cluster mengalami kegagalan perangkat keras. Jika Anda memiliki cluster simpul tunggal, simpul tidak dapat diganti. Untuk memulihkan klaster Anda, pulihkan snapshot. Untuk informasi selengkapnya, lihat Cuplikan dan cadangan Amazon Redshift .
incompatible-hsm	Amazon Redshift tidak dapat terhubung ke modul keamanan perangkat keras (HSM). Periksa konfigurasi HSM antara cluster dan HSM. Untuk informasi selengkapnya, lihat Enkripsi untuk Amazon Redshift menggunakan modul keamanan perangkat keras .
incompatible-network	Ada masalah dengan konfigurasi jaringan yang mendasarinya. Pastikan VPC tempat Anda meluncurkan cluster ada dan pengaturannya benar. Untuk informasi selengkapnya, lihat Mengelola cluster dalam VPC .
incompatible-parameters	Ada masalah dengan satu atau lebih nilai parameter dalam grup parameter terkait, dan nilai parameter atau nilai tidak dapat diterapkan. Ubah grup parameter dan perbarui nilai yang tidak valid. Untuk informasi selengkapnya, lihat Grup parameter Amazon Redshift .
incompatible-restore	Ada masalah saat memulihkan cluster dari snapshot. Coba pulihkan cluster lagi dengan snapshot yang berbeda. Untuk informasi selengkapnya, lihat Cuplikan dan cadangan Amazon Redshift .

Status	Deskripsi
modifying	Amazon Redshift menerapkan perubahan pada cluster. Untuk informasi selengkapnya, lihat Mengubah klaster .
paused	Cluster dijeda. Untuk informasi selengkapnya, lihat Menjeda dan melanjutkan cluster .
rebooting	Amazon Redshift me-reboot cluster. Untuk informasi selengkapnya, lihat Melakukan boot ulang klaster .
renaming	Amazon Redshift menerapkan nama baru ke cluster. Untuk informasi selengkapnya, lihat Mengganti nama cluster .
resizing	Amazon Redshift mengubah ukuran cluster. Untuk informasi selengkapnya, lihat Mengubah ukuran cluster .
rotating-keys	Amazon Redshift memutar kunci enkripsi untuk cluster. Untuk informasi selengkapnya, lihat Rotasi kunci enkripsi di Amazon Redshift .
storage-full	Cluster telah mencapai kapasitas penyimpanannya. Ubah ukuran cluster untuk menambahkan node atau untuk memilih ukuran node yang berbeda. Untuk informasi selengkapnya, lihat Mengubah ukuran cluster .
updating-hsm	Amazon Redshift memperbarui konfigurasi HSM.

Pertimbangan untuk menggunakan cluster yang disediakan Amazon Redshift

Setelah klaster dibuat, Anda dapat menemukan informasi di bagian ini tentang wilayah tempat fitur tersedia, tugas pemeliharaan, jenis node, dan batas penggunaan.

Topik

- [Pertimbangan Wilayah dan Availability Zone](#)
- [Pemeliharaan cluster](#)
- [Mengelola batas penggunaan di Amazon Redshift](#)
- [Fitur jaringan yang didukung oleh node RA3](#)

- [Jenis simpul](#)

Pertimbangan Wilayah dan Availability Zone

Amazon Redshift tersedia di beberapa AWS Wilayah. Secara default, Amazon Redshift menyediakan kluster Anda di Availability Zone (AZ) yang dipilih secara acak dalam AWS Wilayah yang Anda pilih. Semua node cluster disediakan di Availability Zone yang sama.

Anda dapat meminta Availability Zone tertentu secara opsional jika Amazon Redshift tersedia di zona tersebut. Misalnya, jika Anda sudah menjalankan instans Amazon EC2 di satu Availability Zone, Anda mungkin ingin membuat kluster Amazon Redshift di zona yang sama untuk mengurangi latensi. Di sisi lain, Anda mungkin ingin memilih Availability Zone lain untuk ketersediaan yang lebih tinggi. Amazon Redshift mungkin tidak tersedia di semua Availability Zone dalam suatu AWS Wilayah.

Untuk daftar AWS Wilayah yang didukung tempat Anda dapat menyediakan kluster Amazon Redshift, lihat titik akhir [Amazon Redshift di](#) bagian. Referensi Umum Amazon Web

Pemeliharaan cluster

Amazon Redshift secara berkala melakukan pemeliharaan untuk menerapkan peningkatan ke kluster Anda. Selama pembaruan ini, kluster Amazon Redshift Anda tidak tersedia untuk operasi normal. Anda memiliki beberapa cara untuk mengontrol cara kami mempertahankan kluster Anda. Misalnya, Anda dapat mengontrol kapan kami menerapkan pembaruan ke kluster Anda. Anda juga dapat memilih apakah kluster Anda menjalankan versi yang paling baru dirilis, atau versi yang dirilis sebelumnya ke versi yang paling baru dirilis. Terakhir, Anda memiliki opsi untuk menunda pembaruan pemeliharaan non-wajib untuk jangka waktu tertentu.

Topik

- [Jendela pemeliharaan](#)
- [Menunda pemeliharaan](#)
- [Memilih trek pemeliharaan cluster](#)
- [Mengelola versi cluster](#)
- [Menggulung kembali versi cluster](#)
- [Menentukan versi pemeliharaan cluster](#)

Jendela pemeliharaan

Amazon Redshift menetapkan jendela pemeliharaan 30 menit secara acak dari blok waktu 8 jam per AWS Wilayah, terjadi pada hari acak dalam seminggu (Senin hingga Minggu, inklusif).

Jendela pemeliharaan default

Daftar berikut menunjukkan blok waktu untuk setiap AWS Wilayah dari mana jendela pemeliharaan default ditetapkan:

- Wilayah AS Timur (Virginia N.): 03:00 - 11:00 UTC
- Wilayah AS Timur (Ohio): 03:00 - 11:00 UTC
- Wilayah AS Barat (California N.): 06:00 - 14:00 UTC
- Wilayah AS Barat (Oregon): 06:00 - 14:00 UTC
- Afrika (Cape Town) Wilayah: 20:00 - 04:00 UTC
- Wilayah Asia Pasifik (Hong Kong): 13:00 - 21:00 UTC
- Wilayah Asia Pasifik (Hyderabad): 16:30 — 00:30 UTC
- Wilayah Asia Pasifik (Jakarta): 15:00 - 23:00 UTC
- Wilayah Asia Pasifik (Melbourne): 12:00 - 20:00 UTC
- Wilayah Asia Pasifik (Mumbai): 16:30 — 00:30 UTC
- Wilayah Asia Pasifik (Osaka): 13:00 — 21:00 UTC
- Wilayah Asia Pasifik (Seoul): 13:00 - 21:00 UTC
- Wilayah Asia Pasifik (Singapura): 14:00 - 22:00 UTC
- Wilayah Asia Pasifik (Sydney): 12:00 - 20:00 UTC
- Wilayah Asia Pasifik (Tokyo): 13:00 — 21:00 UTC
- Kanada (Tengah) Wilayah: 03:00 - 11:00 UTC
- Kanada Wilayah Barat (Calgary): 04:00 - 12:00 UTC
- Wilayah China (Beijing): 13:00 — 21:00 UTC
- Wilayah China (Ningxia): 13:00 - 21:00 UTC
- Wilayah Eropa (Frankfurt): 06:00 - 14:00 UTC
- Wilayah Eropa (Irlandia): 22:00 - 06:00 UTC
- Wilayah Eropa (London): 22:00 - 06:00 UTC
- Wilayah Eropa (Milan): 21:00 - 05:00 UTC

- Wilayah Eropa (Paris): 23:00 - 07:00 UTC
- Wilayah Eropa (Stockholm): 23:00 - 07:00 UTC
- Wilayah Eropa (Zurich): 20:00 - 04:00 UTC
- Wilayah Israel (Tel Aviv): 20:00 — 04:00 UTC
- Wilayah Eropa (Spanyol): 21:00 - 05:00 UTC
- Wilayah Timur Tengah (Bahrain): 13:00 - 21:00 UTC
- Wilayah Timur Tengah (UEA): 18:00 - 02:00 UTC
- Wilayah Amerika Selatan (São Paulo): 19:00 - 03:00 UTC

Jika acara pemeliharaan dijadwalkan untuk minggu tertentu, itu dimulai selama jendela pemeliharaan 30 menit yang ditetapkan. Saat Amazon Redshift melakukan pemeliharaan, Amazon Redshift menghentikan kueri atau operasi lain yang sedang berlangsung. Sebagian besar pemeliharaan selesai selama jendela pemeliharaan 30 menit, tetapi beberapa tugas pemeliharaan mungkin terus berjalan setelah jendela ditutup. Jika tidak ada tugas pemeliharaan yang harus dilakukan selama jendela pemeliharaan terjadwal, kluster Anda akan terus beroperasi secara normal hingga jendela pemeliharaan terjadwal berikutnya.

Anda dapat mengubah jendela pemeliharaan terjadwal dengan memodifikasi cluster, baik secara terprogram atau dengan menggunakan konsol Amazon Redshift. Anda dapat menemukan jendela pemeliharaan dan mengatur hari dan waktu itu terjadi untuk cluster di bawah tab Maintenance.

Hal ini dimungkinkan untuk sebuah cluster untuk restart di luar jendela pemeliharaan. Ada beberapa alasan ini bisa terjadi. Satu lagi alasan umum adalah bahwa masalah telah terdeteksi dengan cluster dan operasi pemeliharaan sedang dilakukan untuk mengembalikannya ke keadaan sehat. Untuk informasi lebih lanjut, lihat artikel [Mengapa cluster Amazon Redshift saya reboot di luar jendela pemeliharaan?](#) , yang memberikan rincian tentang mengapa ini mungkin terjadi.

Menunda pemeliharaan

Untuk menjadwalkan ulang jendela pemeliharaan kluster Anda, Anda dapat menunda pemeliharaan hingga 45 hari. Misalnya, jika jendela pemeliharaan kluster Anda diatur ke Rabu 08:30 — 09:00 UTC dan Anda perlu mengakses cluster Anda pada saat itu, Anda dapat menunda pemeliharaan ke periode waktu berikutnya.

Jika Anda menunda pemeliharaan, Amazon Redshift akan tetap menerapkan pembaruan perangkat keras atau pembaruan keamanan wajib lainnya ke cluster Anda. Cluster Anda tidak tersedia selama pembaruan ini.

Jika pembaruan perangkat keras atau pembaruan keamanan wajib lainnya dijadwalkan selama jendela pemeliharaan yang akan datang, Amazon Redshift mengirimi Anda pemberitahuan terlebih dahulu di bawah kategori Tertunda. Untuk mempelajari lebih lanjut tentang Pemberitahuan acara Tertunda, lihat [Pemberitahuan acara Amazon Redshift](#).

Anda juga dapat memilih untuk menerima pemberitahuan acara dari Amazon Simple Notification Service (Amazon SNS). Untuk informasi selengkapnya tentang berlangganan notifikasi acara dari Amazon SNS, lihat [Berlangganan notifikasi acara kluster Amazon Redshift](#)

Jika Anda menunda pemeliharaan kluster Anda, jendela pemeliharaan setelah periode penundaan tidak dapat ditangguhkan.

Note

Anda tidak dapat menunda pemeliharaan setelah dimulai.

Untuk informasi selengkapnya tentang pemeliharaan kluster, lihat dokumentasi berikut:

- [Jendela pemeliharaan](#)
- [Mengelola cluster menggunakan konsol](#)
- [Mengubah kluster](#)

Memilih trek pemeliharaan cluster

Saat Amazon Redshift merilis versi cluster baru, kluster Anda diperbarui selama jendela pemeliharaannya. Anda dapat mengontrol apakah kluster Anda diperbarui ke rilis terbaru yang disetujui atau ke rilis sebelumnya.

Track pemeliharaan mengontrol versi cluster mana yang diterapkan selama jendela pemeliharaan. Saat Amazon Redshift merilis versi cluster baru, versi tersebut ditetapkan ke trek saat ini, dan versi sebelumnya ditetapkan ke trailing track. Untuk mengatur trek pemeliharaan untuk cluster, tentukan salah satu nilai berikut:

- Saat ini - Gunakan versi cluster yang disetujui terbaru.
- Trailing — Gunakan versi cluster sebelum versi saat ini.
- Pratinjau - Gunakan versi cluster yang berisi fitur baru yang tersedia untuk pratinjau.

Misalnya, misalkan klaster Anda saat ini menjalankan versi 1.0.2762 dan versi Amazon Redshift saat ini adalah 1.0.3072. Jika Anda menyetel nilai track pemeliharaan ke Current, klaster Anda diperbarui ke versi 1.0.3072 (rilis disetujui berikutnya) selama jendela pemeliharaan berikutnya. Jika Anda menyetel nilai track pemeliharaan ke Trailing, klaster Anda tidak diperbarui hingga ada rilis baru setelah 1.0.3072.

Pratinjau trek

Trek Pratinjau mungkin tidak selalu tersedia untuk dipilih. Saat Anda memilih trek Pratinjau, nama trek juga harus dipilih. Trek pratinjau dan sumber daya terkaitnya bersifat sementara, memiliki keterbatasan fungsional, dan mungkin tidak berisi semua fitur Amazon Redshift saat ini yang tersedia di trek lain. Saat bekerja dengan trek pratinjau:

- Gunakan konsol Amazon Redshift baru saat bekerja dengan trek pratinjau. Misalnya, saat Anda membuat cluster untuk digunakan dengan fitur pratinjau.
- Anda tidak dapat mengalihkan kluster dari satu trek pratinjau ke trek pratinjau lainnya.
- Anda tidak dapat mengalihkan kluster ke trek pratinjau dari trek saat ini atau trailing.
- Anda tidak dapat mengalihkan kluster dari trek pratinjau ke trek saat ini atau trailing.
- Anda tidak dapat memulihkan dari snapshot yang dibuat dari trek pratinjau yang berbeda.
- Anda hanya dapat menggunakan trek pratinjau saat membuat cluster baru, atau saat memulihkan dari snapshot.
- Anda tidak dapat memulihkan dari snapshot yang dibuat dari trek pratinjau yang berbeda, atau dengan versi pemeliharaan klaster yang lebih lambat dari versi klaster trek pratinjau. Misalnya, saat mengembalikan kluster ke trek pratinjau, Anda hanya dapat menggunakan snapshot yang dibuat dari versi pemeliharaan klaster sebelumnya daripada trek pratinjau.

Beralih di antara trek pemeliharaan

Mengubah trek untuk cluster umumnya merupakan keputusan satu kali. Anda harus berhati-hati dalam mengubah trek. Jika Anda mengubah trek pemeliharaan dari Trailing ke Current, kami akan memperbarui cluster ke versi rilis trek saat ini selama jendela pemeliharaan berikutnya. Namun, jika Anda mengubah trek pemeliharaan klaster menjadi Trailing, kami tidak akan memperbarui klaster Anda hingga ada rilis baru setelah versi rilis trek saat ini.

Trek pemeliharaan dan pemulihan

Sebuah snapshot mewarisi jalur pemeliharaan cluster sumber. Jika Anda mengubah trek pemeliharaan cluster sumber setelah mengambil snapshot, snapshot dan cluster sumber berada

di trek yang berbeda. Saat Anda memulihkan dari snapshot, cluster baru akan berada di jalur pemeliharaan yang diwarisi dari cluster sumber. Anda dapat mengubah jalur pemeliharaan setelah operasi pemulihan selesai. Mengubah ukuran cluster tidak memengaruhi jalur pemeliharaan cluster.

Mengelola versi cluster

Trek pemeliharaan adalah serangkaian rilis. Anda dapat memutuskan apakah klaster Anda berada di trek saat ini atau trek Trailing. Jika Anda menempatkan cluster Anda di trek saat ini, itu akan selalu ditingkatkan ke versi rilis cluster terbaru selama jendela pemeliharaannya. Jika Anda menempatkan cluster Anda di Trailing track, itu akan selalu menjalankan versi rilis cluster yang dirilis segera sebelum versi yang paling baru dirilis.

Kolom status rilis dalam daftar cluster konsol Amazon Redshift menunjukkan apakah salah satu cluster Anda tersedia untuk upgrade.

Menggulung kembali versi cluster

Jika cluster Anda up to date dengan versi cluster terbaru, Anda dapat memilih untuk memutar kembali ke versi sebelumnya.

Untuk informasi rinci tentang fitur dan peningkatan yang disertakan dengan setiap versi cluster, lihat [Riwayat versi cluster](#).

Untuk memutar kembali ke versi cluster sebelumnya

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster.
3. Pilih cluster untuk memutar kembali.
4. Untuk Tindakan, pilih Gulung kembali versi cluster. Halaman versi cluster Roll back muncul.
5. Jika ada versi yang tersedia untuk roll back, ikuti instruksi pada halaman.
6. Pilih Roll back sekarang.

Menentukan versi pemeliharaan cluster

Anda dapat menentukan mesin Amazon Redshift dan versi database dengan konsol Amazon Redshift.

Untuk menemukan versi cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, lalu pilih nama cluster dari daftar untuk membuka detailnya. Rincian cluster ditampilkan, yang dapat mencakup kinerja Cluster, pemantauan Kueri, Database, Datashares, Jadwal, Pemeliharaan, dan tab Properti.
3. Pilih tab Pemeliharaan untuk lebih jelasnya.
4. Di bagian Pemeliharaan, temukan Versi cluster saat ini.

Note

Meskipun konsol menampilkan informasi ini dalam satu bidang, ini adalah dua parameter di Amazon Redshift API, `ClusterVersion` dan `ClusterRevisionNumber` Untuk informasi selengkapnya, lihat [Cluster](#) di Referensi Amazon Redshift API.

Mengelola batas penggunaan di Amazon Redshift

Anda dapat menentukan batas untuk memantau dan mengontrol penggunaan dan biaya terkait beberapa fitur Amazon Redshift. Anda dapat membuat batas penggunaan harian, mingguan, dan bulanan, dan menentukan tindakan yang dilakukan secara otomatis Amazon Redshift jika batas tersebut tercapai. Tindakan mencakup hal-hal seperti penebangan acara ke tabel sistem untuk merekam penggunaan melebihi batas yang ditentukan Anda. Tindakan lain yang mungkin termasuk meningkatkan peringatan dengan Amazon SNS dan AmazonCloudWatch untuk memberi tahu administrator dan menonaktifkan penggunaan lebih lanjut untuk mengontrol biaya.

Anda dapat menentukan batas penggunaan untuk setiap cluster. Setelah klaster dibuat, Anda dapat menentukan batas penggunaan untuk fitur berikut:

- Amazon Redshift Spectrum
- Penskalakan Amazon Redshift
- Data Amazon Redshift

Batas penggunaan tersedia dengan versi rilis 1.0.14677 atau yang lebih baru di AWS Wilayah tempat Amazon Redshift Spectrum dan Amazon Redshift Concurrency Scaling tersedia.

Batas Redshift Spectrum menentukan ambang jumlah total data yang dipindai secara bertahap 1-TB. Batas skala konkurensi menentukan ambang jumlah total waktu yang digunakan oleh skala konkurensi dalam kenaikan 1 menit. Batas datasharing lintas wilayah menentukan ambang jumlah total data yang dipindai secara bertahap 1 TB.

Batas dapat ditentukan untuk periode harian, mingguan, atau bulanan (menggunakan UTC untuk menentukan awal dan akhir periode). Jika Anda membuat batas di tengah periode, maka batasnya diukur dari titik itu sampai akhir periode. Misalnya, jika Anda membuat batas bulanan pada 15 Maret, maka periode bulanan pertama diukur dari 15 Maret hingga 31 Maret.

Anda dapat menentukan beberapa batas penggunaan untuk setiap fitur. Setiap batas dapat memiliki tindakan yang berbeda. Tindakan yang mungkin termasuk yang berikut ini:

- Log ke tabel sistem— Ini adalah tindakan default. Informasi dicatat ke tabel `STL_USAGE_CONTROL`. Logging sangat membantu ketika mengevaluasi penggunaan masa lalu dan dalam menentukan batas penggunaan di masa mendatang. Untuk informasi selengkapnya tentang apa yang dicatat, lihat [STL_USAGE_CONTROL](#) di Panduan Pengembang Database Amazon Redshift.
- Pemberitahuan— Amazon Redshift CloudWatch metrik untuk penggunaan yang tersedia dan dikonsumsi. Anda dapat menentukan hingga tiga batas penggunaan untuk setiap fitur. Jika Anda mengaktifkan tindakan peringatan menggunakan konsol Amazon Redshift, a CloudWatch alarm secara otomatis dibuat pada metrik ini. Anda dapat secara opsional melampirkan langganan Amazon SNS ke alarm tersebut. Jika Anda menggunakan AWS CLI atau operasi API, pastikan bahwa Anda membuat CloudWatch alarm secara manual. Ketika ambang batas tercapai, peristiwa juga dicatat ke tabel sistem.
- Menonaktifkan fitur— Ketika ambang batas tercapai, Amazon Redshift menonaktifkan fitur hingga kuota disegarkan untuk periode waktu berikutnya (harian, mingguan, atau bulanan). Hanya satu batas untuk setiap fitur dapat memiliki tindakan menonaktifkan. Acara juga dicatat ke tabel sistem, dan peringatan dapat dipancarkan.

Batas penggunaan bertahan sampai definisi batas penggunaan itu sendiri atau klaster dihapus.

Anda dapat menentukan dan mengelola batas penggunaan dengan konsol Amazon Redshift baru, AWS CLI, atau dengan operasi Amazon Redshift API. Untuk menentukan batas pada konsol Amazon Redshift, navigasikan ke klaster Anda dan pilih Konfigurasi batas penggunaan untuk Tindakan. Untuk melihat batas penggunaan yang telah ditentukan sebelumnya untuk klaster Anda, arahkan ke klaster Anda, dan pilih Pemeliharaan tab, Batas penggunaan bagian.

Untuk melihat jumlah penggunaan yang tersedia dan dikonsumsi untuk kluster Anda, arahkan ke kluster Anda. Pilih Kinerja clustertab, lalu lihat grafik untuk penggunaan yang dikonsumsi untuk fitur.

Anda dapat menggunakan operasi Amazon Redshift untuk mengelola batas penggunaan. Untuk informasi selengkapnya, lihat Referensi Perintah AWS CLI.

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

Anda dapat menggunakan operasi Amazon Redshift untuk mengelola batas penggunaan. Untuk informasi selengkapnya, lihat Referensi Amazon Redshift.

- [CreateUsageBatasan](#)
- [DescribeUsageBatasan](#)
- [ModifyUsageBatasan](#)
- [DeleteUsageBatasan](#)

Tonton video berikut untuk mempelajari cara membuat dan memantau batas penggunaan menggunakan konsol Amazon Redshift: [Kontrol Biaya untuk Amazon Redshift Spectrum dan Concurrency Scaling](#).

Fitur jaringan yang didukung oleh node RA3

Node RA3 mendukung kumpulan fitur jaringan yang tidak tersedia untuk jenis node lainnya. Bagian ini memberikan deskripsi singkat dari setiap fitur dan tautan ke dokumentasi tambahan:

- Titik akhir VPC kluster yang disediakan — Saat Anda membuat atau memulihkan kluster RA3, Amazon Redshift menggunakan port dalam rentang 5431-5455 atau 8191-8215. Saat cluster disetel ke port di salah satu rentang ini, Amazon Redshift secara otomatis membuat titik akhir VPC di AWS akun Anda untuk cluster dan melampirkan alamat IP pribadi ke dalamnya. Jika Anda menyetel kluster agar dapat diakses publik, Redshift akan membuat alamat IP elastis di AWS akun Anda dan menempelkannya ke titik akhir VPC. Untuk informasi selengkapnya, lihat [Mengonfigurasi setelan komunikasi grup keamanan untuk kluster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server](#).

- Cluster RA3 subnet tunggal — Anda dapat membuat cluster RA3 dengan satu subnet, tetapi tidak dapat menggunakan fitur pemulihan bencana. Pengecualian terjadi jika Anda mengaktifkan relokasi klaster saat subnet tidak memiliki beberapa Availability Zones (AZ).
- Cluster RA3 multi-subnet dan grup subnet — Anda dapat membuat klaster RA3 dengan beberapa subnet dengan membuat grup subnet saat Anda menyediakan cluster di cloud pribadi virtual (VPC) Anda. Grup subnet cluster memungkinkan Anda menentukan satu set subnet di VPC Anda dan Amazon Redshift membuat cluster di salah satunya. Setelah membuat grup subnet, Anda dapat menghapus subnet yang sebelumnya Anda tambahkan, atau menambahkan lebih banyak. Untuk informasi selengkapnya, lihat [grup subnet klaster Amazon Redshift](#).
- Akses lintas-akun atau lintas titik akhir VPC — Anda dapat mengakses klaster yang disediakan atau grup kerja Tanpa Server Amazon Redshift dengan menyiapkan titik akhir VPC yang dikelola RedShift. Anda dapat mengaturnya sebagai koneksi pribadi antara VPC yang berisi cluster atau workgroup dan VPC tempat Anda menjalankan alat klien, misalnya. Dengan melakukan ini, Anda dapat mengakses gudang data tanpa menggunakan alamat IP publik dan tanpa merutekan lalu lintas melalui internet. Untuk informasi selengkapnya, lihat [Bekerja dengan titik akhir VPC yang dikelola RedShift](#).
- Relokasi cluster — Anda dapat memindahkan cluster ke Availability Zone (AZ) lain tanpa kehilangan data ketika ada gangguan layanan. Anda mengaktifkannya di konsol. Untuk informasi selengkapnya, lihat [Merelokasi klaster Anda](#).
- Nama domain khusus - Anda dapat membuat nama domain khusus, juga dikenal sebagai URL khusus, untuk klaster Amazon Redshift Anda. Ini adalah catatan easy-to-read DNS yang merutekan koneksi SQL-client ke endpoint cluster Anda. Untuk informasi selengkapnya, lihat [Menggunakan nama domain khusus untuk koneksi klien](#).

Jenis simpul

Bagian ini merinci tugas yang tersedia untuk berbagai jenis node.

Topik

- [Node RA3](#)
- [Jenis simpul DC2](#)

Node RA3

Bagian ini merinci tugas yang tersedia untuk node RA3.

Topik

- [Gambaran Umum](#)
- [Memutakhirkan ke tipe node RA3](#)

Gambaran Umum

Node RA3 memberikan keuntungan sebagai berikut:

- Mereka fleksibel untuk menumbuhkan kapasitas komputasi Anda tanpa meningkatkan biaya penyimpanan Anda. Dan mereka menskalakan penyimpanan Anda tanpa menyediakan kapasitas komputasi yang berlebihan.
- Mereka menggunakan SSD berkinerja tinggi untuk data panas Anda dan Amazon S3 untuk data dingin. Dengan demikian mereka memberikan kemudahan penggunaan, penyimpanan hemat biaya, dan kinerja kueri yang tinggi.
- Mereka menggunakan jaringan bandwidth tinggi yang dibangun di atas Sistem AWS Nitro untuk lebih mengurangi waktu yang dibutuhkan untuk data yang akan diturunkan dan diambil dari Amazon S3.

Pertimbangkan untuk memilih tipe node RA3 dalam kasus ini:

- Anda memerlukan fleksibilitas untuk menskalakan dan membayar komputasi terpisah dari penyimpanan.
- Anda menanyakan sebagian kecil dari total data Anda.
- Volume data Anda berkembang pesat atau diperkirakan akan tumbuh dengan cepat.
- Anda menginginkan fleksibilitas untuk mengukur cluster hanya berdasarkan kebutuhan kinerja Anda.

Untuk menggunakan tipe node RA3, AWS Wilayah Anda harus mendukung RA3. Untuk informasi selengkapnya, lihat [Ketersediaan tipe node RA3 di Wilayah AWS](#).

Important

Anda dapat menggunakan tipe node ra3.xlplus hanya dengan versi cluster 1.0.21262 atau yang lebih baru. Anda dapat melihat versi cluster yang ada dengan konsol Amazon Redshift. Untuk informasi selengkapnya, lihat [Menentukan versi pemeliharaan cluster](#).

Pastikan Anda menggunakan konsol Amazon Redshift baru saat bekerja dengan tipe node RA3.

Selain itu, untuk menggunakan tipe node RA3 dengan operasi Amazon Redshift yang menggunakan jalur pemeliharaan, nilai track pemeliharaan harus disetel ke versi cluster yang mendukung RA3. Untuk informasi selengkapnya tentang trek pemeliharaan, lihat [Memilih trek pemeliharaan cluster](#).

Pertimbangkan hal berikut saat menggunakan tipe node RA3 simpul tunggal.

- Produsen dan konsumen Datasharing didukung.
- Untuk mengubah tipe node, hanya perubahan ukuran klasik yang didukung. Mengubah tipe node dengan perubahan ukuran elastis atau pemulihan snapshot tidak didukung. Skenario berikut didukung:
 - Perubahan ukuran klasik dari 1-node dc2.xlarge menjadi 1-node ra3.xlplus, dan sebaliknya.
 - Perubahan ukuran klasik dari 1-node dc2.xlarge menjadi multiple-node ra3.xlplus, dan sebaliknya.
 - Perubahan ukuran klasik dari multiple-node dc2.xlarge menjadi 1-node ra3.xlplus, dan sebaliknya.

Bekerja dengan penyimpanan terkelola Amazon Redshift

Dengan penyimpanan terkelola Amazon Redshift, Anda dapat menyimpan dan memproses semua data di Amazon Redshift sambil mendapatkan lebih banyak fleksibilitas untuk menskalakan kapasitas komputasi dan penyimpanan secara terpisah. Anda terus menelan data dengan perintah COPY atau INSERT. Untuk mengoptimalkan kinerja dan mengelola penempatan data otomatis di seluruh tingkatan penyimpanan, Amazon Redshift memanfaatkan pengoptimalan seperti suhu blok data, usia blok data, dan pola beban kerja. Bila diperlukan, Amazon Redshift menskalakan penyimpanan secara otomatis ke Amazon S3 tanpa memerlukan tindakan manual apa pun.

Untuk informasi tentang biaya penyimpanan, lihat [harga Amazon Redshift](#).

Mengelola tipe node RA3

Untuk memanfaatkan pemisahan komputasi dari penyimpanan, Anda dapat membuat atau memutakhirkan cluster Anda dengan tipe node RA3. Untuk menggunakan tipe node RA3, buat cluster Anda di cloud pribadi virtual (EC2-VPC).

Untuk mengubah jumlah node cluster Amazon Redshift dengan tipe node RA3, lakukan salah satu hal berikut:

- Tambahkan atau hapus node dengan operasi pengubahan ukuran elastis. Dalam beberapa situasi, menghapus node dari cluster RA3 tidak diperbolehkan dengan pengubahan ukuran elastis. Misalnya, ketika peningkatan jumlah node 2:1 menempatkan jumlah irisan per node pada 32. Untuk informasi selengkapnya, lihat [Mengubah ukuran cluster](#). Jika pengubahan ukuran elastis tidak tersedia, gunakan pengubahan ukuran klasik.
- Tambahkan atau hapus node dengan operasi pengubahan ukuran klasik. Pilih opsi ini saat Anda mengubah ukuran ke konfigurasi yang tidak tersedia melalui pengubahan ukuran elastis. Pengubahan ukuran elastis lebih cepat daripada pengubahan ukuran klasik. Untuk informasi selengkapnya, lihat [Mengubah ukuran cluster](#).

Ketersediaan tipe node RA3 di Wilayah AWS

Jenis node RA3 hanya tersedia di AWS Wilayah berikut:

- Wilayah AS Timur (Virginia N.) (us-east-1)
- Wilayah AS Timur (Ohio) (us-east-2)
- Wilayah AS Barat (California N.) (us-west-1)
- Wilayah AS Barat (Oregon) (us-west-2)
- Wilayah Afrika (Cape Town) (af-south-1)
- Wilayah Asia Pasifik (Hong Kong) (ap-east-1)
- Wilayah Asia Pasifik (Hyderabad) (ap-south-2)
- Wilayah Asia Pasifik (Jakarta) (ap-southeast-3)
- Wilayah Asia Pasifik (Melbourne) (ap-southeast-4)
- Wilayah Asia Pasifik (Mumbai) (ap-south-1)
- Wilayah Asia Pasifik (Osaka) (ap-northeast-3)
- Wilayah Asia Pasifik (Seoul) (ap-northeast-2)
- Wilayah Asia Pasifik (Singapura) (ap-southeast-1)
- Wilayah Asia Pasifik (Sydney) (ap-southeast-2)
- Wilayah Asia Pasifik (Tokyo) (ap-northeast-1)
- Wilayah Kanada (Tengah) (ca-central-1)

- Wilayah Kanada Barat (Calgary) (ca-west-1)
- Wilayah China (Beijing) (cn-utara-1)
- Wilayah China (Ningxia) (cn-barat laut-1)
- Wilayah Eropa (Frankfurt) (eu-central-1)
- Wilayah Eropa (Zurich) (eu-central-2)
- Wilayah Eropa (Irlandia) (eu-west-1)
- Wilayah Eropa (London) (eu-west-2)
- Wilayah Eropa (Milan) (eu-south-1)
- Wilayah Eropa (Spanyol) (eu-south-2)
- Wilayah Eropa (Paris) (eu-west-3)
- Wilayah Eropa (Stockholm) (eu-north-1)
- Wilayah Israel (Tel Aviv) (il-central-1)
- Wilayah Timur Tengah (Bahrain) (me-south-1)
- Wilayah Timur Tengah (UEA) (me-central-1)
- Wilayah Amerika Selatan (São Paulo) (sa-east-1)
- AWS GovCloud (AS-Timur) (kami-gov-timur-1)
- AWS GovCloud (AS-barat) (kami-gov-barat-1)

Memutakhirkan ke tipe node RA3

Untuk memutakhirkan tipe node yang ada ke RA3, Anda memiliki opsi berikut untuk mengubah jenis node:

- Pulihkan dari snapshot — Amazon Redshift menggunakan snapshot terbaru dari cluster Anda dan mengembalikannya untuk membuat cluster RA3 baru. Segera setelah pembuatan cluster selesai (biasanya dalam beberapa menit), node RA3 siap menjalankan beban kerja produksi penuh Anda. Karena komputasi terpisah dari penyimpanan, data panas dibawa ke cache lokal dengan kecepatan cepat berkat bandwidth jaringan yang besar. Jika Anda memulihkan dari snapshot DC2 terbaru, RA3 menyimpan informasi blok panas dari beban kerja DC2 dan mengisi cache lokalnya dengan blok terpanas. Untuk informasi selengkapnya, lihat [Memulihkan cluster dari snapshot](#).

Untuk menjaga endpoint yang sama untuk aplikasi dan pengguna Anda, Anda dapat mengganti nama cluster RA3 baru dengan nama yang sama dengan cluster DC2 asli. Untuk mengganti

nama cluster, ubah cluster di konsol Amazon Redshift ModifyCluster atau operasi API. Untuk informasi selengkapnya, lihat [Mengganti nama cluster](#) atau [operasi ModifyCluster API](#) di Referensi Amazon Redshift API.

- Ubah ukuran elastis — mengubah ukuran cluster menggunakan perubahan ukuran elastis. Saat Anda menggunakan perubahan ukuran elastis untuk mengubah jenis node, Amazon Redshift secara otomatis membuat snapshot, membuat cluster baru, menghapus klaster lama, dan mengganti nama cluster baru. Operasi perubahan ukuran elastis dapat dijalankan sesuai permintaan atau dapat dijadwalkan untuk berjalan di masa mendatang. Anda dapat dengan cepat memutakhirkan cluster tipe node DC2 yang ada ke RA3 dengan perubahan ukuran elastis. Untuk informasi selengkapnya, lihat [Ubah ukuran elastis](#).

Tabel berikut menunjukkan rekomendasi saat memutakhirkan ke tipe node RA3. (Rekomendasi ini juga berlaku untuk node yang dicadangkan.)

Rekomendasi dalam tabel ini adalah memulai jenis dan ukuran node cluster tetapi bergantung pada persyaratan komputasi beban kerja Anda. Untuk memperkirakan kebutuhan Anda dengan lebih baik, pertimbangkan untuk melakukan bukti konsep (POC) yang menggunakan [Test Drive](#) untuk menjalankan konfigurasi potensial. Menyediakan cluster untuk gudang data POC Anda alih-alih Redshift Serverless. Untuk informasi selengkapnya tentang melakukan pembuktian konsep, lihat [Melakukan bukti konsep \(POC\) untuk Amazon Redshift](#) di Panduan Pengembang Basis Data Amazon Redshift.

Jenis node yang ada	Jumlah node yang ada	Jenis node baru yang direkomen dasikan	Upgrade tindakan
dc2.8xlarge	2—15	ra3.4xlarge	Buat 2 node ra3.4xlarge untuk setiap 1 node dc2.8xlarge 1.
dc2.8xlarge	16—128	ra3.16xlarge	Buat 1 node ra3.16xlarge untuk setiap 2 node dc2.8xlarge 1.
dc2.large	1—4	none	Simpan cluster dc2.large yang ada.

Jenis node yang ada	Jumlah node yang ada	Jenis node baru yang direkomen dasikan	Upgrade tindakan
dc2.large	5—15	ra3.xlplus	Buat 3 node ra3.xlplus untuk setiap 8 node dc2.large 1.
dc2.large	16—32	ra3.4xlarge	Buat 1 node ra3.4xlarge untuk setiap 8 node dc2.large 1, 2.

¹ Node tambahan mungkin diperlukan tergantung pada persyaratan beban kerja. Menambahkan atau menghapus node berdasarkan persyaratan komputasi dari kinerja kueri yang Anda butuhkan.

² Cluster dengan tipe node dc2.large dibatasi hingga 32 node.

Jumlah minimum node untuk beberapa tipe node RA3 adalah 2 node. Pertimbangkan hal ini saat membuat cluster RA3.

Jenis simpul DC2

Bagian ini merinci tugas yang tersedia untuk tipe node DC2.

Operasi cluster

Setelah cluster Anda dibuat, ada beberapa operasi yang dapat Anda lakukan di atasnya. Operasi termasuk mengubah ukuran, menjeda, melanjutkan, mengganti nama, dan menghapus.

Topik

- [Mengubah ukuran cluster](#)
- [Menjeda dan melanjutkan cluster](#)
- [Mengganti nama cluster](#)
- [Mematikan dan menghapus cluster](#)
- [Merelokasi klaster Anda](#)
- [Cuplikan dan cadangan Amazon Redshift](#)

Mengubah ukuran cluster

Karena kapasitas dan kinerja pergudangan data Anda perlu berubah, Anda dapat mengubah ukuran kluster Anda untuk memanfaatkan opsi komputasi dan penyimpanan Amazon Redshift sebaik mungkin.

Operasi pengubahan ukuran datang dalam dua jenis:

- **Ubah ukuran elastis** — Anda dapat menambahkan node ke atau menghapus node dari cluster Anda. Anda juga dapat mengubah jenis node, seperti dari node DC2 ke node RA3. Pengubahan ukuran elastis biasanya selesai dengan cepat, rata-rata memakan waktu sepuluh menit. Untuk alasan ini, kami merekomendasikannya sebagai opsi pertama. Ketika Anda melakukan pengubahan ukuran elastis, itu mendistribusikan ulang irisan data, yang merupakan partisi yang dialokasikan memori dan ruang disk di setiap node. Pengubahan ukuran elastis sesuai saat Anda:
 - Tambahkan atau kurangi node di cluster yang ada, tetapi Anda tidak mengubah jenis node — Ini biasa disebut pengubahan ukuran di tempat. Saat Anda melakukan jenis pengubahan ukuran ini, beberapa kueri yang berjalan berhasil diselesaikan, tetapi yang lain dapat dihapus sebagai bagian dari operasi.
 - Ubah tipe node untuk cluster — Saat Anda mengubah tipe node, snapshot dibuat dan data didistribusikan kembali dari cluster sumber ke cluster yang terdiri dari tipe node baru. Setelah selesai, kueri yang sedang berjalan dijatuhkan. Seperti pengubahan ukuran di tempat, itu selesai dengan cepat.
- **Pengubahan ukuran klasik** - Anda dapat mengubah jenis node, jumlah node, atau keduanya, dengan cara yang mirip dengan pengubahan ukuran elastis. Pengubahan ukuran klasik membutuhkan lebih banyak waktu untuk diselesaikan, tetapi ini dapat berguna dalam kasus di mana perubahan jumlah node atau tipe node yang akan dimigrasi tidak termasuk dalam batas untuk mengubah ukuran elastis. Ini dapat diterapkan, misalnya, ketika perubahan jumlah node sangat besar.

Topik

- [Ubah ukuran elastis](#)
- [Ubah ukuran klasik](#)

Ubah ukuran elastis

Operasi pengubahan ukuran elastis, ketika Anda menambah atau menghapus node dari jenis yang sama, memiliki tahapan berikut:

1. Pengubahan ukuran elastis membutuhkan snapshot cluster. Snapshot ini selalu menyertakan [tabel tanpa cadangan](#) untuk node yang berlaku. (Beberapa tipe node, seperti RA3, tidak memiliki tabel tanpa cadangan.) Jika kluster Anda tidak memiliki snapshot terbaru, karena Anda menonaktifkan snapshot otomatis, operasi pencadangan dapat memakan waktu lebih lama. (Untuk meminimalkan waktu sebelum operasi pengubahan ukuran dimulai, kami sarankan Anda mengaktifkan snapshot otomatis atau membuat snapshot manual sebelum memulai pengubahan ukuran.) Saat Anda memulai pengubahan ukuran elastis dan operasi snapshot sedang berlangsung, pengubahan ukuran dapat gagal jika operasi snapshot tidak selesai dalam beberapa menit. Untuk informasi selengkapnya, lihat [Cuplikan dan cadangan Amazon Redshift](#).
2. Operasi memigrasikan metadata cluster. Cluster tidak tersedia selama beberapa menit. Mayoritas kueri dijeda sementara dan koneksi tetap terbuka. Ada kemungkinan, bagaimanapun, untuk beberapa kueri yang akan dihapus. Tahap ini singkat.
3. Koneksi sesi dipulihkan dan kueri dilanjutkan.
4. Pengubahan ukuran elastis mendistribusikan kembali data ke irisan simpul, di latar belakang. Cluster tersedia untuk operasi baca dan tulis, tetapi beberapa kueri dapat memakan waktu lebih lama untuk dijalankan.
5. Setelah operasi selesai, Amazon Redshift mengirimkan pemberitahuan acara.

Saat Anda menggunakan pengubahan ukuran elastis untuk mengubah tipe node, ia bekerja sama dengan saat Anda menambahkan atau mengurangi node dari tipe yang sama. Pertama, snapshot dibuat. Kluster target baru disediakan dengan data terbaru dari snapshot, dan data ditransfer ke cluster baru di latar belakang. Selama periode ini, data hanya dibaca. Saat pengubahan ukuran hampir selesai, Amazon Redshift memperbarui titik akhir untuk menunjuk ke cluster baru dan semua koneksi ke cluster sumber dihapus.

Tidak mungkin pengubahan ukuran elastis akan gagal. Namun, dalam kasus kegagalan, rollback terjadi secara otomatis di sebagian besar kasus tanpa memerlukan intervensi manual.

Jika Anda memiliki node cadangan, misalnya node cadangan DC2, Anda dapat meningkatkan ke node cadangan RA3 saat Anda melakukan pengubahan ukuran. Anda dapat melakukan ini ketika Anda melakukan pengubahan ukuran elastis atau menggunakan konsol untuk memulihkan

dari snapshot. Konsol memandu Anda melalui proses ini. Untuk informasi selengkapnya tentang memutakhirkan ke node RA3, lihat [Memutakhirkan ke tipe node RA3](#).

Pengubahan ukuran elastis tidak mengurutkan tabel atau merebut kembali ruang disk, jadi ini bukan pengganti operasi vakum. Untuk informasi lebih lanjut, lihat tabel [Menyedot debu](#).

Ubah ukuran elastis memiliki kendala berikut:

- Kluster pengubahan ukuran dan berbagi data yang elastis - Saat menambahkan atau mengurangi node pada klaster yang merupakan produsen untuk berbagi data, Anda tidak dapat menghubungkannya dari konsumen saat Amazon Redshift memigrasikan metadata klaster. Demikian pula, jika Anda melakukan pengubahan ukuran elastis dan memilih tipe node baru, berbagi data tidak tersedia saat koneksi dijatuhkan dan ditransfer ke cluster target baru. Dalam kedua jenis pengubahan ukuran elastis, produsen tidak tersedia selama beberapa menit.
- Transfer data dari snapshot bersama - Untuk menjalankan pengubahan ukuran elastis pada klaster yang mentransfer data dari snapshot bersama, setidaknya satu cadangan harus tersedia untuk klaster. Anda dapat melihat cadangan di daftar snapshot konsol Amazon Redshift, perintah `describe-cluster-snapshots` CLI, atau operasi API. `DescribeClusterSnapshots`
- Pembatasan platform - Pengubahan ukuran elastis hanya tersedia untuk cluster yang menggunakan platform EC2-VPC. Untuk informasi selengkapnya, lihat [Gunakan EC2-VPC saat Anda membuat cluster](#).
- Pertimbangan penyimpanan - Pastikan konfigurasi node baru Anda memiliki penyimpanan yang cukup untuk data yang ada. Anda mungkin harus menambahkan node tambahan atau mengubah konfigurasi.
- Ukuran cluster sumber vs target - Jumlah node dan tipe node yang dapat diubah ukurannya dengan pengubahan ukuran elastis ditentukan oleh jumlah node di cluster sumber dan tipe node yang dipilih untuk cluster yang diubah ukurannya. Untuk menentukan kemungkinan konfigurasi yang tersedia, Anda dapat menggunakan konsol. Atau Anda dapat menggunakan `describe-node-configuration-options` AWS CLI perintah dengan `action-type resize-cluster` opsi. Untuk informasi selengkapnya tentang mengubah ukuran menggunakan konsol Amazon Redshift, lihat. [Mengubah ukuran cluster](#)

Contoh perintah CLI berikut menjelaskan opsi konfigurasi yang tersedia. Dalam contoh ini, cluster bernama `mycluster` adalah cluster `dc2.large 8-node`.

```
aws redshift describe-node-configuration-options --cluster-identifier mycluster --  
region eu-west-1 --action-type resize-cluster
```

Perintah ini mengembalikan daftar opsi dengan jenis node yang direkomendasikan, jumlah node, dan pemanfaatan disk untuk setiap opsi. Konfigurasi yang dikembalikan dapat bervariasi berdasarkan cluster input tertentu. Anda dapat memilih salah satu konfigurasi yang dikembalikan saat Anda menentukan opsi perintah `resize-cluster` CLI.

- Langit-langit pada node tambahan - Ubah ukuran elastis memiliki batas pada node yang dapat Anda tambahkan ke cluster. Misalnya, cluster `dc2` mendukung pengubahan ukuran elastis hingga menggandakan jumlah node. Untuk mengilustrasikan, Anda dapat menambahkan node ke cluster `dc2.8xlarge` 4-node untuk menjadikannya cluster lima simpul, atau menambahkan lebih banyak node hingga Anda mencapai delapan.

Note

Batas pertumbuhan dan pengurangan didasarkan pada jenis node asli dan jumlah node di cluster asli atau ukuran klasik terakhirnya. Jika pengubahan ukuran elastis akan melebihi batas pertumbuhan atau pengurangan, gunakan pengubahan ukuran klasik.

Dengan beberapa tipe node `ra3`, Anda dapat meningkatkan jumlah node hingga empat kali jumlah yang ada. Secara khusus, anggaplah cluster Anda terdiri dari node `ra3.4xlarge` atau `ra3.16xlarge`. Anda kemudian dapat menggunakan pengubahan ukuran elastis untuk meningkatkan jumlah node dalam cluster 8-node menjadi 32. Atau Anda dapat memilih nilai di bawah batas. (Perlu diingat bahwa kemampuan untuk menumbuhkan cluster sebesar 4x tergantung pada ukuran cluster sumber.) Jika cluster Anda memiliki node `ra3.xlplus`, batasnya dua kali lipat.

Semua tipe node `ra3` mendukung penurunan jumlah node menjadi seperempat dari jumlah yang ada. Misalnya, Anda dapat mengurangi ukuran cluster dengan node `ra3.4xlarge` dari 12 node menjadi 3, atau ke angka di atas minimum.

Tabel berikut mencantumkan batas pertumbuhan dan pengurangan untuk setiap jenis node yang mendukung pengubahan ukuran elastis.

Jenis simpul asli	Batas pertumbuhan	Batas pengurangan
<code>ra3.16xlarge</code>	4x (dari 4 hingga 16 node, misalnya)	Untuk seperempat dari jumlah (dari 16 hingga 4 node, misalnya)

Jenis simpul asli	Batas pertumbuhan	Batas pengurangan
ra3.4xlarge	4x	Untuk seperempat dari jumlah
ra3.xplus	2x (dari 4 hingga 8 node, misalnya)	Untuk seperempat dari jumlah
dc2.8xlarge	2x	Untuk setengah dari jumlah (dari 16 hingga 8 node, misalnya)
dc2.large	2x	Setengah dari jumlah

Note

Memilih tipe node lama saat Anda mengubah ukuran cluster RA3 — Jika Anda mencoba mengubah ukuran dari cluster dengan node RA3 ke tipe node lain, seperti DC2, pesan peringatan validasi akan muncul di konsol, dan operasi pengubahan ukuran tidak akan selesai. Ini terjadi karena mengubah ukuran ke tipe node lama tidak didukung. Ini untuk mencegah pelanggan mengubah ukuran ke jenis node yang tidak digunakan lagi atau segera tidak digunakan lagi. Ini berlaku untuk pengubahan ukuran elastis dan pengubahan ukuran klasik.

Ubah ukuran klasik

Pengubahan ukuran klasik menangani kasus penggunaan di mana perubahan ukuran cluster atau tipe node tidak didukung oleh pengubahan ukuran elastis. Saat Anda melakukan pengubahan ukuran klasik, Amazon Redshift membuat klaster target dan memigrasikan data dan metadata Anda ke klaster sumber.

Pengubahan ukuran klasik ke RA3 dapat memberikan ketersediaan yang lebih baik

Pengubahan ukuran klasik telah ditingkatkan ketika tipe node target adalah RA3. Hal ini dilakukan dengan menggunakan backup dan restore operasi antara sumber dan target cluster. Ketika pengubahan ukuran dimulai, cluster sumber dimulai ulang dan tidak tersedia selama beberapa menit. Setelah itu, cluster tersedia untuk operasi baca dan tulis sementara pengubahan ukuran berlanjut di latar belakang.

Memeriksa cluster Anda

Untuk memastikan Anda memiliki kinerja dan hasil terbaik saat Anda melakukan perubahan ukuran klasik ke cluster RA3, lengkapi daftar periksa ini. Ketika Anda tidak mengikuti daftar periksa, Anda mungkin tidak mendapatkan beberapa manfaat dari mengubah ukuran klasik dengan node RA3, seperti kemampuan untuk melakukan operasi baca dan tulis.

1. Ukuran data harus di bawah 2 petabyte. (Satu petabyte sama dengan 1.000 terabyte.) Untuk memvalidasi ukuran data Anda, buat snapshot dan periksa ukurannya. Anda juga dapat menjalankan kueri berikut untuk memeriksa ukurannya:

```
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;
```

svv_table_infoTabel hanya terlihat oleh pengguna super.

2. Sebelum Anda memulai perubahan ukuran klasik, pastikan Anda memiliki snapshot manual yang tidak lebih dari 10 jam. Jika tidak, ambil snapshot.
3. Snapshot yang digunakan untuk melakukan perubahan ukuran klasik tidak dapat digunakan untuk pemulihan tabel atau tujuan lain.
4. Cluster harus dalam VPC.

Operasi penyortiran dan distribusi yang dihasilkan dari perubahan ukuran klasik ke RA3

Selama perubahan ukuran klasik ke RA3, tabel dengan distribusi KEY yang dimigrasikan sebagai distribusi EVEN dikonversi kembali ke gaya distribusi aslinya. Durasi ini tergantung pada ukuran data dan seberapa sibuk cluster Anda. Beban kerja kueri diberikan prioritas yang lebih tinggi untuk menjalankan migrasi data. Untuk informasi selengkapnya, lihat [Gaya distribusi](#). Baik membaca dan menulis ke database bekerja selama proses migrasi ini, tetapi dapat memakan waktu lebih lama untuk menyelesaikan kueri. Namun, penskalaan konkurensi dapat meningkatkan kinerja selama waktu ini dengan menambahkan sumber daya untuk beban kerja kueri. [Anda dapat melihat kemajuan migrasi data dengan melihat hasil dari tampilan SYS_RESTORE_STATE dan SYS_RESTORE_LOG.](#) Informasi lebih lanjut tentang pemantauan berikut.

Setelah cluster diubah ukurannya sepenuhnya, perilaku pengurutan berikut terjadi:

- Jika pengubahan ukuran menghasilkan cluster yang memiliki lebih banyak irisan, tabel distribusi KEY menjadi sebagian tidak disortir, tetapi tabel EVEN tetap diurutkan. Selain itu, informasi tentang berapa banyak data yang diurutkan mungkin tidak mutakhir, langsung mengikuti pengubahan ukuran. Setelah pemulihan kunci, vakum otomatis menyortir tabel dari waktu ke waktu.
- Jika pengubahan ukuran menghasilkan cluster yang memiliki irisan lebih sedikit, distribusi KEY dan tabel distribusi EVEN menjadi sebagian tidak disortir. Vakum otomatis menyortir meja dari waktu ke waktu.

Untuk informasi lebih lanjut tentang vakum meja otomatis, lihat [Menyedot debu](#) tabel. Untuk informasi selengkapnya tentang irisan di node komputasi, lihat [Arsitektur sistem gudang data](#).

Langkah mengubah ukuran klasik saat cluster target adalah RA3

Pengubahan ukuran klasik terdiri dari langkah-langkah berikut, ketika tipe cluster target adalah RA3 dan Anda telah memenuhi prasyarat yang dirinci di bagian sebelumnya.

1. Migrasi dimulai dari cluster sumber ke cluster target. Saat kluster target baru disediakan, Amazon Redshift mengirimkan pemberitahuan peristiwa bahwa pengubahan ukuran telah dimulai. Ini memulai ulang cluster Anda yang ada, yang menutup semua koneksi. Jika kluster Anda yang ada adalah cluster produsen berbagi data, koneksi dengan cluster konsumen juga ditutup. Restart membutuhkan waktu beberapa menit.

Perhatikan bahwa setiap relasi database, seperti tabel atau tampilan terwujud, dibuat dengan tidak BACKUP NO dipertahankan selama pengubahan ukuran klasik. Untuk informasi selengkapnya, lihat [MEMBUAT TAMPILAN TERWUJUD](#).

2. Setelah restart, database tersedia untuk dibaca dan ditulis. Selain itu, berbagi data dilanjutkan, yang membutuhkan beberapa menit tambahan.
3. Data dimigrasikan ke kluster target. Ketika tipe node target adalah RA3, membaca dan menulis tersedia selama migrasi data.
4. Saat proses pengubahan ukuran hampir selesai, Amazon Redshift memperbarui titik akhir ke cluster target, dan semua koneksi ke cluster sumber akan dihapus. Cluster target menjadi produsen untuk berbagi data.
5. Pengubahan ukuran selesai. Amazon Redshift mengirimkan pemberitahuan acara.

Anda dapat melihat kemajuan pengubahan ukuran di konsol Amazon Redshift. Waktu yang dibutuhkan untuk mengubah ukuran cluster tergantung pada jumlah data.

Note

Memilih tipe node lama saat Anda mengubah ukuran cluster RA3 — Jika Anda mencoba mengubah ukuran dari cluster dengan node RA3 ke tipe node lain, seperti DC2, pesan peringatan validasi akan muncul di konsol, dan operasi pengubahan ukuran tidak akan selesai. Ini terjadi karena mengubah ukuran ke tipe node lama tidak didukung. Ini untuk mencegah pelanggan mengubah ukuran ke jenis node yang tidak digunakan lagi atau segera tidak digunakan lagi. Ini berlaku untuk pengubahan ukuran elastis dan pengubahan ukuran klasik.

Memantau pengubahan ukuran klasik saat cluster target adalah RA3

[Untuk memantau pengubahan ukuran klasik dari klaster yang disediakan yang sedang berlangsung, termasuk distribusi KEY, gunakan SYS_RESTORE_STATE.](#) Ini menunjukkan persentase selesai untuk tabel yang dikonversi. Anda harus menjadi pengguna super untuk mengakses data.

Jatuhkan tabel yang tidak Anda butuhkan saat Anda melakukan pengubahan ukuran klasik. Ketika Anda melakukan ini, tabel yang ada dapat didistribusikan lebih cepat.

Langkah mengubah ukuran klasik saat cluster target bukan RA3

Pengubahan ukuran klasik terdiri dari berikut ini, ketika tipe node target adalah apa pun selain RA3, seperti DC2, misalnya.

1. Migrasi dimulai dari cluster sumber ke cluster target. Saat kluster target baru disediakan, Amazon Redshift mengirimkan pemberitahuan peristiwa bahwa pengubahan ukuran telah dimulai. Ini memulai ulang cluster Anda yang ada, yang menutup semua koneksi. Jika klaster Anda yang ada adalah cluster produsen berbagi data, koneksi dengan cluster konsumen juga ditutup. Restart membutuhkan waktu beberapa menit.

Perhatikan bahwa setiap relasi database, seperti tabel atau tampilan terwujud, dibuat dengan tidak BACKUP NO dipertahankan selama pengubahan ukuran klasik. Untuk informasi selengkapnya, lihat [MEMBUAT TAMPILAN TERWUJUD.](#)

2. Setelah restart, database tersedia hanya sebagai baca. Berbagi data dilanjutkan, yang membutuhkan beberapa menit tambahan.
3. Data dimigrasikan ke kluster target. Database tetap dibaca saja.

4. Saat proses pengubahan ukuran hampir selesai, Amazon Redshift memperbarui titik akhir ke cluster target, dan semua koneksi ke cluster sumber akan dihapus. Cluster target menjadi produsen untuk berbagi data.
5. Pengubahan ukuran selesai. Amazon Redshift mengirimkan pemberitahuan acara.

Anda dapat melihat kemajuan pengubahan ukuran di konsol Amazon Redshift. Waktu yang dibutuhkan untuk mengubah ukuran cluster tergantung pada jumlah data.

Note

Diperlukan waktu berhari-hari atau mungkin berminggu-minggu untuk mengubah ukuran cluster dengan sejumlah besar data ketika cluster target bukan RA3, atau tidak memenuhi prasyarat untuk cluster target RA3 yang dirinci di bagian sebelumnya.

Perhatikan juga bahwa kapasitas penyimpanan yang digunakan untuk cluster dapat naik setelah mengubah ukuran klasik. Ini adalah perilaku sistem normal ketika cluster memiliki irisan data tambahan yang dihasilkan dari pengubahan ukuran klasik. Penggunaan kapasitas tambahan ini dapat terjadi bahkan ketika jumlah node di cluster tetap sama.

Ubah ukuran elastis vs ukuran klasik

Tabel berikut membandingkan perilaku antara dua jenis pengubahan ukuran.

Ubah ukuran elastis vs ukuran klasik

Perilaku	Ubah ukuran elastis	Ubah ukuran klasik	Koment				
Retensi data sistem	Pengubahan ukuran elastis mempertahankan data log sistem.	Pengubahan ukuran klasik tidak menyimpan tabel dan data sistem.	Jika Anda mengaktifkan pencatatan audit di kluster sumber,				

Perilaku	Ubah ukuran elastis	Ubah ukuran klasik	Koment				
			Anda dapat terus mengakses log di Amazon S3 atau di CloudWatch, setelah mengubah ukuran. Anda dapat menyimpan atau menghapus log ini sesuai kebijakan data yang ditentukan.				

Perilaku	Ubah ukuran elastis	Ubah ukuran klasik	Koment				
Mengubah jenis node	<p>Ubah ukuran elastis, ketika tipe node tidak berubah: Ubah ukuran di tempat, dan sebagian besar kueri ditahan.</p> <p>Ubah ukuran elastis, dengan tipe node baru dipilih: Sebuah cluster baru dibuat. Kueri dijatuhkan saat proses perubahan ukuran selesai.</p>	Classic Resize: Sebuah cluster baru dibuat. Kueri dijatuhkan selama proses perubahan ukuran.					

Perilaku	Ubah ukuran elastis	Ubah ukuran klasik	Koment				
Sesi dan retensi kueri	Pengubahan ukuran elastis mempertahankan sesi dan kueri saat tipe node sama di cluster sumber dan target. Jika Anda memilih jenis node baru, kueri akan dihapus.	Pengubahan ukuran klasik tidak mempertahankan sesi dan kueri. Pertanyaan dijatuhkan.	Saat kueri dihapus, Anda dapat mengharapkan beberapa penurunan kinerja. Yang terbaik adalah melakukan operasi pengubahan ukuran selama periode penggunaan ringan.				

Perilaku	Ubah ukuran elastis	Ubah ukuran klasik	Koment
Membatalkan operasi perubahan ukuran	Anda tidak dapat membatalkan perubahan ukuran elastis.	Anda dapat membatalkan operasi perubahan ukuran klasik sebelum selesai dengan memilih Batalkan perubahan ukuran dari detail cluster di konsol Amazon Redshift.	Jumlah waktu yang diperlukan untuk membatalkan perubahan ukuran tergantung pada tahap operasi perubahan ukuran saat Anda membatalkan. Saat Anda melakukan ini, klaster tidak tersedia sampai operasi pembatalan selesai.

Perilaku	Ubah ukuran elastis	Ubah ukuran klasik	Koment				
			<p>n selesai. Jika operasi pengubahan ukuran berada di tahap akhir, Anda tidak dapat membatalkan.</p> <p>Untuk mengubah ukuran klasik ke cluster RA3, Anda tidak dapat membatalkan.</p>				

Menjadwalkan perubahan ukuran

Anda dapat menjadwalkan operasi perubahan ukuran untuk klaster Anda untuk ditingkatkan guna mengantisipasi penggunaan yang tinggi atau untuk mengurangi penghematan biaya. Penjadwalan

berfungsi untuk mengubah ukuran elastis dan mengubah ukuran klasik. Anda dapat mengatur jadwal di konsol Amazon Redshift. Untuk informasi selengkapnya, lihat [Mengubah ukuran cluster](#), di bagian Mengelola kluster menggunakan konsol. Anda juga dapat menggunakan AWS CLI atau operasi Amazon Redshift API untuk menjadwalkan perubahan ukuran. [Untuk informasi selengkapnya, lihat create-scheduled-action di Referensi AWS CLI Perintah atau Tindakan di Referensi API Amazon CreateScheduled Redshift.](#)

Snapshot, pulihkan, dan ubah ukuran

[Pengubahan ukuran elastis](#) adalah metode tercepat untuk mengubah ukuran cluster Amazon Redshift. Jika pengubahan ukuran elastis bukan pilihan untuk Anda dan Anda memerlukan akses tulis hampir konstan ke kluster Anda, gunakan operasi snapshot dan pulihkan dengan pengubahan ukuran klasik seperti yang dijelaskan di bagian berikut. Pendekatan ini mensyaratkan bahwa setiap data yang ditulis ke cluster sumber setelah snapshot diambil harus disalin secara manual ke cluster target setelah sakelar. Bergantung pada berapa lama salinannya, Anda mungkin perlu mengulanginya beberapa kali sampai Anda memiliki data yang sama di kedua cluster. Kemudian Anda dapat beralih ke cluster target. Proses ini mungkin berdampak negatif pada kueri yang ada sampai kumpulan data lengkap tersedia di kluster target. Namun, ini meminimalkan jumlah waktu yang tidak dapat Anda tulis ke database.

Pendekatan snapshot, restore, dan classic resize menggunakan proses berikut:

1. Ambil snapshot dari cluster Anda yang ada. Cluster yang ada adalah cluster sumber.
2. Perhatikan waktu snapshot diambil. Melakukan hal ini berarti Anda nantinya dapat mengidentifikasi titik ketika Anda perlu menjalankan kembali proses ekstrak, bertransaksi, memuat (ETL) untuk memuat data pasca-snapshot apa pun ke dalam basis data target.
3. Kembalikan snapshot ke cluster baru. Cluster baru ini adalah cluster target. Verifikasi bahwa data sampel ada di cluster target.
4. Ubah ukuran cluster target. Pilih jenis node baru, jumlah node, dan pengaturan lain untuk cluster target.
5. Tinjau beban dari proses ETL Anda yang terjadi setelah Anda mengambil snapshot dari cluster sumber. Pastikan untuk memuat ulang data yang sama dalam urutan yang sama ke dalam cluster target. Jika Anda memiliki pemuatan data yang sedang berlangsung, ulangi proses ini beberapa kali hingga data sama di cluster sumber dan target.
6. Hentikan semua kueri yang berjalan di cluster sumber. [Untuk melakukan ini, Anda dapat me-reboot cluster, atau Anda dapat masuk sebagai superuser dan menggunakan perintah](#)

[PG_CANCEL_BACKEND](#) dan [PG_TERMINATE_BACKEND](#). Mem-boot ulang cluster adalah cara termudah untuk memastikan bahwa cluster tidak tersedia.

7. Ganti nama cluster sumber. Misalnya, ganti nama dari `examplecluster` ke `examplecluster-source`.
8. Ganti nama cluster target untuk menggunakan nama cluster sumber sebelum mengganti nama. Misalnya, ganti nama cluster target dari sebelumnya menjadi `examplecluster`. Mulai saat ini, aplikasi apa pun yang menggunakan titik akhir yang berisi `examplecluster` terhubung ke cluster target.
9. Hapus cluster sumber setelah Anda beralih ke cluster target, dan verifikasi bahwa semua proses bekerja seperti yang diharapkan.

Atau, Anda dapat mengganti nama cluster sumber dan target sebelum memuat ulang data ke cluster target. Pendekatan ini berfungsi jika Anda tidak mengharuskan sistem dan laporan dependen apa pun segera diperbarui dengan yang ada di cluster target. Dalam hal ini, langkah 6 bergerak ke akhir proses yang dijelaskan sebelumnya.

Proses rename hanya diperlukan jika Anda ingin aplikasi terus menggunakan endpoint yang sama untuk terhubung ke cluster. Jika Anda tidak memerlukan ini, Anda dapat memperbarui aplikasi apa pun yang terhubung ke cluster untuk menggunakan titik akhir klaster target tanpa mengganti nama cluster.

Ada beberapa manfaat untuk menggunakan kembali nama cluster. Pertama, Anda tidak perlu memperbarui string koneksi aplikasi karena titik akhir tidak berubah, meskipun klaster yang mendasarinya berubah. Kedua, item terkait seperti CloudWatch alarm Amazon dan notifikasi Amazon Simple Notification Service (Amazon SNS) terkait dengan nama cluster. Ikatan ini berarti Anda dapat terus menggunakan alarm dan notifikasi yang sama dengan yang Anda atur untuk cluster. Penggunaan berkelanjutan ini terutama menjadi perhatian di lingkungan produksi di mana Anda menginginkan fleksibilitas untuk mengubah ukuran cluster tanpa mengonfigurasi ulang item terkait, seperti alarm dan notifikasi.

Menjeda dan melanjutkan cluster

Jika Anda memiliki cluster yang hanya perlu tersedia pada waktu tertentu, Anda dapat menjeda cluster dan kemudian melanjutkannya. Sementara cluster dijeda, penagihan sesuai permintaan ditangguhkan. Hanya penyimpanan cluster yang dikenakan biaya. Untuk informasi selengkapnya tentang harga, lihat halaman [harga Amazon Redshift](#).

Saat Anda menjeda klaster, Amazon Redshift membuat snapshot, mulai menghentikan kueri, dan menempatkan cluster dalam status jeda. Jika Anda menghapus klaster yang dijeda tanpa meminta snapshot akhir, maka Anda tidak dapat memulihkan cluster. Anda tidak dapat membatalkan atau memutar kembali jeda atau melanjutkan operasi setelah dimulai.

Anda dapat menjeda dan melanjutkan cluster di konsol Amazon Redshift, dengan, atau dengan AWS CLI operasi Amazon Redshift API.

Anda dapat menjadwalkan tindakan untuk menjeda dan melanjutkan cluster. Saat Anda menggunakan konsol Amazon Redshift baru untuk membuat jadwal berulang untuk menjeda dan melanjutkan, maka dua tindakan terjadwal dibuat untuk rentang tanggal yang Anda pilih. Nama tindakan terjadwal diberi akhiran dengan `-pause` dan `-resume`. Panjang total nama harus sesuai dengan ukuran maksimum nama tindakan terjadwal.

Anda tidak dapat menjeda jenis cluster berikut:

- Cluster EC2-klasik.
- Cluster yang tidak aktif, misalnya, cluster yang saat ini sedang dimodifikasi.
- Cluster modul keamanan perangkat keras (HSM).
- Cluster yang memiliki snapshot otomatis dimatikan.

Saat memutuskan untuk menjeda klaster, pertimbangkan hal berikut:

- Koneksi atau kueri ke klaster tidak tersedia.
- Anda tidak dapat melihat informasi pemantauan kueri klaster yang dijeda di konsol Amazon Redshift.
- Anda tidak dapat memodifikasi cluster yang dijeda. Tindakan terjadwal apa pun di cluster tidak dilakukan. Ini termasuk membuat snapshot, mengubah ukuran cluster, dan operasi pemeliharaan cluster.
- Metrik perangkat keras tidak dibuat. Perbarui CloudWatch alarm Anda jika alarm disetel pada metrik yang hilang.
- Anda tidak dapat menyalin snapshot otomatis terbaru dari cluster yang dijeda ke snapshot manual.
- Sementara cluster berhenti, itu tidak dapat dilanjutkan sampai operasi jeda selesai.
- Saat Anda menjeda klaster, penagihan ditangguhkan. Namun, operasi jeda biasanya selesai dalam waktu 15 menit, tergantung pada ukuran cluster.
- Log audit diarsipkan dan tidak dipulihkan pada resume.

- Setelah klaster dijeda, jejak dan log mungkin tidak tersedia untuk memecahkan masalah yang terjadi sebelum jeda.
- Tabel tanpa cadangan di cluster tidak dipulihkan saat resume. Untuk informasi selengkapnya tentang tabel tanpa cadangan, lihat [Mengecualikan tabel dari snapshot](#).
- Jika Anda mengelola kredensi admin Anda menggunakan AWS Secrets Manager dan menjeda klaster Anda, rahasia klaster Anda tidak akan dihapus dan Anda akan terus ditagih untuk rahasia tersebut. Untuk informasi selengkapnya tentang mengelola kata sandi admin Redshift Anda AWS Secrets Manager, lihat. [Mengelola kata sandi admin Amazon Redshift menggunakan AWS Secrets Manager](#)

Saat Anda melanjutkan cluster, pertimbangkan hal berikut:

- Versi cluster dari cluster yang dilanjutkan diperbarui ke versi pemeliharaan berdasarkan jendela pemeliharaan cluster.
- Jika Anda menghapus subnet yang terkait dengan cluster yang dijeda, Anda mungkin memiliki jaringan yang tidak kompatibel. Dalam hal ini, pulihkan cluster Anda dari snapshot terbaru.
- Jika Anda menghapus alamat IP Elastis saat cluster dijeda, maka alamat IP Elastis baru diminta.
- Jika Amazon Redshift tidak dapat melanjutkan cluster dengan elastic network interface sebelumnya, Amazon Redshift mencoba mengalokasikan yang baru.
- Saat Anda melanjutkan cluster, alamat IP node Anda mungkin berubah. Anda mungkin perlu memperbarui pengaturan VPC Anda untuk mendukung alamat IP baru ini untuk fitur seperti COPY from Secure Shell (SSH) atau COPY dari Amazon EMR.
- Jika Anda mencoba melanjutkan cluster yang tidak dijeda, operasi resume mengembalikan kesalahan. Jika operasi resume merupakan bagian dari tindakan terjadwal, ubah atau hapus tindakan terjadwal untuk mencegah kesalahan di masa depan.
- Bergantung pada ukuran cluster, dibutuhkan beberapa menit untuk melanjutkan cluster sebelum kueri dapat diproses. Selain itu, kinerja kueri dapat terpengaruh untuk beberapa periode waktu saat cluster sedang dihidrasi ulang setelah resume selesai.

Mengganti nama cluster

Anda dapat mengganti nama cluster jika Anda ingin cluster menggunakan nama yang berbeda. Karena titik akhir klaster Anda menyertakan nama cluster (juga disebut sebagai pengidentifikasi cluster), titik akhir berubah untuk menggunakan nama baru setelah penggantian nama selesai. Misalnya, jika Anda memiliki klaster bernama `examplecluster` dan mengganti namanya

menjadinewcluster, titik akhir berubah untuk menggunakan pengenal. newcluster Setiap aplikasi yang terhubung ke cluster harus diperbarui dengan endpoint baru.

Anda dapat mengganti nama cluster jika Anda ingin mengubah cluster yang terhubung dengan aplikasi Anda tanpa harus mengubah titik akhir dalam aplikasi tersebut. Dalam hal ini, Anda harus terlebih dahulu mengganti nama cluster asli dan kemudian mengubah cluster kedua untuk menggunakan kembali nama cluster asli sebelum mengganti nama. Melakukan hal ini diperlukan karena pengidentifikasi cluster harus unik di dalam akun dan wilayah Anda, sehingga cluster asli dan cluster kedua tidak dapat memiliki nama yang sama. Anda dapat melakukan ini jika memulihkan cluster dari snapshot dan tidak ingin mengubah properti koneksi dari aplikasi dependen apa pun.

Note

Jika Anda menghapus cluster asli, Anda bertanggung jawab untuk menghapus snapshot cluster yang tidak diinginkan.

Saat Anda mengganti nama cluster, status klaster berubah renaming hingga proses selesai. Nama DNS lama yang digunakan oleh cluster segera dihapus, meskipun bisa tetap di-cache selama beberapa menit. Nama DNS baru untuk cluster yang diganti namanya menjadi efektif dalam waktu sekitar 10 menit. Cluster yang diganti namanya tidak tersedia sampai nama baru menjadi efektif. Cluster akan di-boot ulang dan koneksi yang ada ke cluster akan dihapus. Setelah ini selesai, titik akhir akan berubah untuk menggunakan nama baru. Untuk alasan ini, Anda harus menghentikan kueri agar tidak berjalan sebelum memulai penggantian nama dan memulai ulang setelah penggantian nama selesai.

Snapshot cluster dipertahankan, dan semua snapshot yang terkait dengan cluster tetap terkait dengan cluster tersebut setelah diganti namanya. Misalnya, Anda memiliki cluster yang melayani database produksi Anda dan cluster memiliki beberapa snapshot. Jika Anda mengganti nama cluster dan kemudian menggantinya di lingkungan produksi dengan snapshot, cluster yang Anda ganti nama masih memiliki snapshot yang ada yang terkait dengannya.

CloudWatch Alarm Amazon dan notifikasi acara Amazon Simple Notification Service (Amazon SNS) dikaitkan dengan nama cluster. Jika Anda mengganti nama cluster, Anda harus memperbaruinya. Anda dapat memperbarui CloudWatch alarm di CloudWatch konsol, dan Anda dapat memperbarui notifikasi acara Amazon SNS di konsol Amazon Redshift di panel Acara. Data pemuatan dan kueri untuk cluster terus menampilkan data dari sebelum penggantian nama dan setelah penggantian nama. Namun, data kinerja diatur ulang setelah proses penggantian nama selesai.

Untuk informasi selengkapnya, lihat [Mengubah klaster](#).

Mematikan dan menghapus cluster

Anda dapat mematikan klaster Anda jika Anda ingin menghentikannya agar tidak berjalan dan menimbulkan biaya. Saat Anda memamatkannya, Anda dapat membuat snapshot akhir secara opsional. Jika Anda membuat snapshot akhir, Amazon Redshift akan membuat snapshot manual cluster Anda sebelum memamatkannya. Anda nantinya dapat memulihkan snapshot itu jika Anda ingin melanjutkan menjalankan cluster dan menanyakan data.

Jika Anda tidak lagi membutuhkan cluster dan datanya, Anda dapat memamatkannya tanpa membuat snapshot akhir. Dalam hal ini, cluster dan data dihapus secara permanen. Untuk informasi selengkapnya tentang mematikan dan menghapus cluster, lihat [Menghapus klaster](#)

Terlepas dari apakah Anda mematikan cluster Anda dengan snapshot manual terakhir, semua snapshot otomatis yang terkait dengan cluster akan dihapus setelah cluster dimatikan. Setiap snapshot manual yang terkait dengan cluster dipertahankan. Setiap snapshot manual yang disimpan, termasuk snapshot akhir opsional, dikenakan biaya pada tingkat penyimpanan Amazon Simple Storage Service jika Anda tidak memiliki cluster lain yang berjalan saat Anda mematikan klaster, atau jika Anda melebihi penyimpanan gratis yang tersedia yang disediakan untuk klaster Amazon Redshift yang sedang berjalan. Untuk informasi selengkapnya tentang biaya penyimpanan snapshot, lihat halaman [harga Amazon Redshift](#).

Menghapus cluster juga menghapus rahasia terkait AWS Secrets Manager .

Merelokasi klaster Anda

Dengan menggunakan relokasi di Amazon Redshift, Anda mengizinkan Amazon Redshift memindahkan klaster ke Availability Zone (AZ) lain tanpa kehilangan data atau perubahan pada aplikasi Anda. Dengan relokasi, Anda dapat melanjutkan operasi ketika ada gangguan layanan pada cluster Anda dengan dampak minimal.

Saat relokasi cluster diaktifkan, Amazon Redshift mungkin memilih untuk merelokasi cluster dalam beberapa situasi. Secara khusus, ini terjadi ketika masalah di Availability Zone saat ini mencegah operasi cluster yang optimal atau untuk meningkatkan ketersediaan layanan. Anda juga dapat menjalankan fungsi relokasi jika kendala sumber daya di Availability Zone tertentu mengganggu operasi klaster. Contohnya adalah kemampuan untuk melanjutkan atau mengubah ukuran cluster. Amazon Redshift menawarkan fitur relokasi tanpa biaya tambahan.

Saat klaster Amazon Redshift dipindahkan ke Availability Zone baru, cluster baru memiliki titik akhir yang sama dengan cluster asli. Aplikasi Anda dapat terhubung kembali ke titik akhir dan melanjutkan operasi tanpa modifikasi atau kehilangan data. Namun, relokasi mungkin tidak selalu dimungkinkan karena potensi kendala sumber daya di Availability Zone tertentu.

Relokasi klaster Amazon Redshift hanya didukung untuk jenis instans RA3, seperti ra3.16xlarge, ra3.4xlarge, dan ra3.xlplus. Jenis instans RA3 menggunakan Redshift Managed Storage (RMS) sebagai lapisan penyimpanan yang tahan lama. Salinan terbaru dari data klaster selalu tersedia di Availability Zone lainnya di suatu AWS Wilayah. Dengan kata lain, Anda dapat memindahkan cluster Amazon Redshift ke Availability Zone lain tanpa kehilangan data.

Saat Anda mengaktifkan relokasi untuk klaster, Amazon Redshift memigrasikan klaster Anda untuk berada di belakang proxy. Melakukan hal ini membantu mengimplementasikan akses independen lokasi ke sumber daya komputasi klaster. Migrasi menyebabkan cluster di-boot ulang. Saat klaster dipindahkan ke Availability Zone lain, pemadaman terjadi saat klaster baru dibawa kembali online di Availability Zone yang baru. Namun, Anda tidak perlu membuat perubahan apa pun pada aplikasi Anda karena titik akhir cluster tetap tidak berubah bahkan setelah cluster dipindahkan ke Availability Zone yang baru.

Relokasi cluster dinonaktifkan secara default pada semua cluster RA3. Amazon Redshift menetapkan 5439 sebagai port default saat membuat klaster yang disediakan. Anda dapat mengubah ke port lain dari rentang port 5431-5455 atau 8191-8215. (Jangan mengubah ke port di luar rentang. Ini menghasilkan kesalahan.) Untuk mengubah port default untuk klaster yang disediakan, gunakan konsol Amazon Redshift AWS CLI, atau Amazon Redshift API. Untuk mengubah port default untuk grup kerja tanpa server, gunakan API Tanpa Server Amazon Redshift AWS CLI atau Amazon Redshift.

Jika Anda mengaktifkan relokasi dan saat ini Anda menggunakan alamat IP node pemimpin untuk mengakses klaster Anda, pastikan untuk mengubah akses itu. Sebagai gantinya, gunakan alamat IP yang terkait dengan titik akhir virtual private cloud (VPC) cluster. Untuk menemukan alamat IP cluster ini, temukan dan gunakan titik akhir VPC di bagian Jaringan dan keamanan pada halaman detail cluster. Untuk mendapatkan detail selengkapnya tentang titik akhir VPC, masuk ke konsol VPC Amazon.

Anda juga dapat menggunakan perintah AWS Command Line Interface (AWS CLI) `describe-vpc-endpoints` untuk mendapatkan elastic network interface yang terkait dengan endpoint. Anda dapat menggunakan `describe-network-interfaces` perintah untuk mendapatkan alamat IP terkait. Untuk informasi selengkapnya tentang perintah Amazon Redshift, lihat [AWS CLI Perintah yang tersedia di Referensi AWS CLI Perintah](#).

Note

Sebagai pengingat, relokasi cluster bukanlah prasyarat untuk mengonfigurasi fitur jaringan Redshift tambahan. Misalnya, Anda dapat memujinya dengan [penyalinan snapshot lintas wilayah](#), untuk memberikan ketahanan yang lebih bagi lingkungan Anda, tetapi itu tidak diperlukan. Anda juga tidak perlu menyalakannya untuk mengaktifkan fitur-fitur berikut:

- Menghubungkan dari VPC lintas akun atau lintas wilayah ke Redshift — Anda dapat terhubung dari satu AWS virtual private cloud (VPC) ke yang lain yang berisi database Redshift. Ini membuatnya lebih mudah untuk mengelola, misalnya, akses klien dari akun yang berbeda atau VPC, tanpa harus menyediakan akses VPC lokal ke identitas yang terhubung ke database. Untuk informasi selengkapnya, lihat [Menghubungkan ke Amazon Redshift Tanpa Server dari titik akhir VPC Redshift](#) di akun atau wilayah lain.
- Menyiapkan nama domain khusus — Anda dapat membuat nama domain khusus, juga dikenal sebagai URL khusus, untuk klaster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server, untuk membuat nama titik akhir lebih mudah diingat dan sederhana. Untuk informasi selengkapnya, lihat [Menggunakan nama domain khusus untuk koneksi klien](#).

Batasan

Saat menggunakan relokasi Amazon Redshift, perhatikan batasan berikut:

- Relokasi klaster mungkin tidak dapat dilakukan di semua skenario karena potensi keterbatasan sumber daya di Availability Zone tertentu. Jika ini terjadi, Amazon Redshift tidak mengubah cluster asli.
- Relokasi tidak didukung pada keluarga produk instans DC2.
- Anda tidak dapat melakukan relokasi di seluruh AWS Wilayah.
- Relokasi Amazon Redshift default ke nomor port 5439. Anda juga dapat mengubah ke port lain dalam rentang 5431-5455 atau 8191-8215.

Mengaktifkan relokasi cluster

Anda dapat mengaktifkan dan mengelola relokasi klaster dari konsol Amazon Redshift AWS CLI, dan Amazon Redshift API.

Untuk mengaktifkan relokasi klaster, tentukan grup subnet yang menyertakan beberapa Availability Zone. Jika Amazon Redshift mengidentifikasi lebih dari satu Availability Zone yang dapat diakses, Amazon Redshift secara otomatis memilih dari daftar Availability Zone yang dapat diakses untuk memindahkan cluster.

Setelah relokasi selesai, Anda menggunakan endpoint yang sama untuk mengakses cluster. Amazon Redshift menghapus sumber daya komputasi cluster asli dan mengembalikannya ke kumpulan sumber daya.

Mengelola relokasi menggunakan konsol

Anda dapat mengelola pengaturan untuk relokasi cluster menggunakan konsol Amazon Redshift.

Mengaktifkan relokasi saat membuat cluster baru

Gunakan prosedur berikut untuk mengaktifkan relokasi saat membuat cluster baru.

Untuk mengaktifkan relokasi untuk cluster baru

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster.
3. Pilih Buat cluster untuk membuat cluster baru. Untuk informasi selengkapnya tentang cara membuat klaster, lihat klaster yang [disediakan Amazon Redshift di Panduan Memulai Pergeseran Merah Amazon](#).
4. Di bagian Backup, untuk relokasi Cluster, pilih Diaktifkan. Relokasi dimatikan secara default.
5. Pilih Buat klaster.

Memodifikasi relokasi untuk cluster yang ada

Gunakan prosedur berikut untuk mengubah pengaturan relokasi untuk cluster yang ada.

Untuk mengubah setelan relokasi untuk klaster yang ada

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster. Cluster untuk akun Anda di AWS Wilayah saat ini terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.

3. Pilih nama cluster yang ingin Anda ubah dari daftar. Halaman detail cluster muncul.
4. Pilih tab Maintenance, lalu di bagian Backup details pilih Edit.
5. Di bawah Backup, pilih Diaktifkan. Relokasi dimatikan secara default.
6. Pilih Ubah klaster.

Merelokasi cluster

Gunakan prosedur berikut untuk memindahkan cluster secara manual ke Availability Zone lain. Ini sangat berguna ketika Anda ingin menguji pengaturan jaringan Anda di Availability Zone sekunder atau ketika Anda mengalami kendala sumber daya di Availability Zone saat ini.

Untuk memindahkan klaster ke Availability Zone lain

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster. Cluster untuk akun Anda di AWS Wilayah saat ini terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih nama cluster yang ingin Anda pindahkan dari daftar. Halaman detail cluster muncul.
4. Untuk Tindakan, pilih Relokasi. Halaman klaster Relokasi muncul.
5. (Opsional) Pilih Availability Zone. Jika Anda tidak memilih Availability Zone, Amazon Redshift memilihnya untuk Anda.

Amazon Redshift memulai relokasi dan menampilkan cluster sebagai relokasi. Setelah relokasi selesai, status cluster berubah menjadi tersedia.

Mengelola relokasi menggunakan Amazon Redshift CLI

Anda dapat mengelola pengaturan untuk relokasi cluster menggunakan AWS Command Line Interface (CLI).

Dengan AWS CLI, perintah contoh berikut membuat cluster Amazon Redshift **mycluster** bernama yang telah diaktifkan relokasi.

```
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
```

Jika cluster Anda saat ini menggunakan port yang berbeda, Anda harus memodifikasinya untuk digunakan dari rentang port 5431-5455 atau 8191-8215 sebelum memodifikasinya untuk mengaktifkan relokasi. Defaultnya adalah 5439. Contoh perintah berikut memodifikasi port jika cluster Anda tidak menggunakan salah satu dari rentang yang diberikan.

```
aws redshift modify-cluster --cluster-identifier mycluster --port 5439
```

Contoh perintah berikut mencakup `availability-zone-relocation` parameter pada cluster Amazon Redshift.

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

Contoh perintah berikut mematikan `availability-zone-relocation` parameter pada cluster Amazon Redshift.

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

Contoh perintah berikut memanggil relokasi di cluster Amazon Redshift.

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

Cuplikan dan cadangan Amazon Redshift

Topik

- [Ikhtisar snapshot](#)
- [Snapshot otomatis](#)
- [Jadwal snapshot otomatis](#)
- [Format jadwal snapshot](#)
- [Snapshot manual](#)
- [Mengelola penyimpanan snapshot](#)
- [Tidak termasuk tabel dari snapshot](#)
- [Menyalin snapshot ke Wilayah lain AWS](#)

- [Memulihkan cluster dari snapshot](#)
- [Memulihkan tabel dari snapshot](#)
- [Berbagi snapshot](#)
- [Mengelola snapshot menggunakan konsol](#)
- [Mengelola snapshot menggunakan API Amazon AWS CLI Redshift dan Amazon](#)
- [Bekerja dengan AWS Backup](#)

Ikhtisar snapshot

Snapshot adalah point-in-time backup dari sebuah cluster. Ada dua jenis snapshot: otomatis dan manual. Amazon Redshift menyimpan snapshot ini secara internal di Amazon S3 dengan menggunakan koneksi Secure Sockets Layer (SSL) terenkripsi.

Amazon Redshift secara otomatis mengambil snapshot tambahan yang melacak perubahan pada cluster sejak snapshot otomatis sebelumnya. Snapshot otomatis menyimpan semua data yang diperlukan untuk memulihkan cluster dari snapshot. Anda dapat membuat jadwal snapshot untuk mengontrol kapan snapshot otomatis diambil, atau Anda dapat mengambil snapshot manual kapan saja.

Saat memulihkan dari snapshot, Amazon Redshift membuat cluster baru dan membuat klaster baru tersedia sebelum semua data dimuat, sehingga Anda dapat segera mulai menanyakan klaster baru. Cluster mengalirkan data sesuai permintaan dari snapshot sebagai respons terhadap kueri aktif, lalu memuat data yang tersisa di latar belakang.

Saat meluncurkan cluster, Anda dapat mengatur periode retensi untuk snapshot otomatis dan manual. Anda dapat mengubah periode retensi default untuk snapshot otomatis dan manual dengan memodifikasi cluster. Anda dapat mengubah periode retensi untuk snapshot manual saat membuat snapshot atau dengan memodifikasi snapshot.

[Anda dapat memantau kemajuan snapshot dengan melihat detail snapshot di AWS Management Console, atau dengan memanggil `describe-cluster-snapshot` di CLI atau tindakan `Snapshots API DescribeCluster`](#) Untuk snapshot yang sedang berlangsung, ini menampilkan informasi seperti ukuran snapshot tambahan, kecepatan transfer, waktu yang telah berlalu, dan perkiraan waktu yang tersisa.

Untuk memastikan bahwa cadangan Anda selalu tersedia untuk klaster Anda, Amazon Redshift menyimpan snapshot dalam bucket Amazon S3 yang dikelola secara internal yang dikelola oleh

Amazon Redshift. Untuk mengelola biaya penyimpanan, evaluasi berapa hari Anda perlu menyimpan snapshot otomatis dan mengonfigurasi periode retensi yang sesuai. Hapus snapshot manual yang tidak lagi Anda butuhkan. Untuk informasi selengkapnya tentang biaya penyimpanan cadangan, lihat halaman [harga Amazon Redshift](#).

Bekerja dengan snapshot dan backup di Amazon Redshift Serverless

Amazon Redshift Tanpa Server, seperti kluster yang disediakan, memungkinkan Anda mengambil cadangan sebagai point-in-time representasi objek dan data di namespace. Ada dua jenis cadangan di Amazon Redshift Serverless: snapshot yang dibuat secara manual dan titik pemulihan yang dibuat Amazon Redshift Serverless secara otomatis. Anda dapat menemukan informasi lebih lanjut tentang bekerja dengan snapshot untuk Amazon Redshift Tanpa Server [di Bekerja dengan snapshot dan titik pemulihan](#).

Anda juga dapat memulihkan snapshot dari kluster yang disediakan ke namespace tanpa server. Untuk informasi selengkapnya, lihat [Memulihkan namespace tanpa server dari snapshot](#).

Snapshot otomatis

Saat snapshot otomatis diaktifkan untuk kluster, Amazon Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default Amazon Redshift mengambil snapshot setiap delapan jam atau mengikuti setiap 5 GB per node perubahan data, atau mana yang lebih dulu. Jika data Anda lebih besar dari 5 GB* jumlah node, jumlah waktu terpendek di antara pembuatan snapshot otomatis adalah 15 menit. Atau, Anda dapat membuat jadwal snapshot untuk mengontrol saat snapshot otomatis diambil. Jika Anda menggunakan jadwal khusus, jumlah waktu minimum antara snapshot otomatis adalah satu jam. Snapshot otomatis diaktifkan secara default saat Anda membuat cluster.

Snapshot otomatis dihapus pada akhir periode retensi. Periode retensi default adalah satu hari, tetapi Anda dapat memodifikasinya dengan menggunakan konsol Amazon Redshift atau secara terprogram dengan menggunakan Amazon Redshift API atau CLI.

Untuk menonaktifkan snapshot otomatis, atur periode retensi ke nol. Jika Anda menonaktifkan snapshot otomatis, Amazon Redshift berhenti mengambil snapshot dan menghapus snapshot otomatis yang ada untuk cluster. Anda tidak dapat menonaktifkan snapshot otomatis untuk tipe node RA3. Anda dapat mengatur periode retensi otomatis tipe node RA3 dari 1—35 hari.

Hanya Amazon Redshift yang dapat menghapus snapshot otomatis; Anda tidak dapat menghapusnya secara manual. Amazon Redshift menghapus snapshot otomatis di akhir periode retensi snapshot, saat Anda menonaktifkan snapshot otomatis untuk kluster, atau saat Anda

menghapus klaster. [Amazon Redshift mempertahankan snapshot otomatis terbaru hingga Anda menonaktifkan snapshot otomatis atau menghapus cluster.](#)

Jika Anda ingin menyimpan snapshot otomatis untuk jangka waktu yang lebih lama, Anda dapat membuat salinannya sebagai snapshot manual. Snapshot otomatis dipertahankan hingga akhir periode retensi, tetapi snapshot manual yang sesuai dipertahankan hingga Anda menghapusnya secara manual atau hingga akhir periode retensi.

Jadwal snapshot otomatis

Untuk mengontrol secara tepat kapan snapshot diambil, Anda dapat membuat jadwal snapshot dan melampirkannya ke satu atau lebih cluster. Saat Anda mengubah jadwal snapshot, jadwal diubah untuk semua cluster terkait. Jika klaster tidak memiliki jadwal snapshot terlampir, klaster menggunakan jadwal snapshot otomatis default.

Jadwal snapshot adalah seperangkat aturan jadwal. Anda dapat menentukan aturan jadwal sederhana berdasarkan interval tertentu, seperti setiap 8 jam atau setiap 12 jam. Anda juga dapat menambahkan aturan untuk mengambil foto pada hari-hari tertentu dalam seminggu, pada waktu tertentu, atau selama periode tertentu. Aturan juga dapat didefinisikan menggunakan ekspresi cron mirip Unix.

Format jadwal snapshot

Di konsol Amazon Redshift, Anda dapat membuat jadwal snapshot. Kemudian, Anda dapat melampirkan jadwal ke cluster untuk memicu pembuatan snapshot sistem. Jadwal dapat dilampirkan ke beberapa cluster, dan Anda dapat membuat beberapa definisi cron dalam jadwal untuk memicu snapshot.

Anda dapat menentukan jadwal untuk snapshot Anda menggunakan sintaks cron. [Definisi jadwal ini menggunakan sintaks cron mirip Unix yang dimodifikasi.](#) Anda menentukan waktu di [Waktu universal terkoordinasi \(UTC\)](#). Anda dapat membuat jadwal dengan frekuensi maksimum satu jam dan presisi minimum satu menit.

Ekspresi cron yang dimodifikasi Amazon Redshift memiliki 3 bidang wajib, yang dipisahkan oleh spasi putih.

Sintaksis

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

Bidang	Nilai-nilai	Wildcard
Menit	0–59	, - * /
Jam	0–23	, - * /
Tanggal	1–31	, - * ? / L W
Bulan	1–12 atau JAN-DEC	, - * /
Hari	1–7 atau SUN-SAT	, - * ? L #
Tahun	1970–2199	, - * /

Wildcard

- Wildcard , (koma) mencakup nilai tambahan. Di Day-of-week lapangan, MON, WED, FRI akan mencakup Senin, Rabu, dan Jumat. Nilai total dibatasi hingga 24 per bidang.
- Wildcard - (tanda hubung) menentukan rentang. Di Hour lapangan, 1-15 akan mencakup jam 1 hingga 15 dari hari yang ditentukan.
- Wildcard * (bintang) mencakup semua nilai di bidang. Di kolom Hours, * akan mencakup setiap jam.
- Wildcard / (garis miring) menentukan tambahan. Di Hours lapangan, Anda bisa masuk **1/10** untuk menentukan setiap jam ke-10, mulai dari jam pertama hari itu (misalnya, 01:00, 11:00, dan 21:00).
- Wildcard ? (tanda tanya) menentukan satu atau yang lain. Di **Day-of-month** lapangan Anda bisa masuk 7, dan jika Anda tidak peduli hari apa dalam minggu ketujuh, Anda bisa masuk? di ay-of-week bidang D.
- Wildcard L di kolom Day-of-month atau Day-of-week menentukan hari terakhir pada bulan atau minggu.
- Wildcard W di kolom Day-of-month menentukan hari kerja. Di kolom Day-of-month, 3W menentukan hari kerja yang paling dekat dengan pekan ketiga di bulan itu.
- Wildcard # di ay-of-week bidang D menentukan contoh tertentu dari hari yang ditentukan dalam seminggu dalam sebulan. Sebagai contoh, 3#2 akan menjadi hari Selasa kedua setiap bulan: 3 mengacu pada hari Selasa karena itu adalah hari ketiga setiap minggu, dan 2 mengacu pada hari kedua dari jenis tersebut dalam bulan tersebut.

Note

Jika Anda menggunakan karakter '#', Anda hanya dapat menentukan satu ekspresi di day-of-week bidang. Misalnya, "3 #1 ,6 #3" tidak valid karena ditafsirkan sebagai dua ekspresi.

Batas

- Anda tidak dapat menentukan kolom Day-of-month dan Day-of-week dalam ekspresi cron yang sama. Jika Anda menentukan sebuah nilai di salah satu kolom, maka Anda harus menggunakan ? (tanda tanya) di kolom yang lain.
- Jadwal snapshot tidak mendukung frekuensi berikut:
 - Snapshot dijadwalkan lebih sering dari 1 per jam.
 - Snapshot dijadwalkan kurang dari 1 per hari (24 jam).

Jika Anda memiliki jadwal yang tumpang tindih yang menghasilkan penjadwalan snapshot dalam jendela 1 jam, kesalahan validasi akan terjadi.

Anda dapat membuat jadwal, Anda dapat menggunakan contoh cron berikut.

Menit	Jam	Hari dalam seminggu	Arti			
0	14-20/1	SEL	Setiap jam antara jam 2 siang dan 8 malam pada hari Selasa.			
0	21	MON-FRI	Setiap malam jam 9 malam Senin-Jumat.			
30	0/6	SAT-MATAHARI	Setiap kenaikan 6 jam pada hari Sabtu dan Minggu dimulai pada 30 menit setelah tengah malam (00:30)			

Menit	Jam	Hari dalam seminggu	Arti			
			hari itu. Ini menghasilkan snapshot pada [00:30, 06:30, 12:30, dan 18:30] setiap hari.			
30	12/4	*	Setiap kenaikan 4 jam mulai pukul 12:30 setiap hari. Ini memutuskan untuk [12:30, 16:30, 20:30].			

Misalnya berjalan sesuai jadwal dengan kenaikan setiap 2 jam mulai pukul 15:15 setiap hari. Ini memutuskan untuk [15:15, 17:15, 19:15, 21:15, 23:15], tentukan:

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

Anda dapat membuat beberapa definisi jadwal cron dalam sebagai jadwal. Misalnya AWS CLI perintah berikut berisi dua jadwal cron dalam satu jadwal.

```
create-snapshot-schedule --schedule-identifier "my-test" --schedule-definition "cron(0 17 SAT,SUN)" "cron(0 9,17 MON-FRI)"
```

Snapshot manual

Anda dapat mengambil snapshot manual kapan saja. Secara default, snapshot manual dipertahankan tanpa batas waktu, bahkan setelah Anda menghapus klaster Anda. Anda dapat menentukan periode retensi saat membuat snapshot manual, atau Anda dapat mengubah periode retensi dengan memodifikasi snapshot. Untuk informasi selengkapnya tentang mengubah periode retensi, lihat [Mengubah periode retensi snapshot manual](#).

Jika snapshot dihapus, Anda tidak dapat memulai operasi baru yang mereferensikan snapshot itu. Namun, jika operasi pemulihan sedang berlangsung, operasi pemulihan itu akan berjalan hingga selesai.

Amazon Redshift memiliki kuota yang membatasi jumlah snapshot manual yang dapat Anda buat; kuota ini per akun per Wilayah. AWS AWS Kuota default tercantum di [Kuota dan batas di Amazon Redshift](#).

Mengelola penyimpanan snapshot

Karena snapshot menimbulkan biaya penyimpanan, penting bagi Anda untuk menghapusnya saat Anda tidak lagi membutuhkannya. Amazon Redshift menghapus snapshot otomatis dan manual di akhir periode retensi snapshot masing-masing. Anda juga dapat menghapus snapshot manual menggunakan AWS Management Console atau dengan perintah CLI [batch-delete-cluster-snapshots](#).

Anda dapat mengubah periode retensi untuk snapshot manual dengan memodifikasi pengaturan snapshot manual.

Anda bisa mendapatkan informasi tentang berapa banyak penyimpanan yang dikonsumsi snapshot Anda menggunakan Amazon Redshift Console atau menggunakan [perintah CLI deskripsi-penyimpanan](#).

Tidak termasuk tabel dari snapshot

Secara default, semua tabel permanen yang ditentukan pengguna disertakan dalam snapshot. Jika tabel, seperti tabel pementasan, tidak perlu dicadangkan, Anda dapat secara signifikan mengurangi waktu yang dibutuhkan untuk membuat snapshot dan memulihkan dari snapshot. Anda juga mengurangi ruang penyimpanan di Amazon S3 dengan menggunakan tabel tanpa cadangan. Untuk membuat tabel tanpa cadangan, sertakan parameter BACKUP NO saat Anda membuat tabel. Untuk informasi selengkapnya, lihat [MEMBUAT TABEL](#) dan [MEMBUAT TABEL AS](#) di Panduan Pengembang Database Amazon Redshift.

Menyalin snapshot ke Wilayah lain AWS

Anda dapat mengonfigurasi Amazon Redshift untuk secara otomatis menyalin snapshot (otomatis atau manual) untuk cluster ke Wilayah lain. AWS Ketika snapshot dibuat di AWS Region utama cluster, itu disalin ke Region sekunder AWS . Kedua AWS Wilayah tersebut masing-masing dikenal sebagai AWS Wilayah sumber dan AWS Wilayah tujuan. Jika Anda menyimpan salinan snapshot Anda di AWS Wilayah lain, Anda dapat memulihkan klaster Anda dari data terbaru jika ada yang memengaruhi AWS Wilayah utama. Anda dapat mengonfigurasi klaster Anda untuk menyalin

snapshot ke hanya satu AWS Wilayah tujuan pada satu waktu. Untuk daftar Wilayah Amazon Redshift, lihat [Wilayah dan titik akhir](#) di. Referensi Umum Amazon Web Services

Saat Anda mengaktifkan Amazon Redshift untuk secara otomatis menyalin snapshot ke AWS Wilayah lain, Anda menentukan AWS Wilayah tujuan untuk menyalin snapshot. Untuk snapshot otomatis, Anda juga dapat menentukan periode retensi untuk menyimpannya di AWS Wilayah tujuan. Setelah snapshot otomatis disalin ke AWS Wilayah tujuan dan mencapai periode waktu penyimpanan di sana, snapshot tersebut dihapus dari Wilayah tujuan AWS. Melakukan hal ini membuat penggunaan snapshot Anda tetap rendah. Untuk menyimpan snapshot otomatis untuk waktu yang lebih singkat atau lebih lama di AWS Wilayah tujuan, ubah periode retensi ini.

Periode penyimpanan yang Anda tetapkan untuk snapshot otomatis yang disalin ke AWS Wilayah tujuan terpisah dari periode penyimpanan untuk snapshot otomatis di Wilayah sumber. AWS Periode retensi default untuk snapshot yang disalin adalah tujuh hari. Periode tujuh hari itu hanya berlaku untuk snapshot otomatis. Di AWS Wilayah sumber dan tujuan, snapshot manual dihapus pada akhir periode retensi snapshot atau saat Anda menghapusnya secara manual.

Anda dapat menonaktifkan salinan snapshot otomatis untuk cluster kapan saja. Saat Anda menonaktifkan fitur ini, snapshot tidak lagi disalin dari Wilayah sumber ke AWS Wilayah tujuan AWS. Setiap snapshot otomatis yang disalin ke AWS Wilayah tujuan akan dihapus saat mencapai batas periode retensi, kecuali Anda membuat salinan snapshot manual dari mereka. Cuplikan manual ini, dan snapshot manual apa pun yang disalin dari AWS Wilayah tujuan, disimpan di AWS Wilayah tujuan hingga Anda menghapusnya secara manual.

Untuk mengubah AWS Wilayah tujuan tempat Anda menyalin snapshot, pertama nonaktifkan fitur salin otomatis. Kemudian aktifkan kembali, tentukan Wilayah tujuan AWS baru.

Setelah snapshot disalin ke AWS Wilayah tujuan, itu menjadi aktif dan tersedia untuk tujuan restorasi.

Untuk menyalin snapshot untuk kluster yang AWS KMS dienkripsi —ke AWS Wilayah lain, buat hibah untuk Amazon Redshift untuk menggunakan kunci terkelola pelanggan di Wilayah tujuan. AWS Kemudian pilih hibah itu saat Anda mengaktifkan penyalinan snapshot di Wilayah sumber AWS. Untuk informasi selengkapnya tentang mengonfigurasi hibah salinan snapshot, lihat [Menyalin AWS KMS—snapshot terenkripsi ke Wilayah lain AWS](#)

Memulihkan cluster dari snapshot

Snapshot berisi data dari database apa pun yang berjalan di cluster Anda. Ini juga berisi informasi tentang cluster Anda, termasuk jumlah node, tipe node, dan nama pengguna admin. Jika Anda

memulihkan klaster dari snapshot, Amazon Redshift menggunakan informasi klaster untuk membuat klaster baru. Kemudian mengembalikan semua database dari data snapshot.

Untuk cluster baru yang dibuat dari snapshot asli, Anda dapat memilih konfigurasi, seperti jenis node dan jumlah node. Cluster dipulihkan di AWS Wilayah yang sama dan Availability Zone acak yang dipilih sistem, kecuali Anda menentukan Availability Zone lain dalam permintaan Anda. Saat memulihkan klaster dari snapshot, Anda dapat memilih trek pemeliharaan yang kompatibel untuk klaster baru secara opsional.

Note

Saat Anda mengembalikan snapshot ke cluster dengan konfigurasi yang berbeda, snapshot harus diambil pada cluster dengan versi cluster 1.0.10013, atau yang lebih baru.

Saat pemulihan sedang berlangsung, peristiwa biasanya dipancarkan dalam urutan berikut:

1. RESTORE_STARTED - REDSHIFT-EVENT-2008 dikirim ketika proses pemulihan dimulai.
2. RESTORE_SUCCEEDED — REDSHIFT-EVENT-3003 dikirim ketika cluster baru telah dibuat.

Cluster tersedia untuk kueri.

3. DATA_TRANSFER_COMPLETED — REDSHIFT-EVENT-3537 dikirim saat transfer data selesai.

Note

Cluster RA3 hanya memancarkan peristiwa RESTORE_STARTED dan RESTORE_SUCCEEDED. Tidak ada transfer data eksplisit yang harus dilakukan setelah RESTORE berhasil karena tipe node RA3 menyimpan data di penyimpanan terkelola Amazon Redshift. Dengan node RA3, data terus ditransfer antara node RA3 dan penyimpanan terkelola Amazon Redshift sebagai bagian dari pemrosesan kueri normal. Node RA3 menyimpan data panas secara lokal dan menyimpan blok yang lebih jarang ditanyakan di penyimpanan terkelola Amazon Redshift secara otomatis.

Anda dapat memantau kemajuan pemulihan dengan memanggil operasi [DescribeClusters](#) API, atau melihat detail klaster di AWS Management Console. Untuk pemulihan yang sedang berlangsung, ini menampilkan informasi seperti ukuran data snapshot, kecepatan transfer, waktu yang telah berlalu, dan perkiraan waktu yang tersisa. Untuk deskripsi metrik ini, lihat [RestoreStatus](#).

Anda tidak dapat menggunakan snapshot untuk mengembalikan cluster aktif ke status sebelumnya.

Note

Saat Anda mengembalikan snapshot ke cluster baru, grup keamanan default dan grup parameter digunakan kecuali Anda menentukan nilai yang berbeda.

Anda mungkin ingin mengembalikan snapshot ke cluster dengan konfigurasi berbeda karena alasan berikut:

- Ketika sebuah cluster terdiri dari tipe node yang lebih kecil dan Anda ingin mengkonsolidasikannya menjadi tipe node yang lebih besar dengan node yang lebih sedikit.
- Ketika Anda telah memantau beban kerja Anda dan menentukan kebutuhan untuk pindah ke tipe node dengan lebih banyak CPU dan penyimpanan.
- Bila Anda ingin mengukur kinerja beban kerja pengujian dengan tipe node yang berbeda.

Restore memiliki kendala berikut:

- Konfigurasi node baru harus memiliki penyimpanan yang cukup untuk data yang ada. Bahkan ketika Anda menambahkan node, konfigurasi baru Anda mungkin tidak memiliki penyimpanan yang cukup karena cara data didistribusikan kembali.
- Operasi pemulihan memeriksa apakah snapshot dibuat pada versi cluster yang kompatibel dengan versi cluster dari cluster baru. Jika cluster baru memiliki tingkat versi yang terlalu dini, maka operasi pemulihan gagal dan melaporkan lebih banyak informasi dalam pesan kesalahan.
- Konfigurasi yang mungkin (jumlah node dan tipe node) yang dapat Anda pulihkan ditentukan oleh jumlah node di cluster asli dan tipe node target dari cluster baru. Untuk menentukan kemungkinan konfigurasi yang tersedia, Anda dapat menggunakan konsol Amazon Redshift atau perintah `describe-node-configuration-options` AWS CLI dengan `action-type restore-cluster` Untuk informasi selengkapnya tentang pemulihan menggunakan konsol Amazon Redshift, lihat [Memulihkan cluster dari snapshot](#)

Langkah-langkah berikut mengambil sebuah cluster dengan banyak node dan mengkonsolidasikannya menjadi tipe node yang lebih besar dengan jumlah node yang lebih kecil menggunakan AWS CLI Untuk contoh ini, kita mulai dengan cluster sumber 24 node. Dalam hal ini,

misalkan kita sudah membuat snapshot dari cluster ini dan ingin mengembalikannya ke tipe node yang lebih besar.

1. Jalankan perintah berikut untuk mendapatkan rincian cluster 24-node kami.

```
aws redshift describe-clusters --region eu-west-1 --cluster-identifier
mycluster-123456789012
```

2. Jalankan perintah berikut untuk mendapatkan detail snapshot.

```
aws redshift describe-cluster-snapshots --region eu-west-1 --snapshot-identifier
mycluster-snapshot
```

3. Jalankan perintah berikut untuk menjelaskan opsi yang tersedia untuk snapshot ini.

```
aws redshift describe-node-configuration-options --snapshot-identifier mycluster-
snapshot --region eu-west-1 --action-type restore-cluster
```

Perintah ini mengembalikan daftar opsi dengan jenis node yang direkomendasikan, jumlah node, dan pemanfaatan disk untuk setiap opsi. Untuk contoh ini, perintah sebelumnya mencantumkan konfigurasi node yang mungkin berikut. Kami memilih untuk mengembalikan ke cluster tiga simpul.

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

```

```

    "NumberOfNodes": 4
  },
  {
    "EstimatedDiskUtilizationPercent": 39.156808853149414,
    "NodeType": "dc2.8xlarge",
    "NumberOfNodes": 5
  },
  {
    "EstimatedDiskUtilizationPercent": 32.630674044291176,
    "NodeType": "dc2.8xlarge",
    "NumberOfNodes": 6
  }
]
}

```

4. Jalankan perintah berikut untuk mengembalikan snapshot ke dalam konfigurasi cluster yang kita pilih. Setelah cluster ini dipulihkan, kami memiliki konten yang sama dengan cluster sumber, tetapi data telah dikonsolidasikan menjadi tiga dc2.8xlarge node.

```

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

```

Jika Anda memiliki node cadangan, misalnya node cadangan DC2, Anda dapat meningkatkan ke node cadangan RA3. Anda dapat melakukan ini saat memulihkan dari snapshot atau melakukan pengubahan ukuran elastis. Anda dapat menggunakan konsol untuk memandu Anda melalui proses ini. Untuk informasi selengkapnya tentang memutakhirkan ke node RA3, lihat [Memutakhirkan ke tipe node RA3](#).

Memulihkan tabel dari snapshot

Anda dapat memulihkan satu tabel dari snapshot alih-alih memulihkan seluruh cluster. Saat memulihkan satu tabel dari snapshot, Anda menentukan snapshot sumber, database, skema, dan nama tabel, serta database target, skema, dan nama tabel baru untuk tabel yang dipulihkan.

Nama tabel baru tidak bisa menjadi nama tabel yang ada. Untuk mengganti tabel yang ada dengan tabel yang dipulihkan dari snapshot, ganti nama atau jatuhkan tabel yang ada sebelum Anda mengembalikan tabel dari snapshot.

Tabel target dibuat menggunakan definisi kolom tabel sumber, atribut tabel, dan atribut kolom kecuali untuk kunci asing. Untuk mencegah konflik karena dependensi, tabel target tidak mewarisi kunci

asing dari tabel sumber. Dependensi apa pun, seperti tampilan atau izin yang diberikan pada tabel sumber, tidak diterapkan ke tabel target.

Jika pemilik tabel sumber ada, maka pengguna database tersebut adalah pemilik tabel dipulihkan, asalkan pengguna memiliki izin yang cukup untuk menjadi pemilik relasi dalam database dan skema yang ditentukan. Jika tidak, tabel yang dipulihkan dimiliki oleh pengguna admin yang dibuat saat cluster diluncurkan.

Tabel yang dipulihkan kembali ke keadaan semula pada saat cadangan diambil. Ini termasuk aturan visibilitas transaksi yang ditentukan oleh kepatuhan Amazon Redshift terhadap isolasi [serial](#), yang berarti bahwa data akan segera terlihat dalam transaksi penerbangan yang dimulai setelah pencadangan.

Memulihkan tabel dari snapshot memiliki batasan berikut:

- Anda dapat memulihkan tabel hanya ke cluster yang sedang berjalan aktif dan dari snapshot yang diambil dari cluster itu.
- Anda dapat mengembalikan hanya satu tabel pada satu waktu.
- Anda tidak dapat memulihkan tabel dari snapshot cluster yang diambil sebelum cluster diubah ukurannya. Pengecualian adalah Anda dapat mengembalikan tabel setelah mengubah ukuran elastis jika jenis simpul tidak berubah.
- Dependensi apa pun, seperti tampilan atau izin yang diberikan pada tabel sumber, tidak diterapkan ke tabel target.
- Jika keamanan tingkat baris dihidupkan untuk tabel dipulihkan, Amazon Redshift mengembalikan tabel dengan keamanan tingkat baris diaktifkan.

Untuk mengembalikan tabel dari snapshot

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Clusters, lalu pilih cluster yang ingin Anda gunakan untuk mengembalikan tabel.
3. Untuk Tindakan, pilih Pulihkan tabel untuk menampilkan halaman Pulihkan tabel.
4. Masukkan informasi tentang snapshot, tabel sumber, dan tabel target yang akan digunakan, lalu pilih Pulihkan tabel.

Example Contoh: Memulihkan tabel dari snapshot menggunakan AWS CLI

Contoh berikut menggunakan `restore-table-from-cluster-snapshot` AWS CLI perintah untuk mengembalikan `my-source-table` tabel dari `sample-database` skema di `my-snapshot-id` Anda dapat menggunakan AWS CLI perintah `describe-table-restore-status` untuk meninjau status operasi pemulihan Anda. Contoh mengembalikan snapshot ke `mycluster-example` cluster dengan nama tabel baru. `my-new-table`

```
aws redshift restore-table-from-cluster-snapshot --cluster-identifier mycluster-  
example  
  
--new-table-name my-new-table  
--snapshot-identifier my-snapshot-id  
--source-database-name sample-  
database  
  
--source-table-name my-source-table
```

Berbagi snapshot

Anda dapat membagikan snapshot manual yang ada dengan akun AWS pelanggan lain dengan mengotorisasi akses ke snapshot. Anda dapat mengotorisasi hingga 20 untuk setiap snapshot dan 100 untuk setiap AWS Key Management Service (AWS KMS) kunci. Artinya, jika Anda memiliki 10 snapshot yang dienkrpsi dengan satu kunci KMS, maka Anda dapat mengotorisasi 10 AWS akun untuk memulihkan setiap snapshot, atau kombinasi lain yang menambahkan hingga 100 akun dan tidak melebihi 20 akun untuk setiap snapshot. Seseorang yang masuk sebagai pengguna di salah satu akun resmi kemudian dapat menjelaskan snapshot atau mengembalikannya untuk membuat cluster Amazon Redshift baru di bawah akun mereka. Misalnya, jika Anda menggunakan akun AWS pelanggan terpisah untuk produksi dan pengujian, pengguna dapat masuk menggunakan akun produksi dan berbagi snapshot dengan pengguna di akun pengujian. Seseorang yang masuk sebagai pengguna akun pengujian kemudian dapat memulihkan snapshot untuk membuat cluster baru yang dimiliki oleh akun pengujian untuk pengujian atau pekerjaan diagnostik.

Snapshot manual dimiliki secara permanen oleh akun AWS pelanggan tempat akun itu dibuat. Hanya pengguna di akun yang memiliki snapshot yang dapat mengotorisasi akun lain untuk mengakses snapshot, atau untuk mencabut otorisasi. Pengguna di akun resmi hanya dapat mendeskripsikan atau memulihkan snapshot apa pun yang telah dibagikan dengan mereka; mereka tidak dapat menyalin atau menghapus snapshot yang telah dibagikan dengan mereka. Otorisasi tetap berlaku sampai pemilik snapshot mencabutnya. Jika otorisasi dicabut, pengguna yang sebelumnya

berwenang kehilangan visibilitas snapshot dan tidak dapat meluncurkan tindakan baru apa pun yang mereferensikan snapshot. Jika akun sedang dalam proses memulihkan snapshot saat akses dicabut, pemulihan berjalan hingga selesai. Anda tidak dapat menghapus snapshot saat memiliki otorisasi aktif; Anda harus terlebih dahulu mencabut semua otorisasi.

AWS Akun pelanggan selalu diizinkan untuk mengakses snapshot yang dimiliki oleh akun. Upaya untuk mengotorisasi atau mencabut akses ke akun pemilik akan menerima kesalahan. Anda tidak dapat memulihkan atau menggambarkan snapshot yang dimiliki oleh akun AWS pelanggan yang tidak aktif.

Setelah Anda memiliki akses resmi ke akun AWS pelanggan, tidak ada pengguna di akun tersebut yang dapat melakukan tindakan apa pun pada snapshot kecuali mereka berperan dengan kebijakan yang memungkinkan mereka melakukannya.

- Pengguna di akun pemilik snapshot dapat mengotorisasi dan mencabut akses ke snapshot hanya jika mereka mengambil peran dengan kebijakan IAM yang memungkinkan mereka melakukan tindakan tersebut dengan spesifikasi sumber daya yang menyertakan snapshot. Misalnya, kebijakan berikut memungkinkan pengguna atau peran dalam AWS akun 012345678912 untuk mengotorisasi akun lain untuk mengakses snapshot bernama: my-snapshot20130829

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "redshift:AuthorizeSnapshotAccess",
        "redshift:RevokeSnapshotAccess"
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-snapshot20130829"
      ]
    }
  ]
}
```

- Pengguna di AWS akun yang telah dibagikan snapshot tidak dapat melakukan tindakan pada snapshot itu kecuali mereka memiliki izin yang mengizinkan tindakan tersebut. Anda dapat melakukan ini dengan menetapkan kebijakan untuk peran dan mengambil peran.

- Untuk membuat daftar atau mendeskripsikan snapshot, mereka harus memiliki kebijakan IAM yang memungkinkan tindakan tersebut. DescribeClusterSnapshots Kode berikut menunjukkan contoh:

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

- Untuk memulihkan snapshot, pengguna harus mengambil peran dengan kebijakan IAM yang memungkinkan RestoreFromClusterSnapshot tindakan dan memiliki elemen sumber daya yang mencakup cluster yang mereka coba buat dan snapshot. Misalnya, jika pengguna dalam akun 012345678912 telah berbagi snapshot my-snapshot20130829 dengan akun219876543210, untuk membuat klaster dengan memulihkan snapshot, pengguna dalam akun 219876543210 harus mengambil peran dengan kebijakan seperti berikut:

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

```
}
```

- Setelah akses ke snapshot dicabut dari AWS akun, tidak ada pengguna di akun itu yang dapat mengakses snapshot tersebut. Hal ini terjadi bahkan jika akun tersebut memiliki kebijakan IAM yang memungkinkan tindakan pada sumber snapshot yang dibagikan sebelumnya.

Mengelola snapshot menggunakan konsol

Amazon Redshift mengambil snapshot otomatis dan bertahap dari data Anda secara berkala dan menyimpannya ke Amazon S3. Selain itu, Anda dapat mengambil snapshot manual dari data Anda kapan pun Anda mau. Di bagian ini, Anda dapat menemukan cara mengelola snapshot Anda dari konsol Amazon Redshift. Untuk informasi selengkapnya tentang snapshot, lihat [Cuplikan dan cadangan Amazon Redshift](#).

Semua tugas snapshot di konsol Amazon Redshift dimulai dari daftar snapshot. Anda dapat memfilter daftar dengan menggunakan rentang waktu, jenis snapshot, dan cluster yang terkait dengan snapshot. Selain itu, Anda dapat mengurutkan daftar berdasarkan tanggal, ukuran, dan jenis snapshot. Bergantung pada jenis snapshot yang Anda pilih, Anda mungkin memiliki opsi berbeda yang tersedia untuk bekerja dengan snapshot.

Topik

- [Membuat jadwal snapshot](#)
- [Membuat snapshot manual](#)
- [Mengubah periode retensi snapshot manual](#)
- [Menghapus snapshot manual](#)
- [Menyalin snapshot otomatis](#)
- [Memulihkan cluster dari snapshot](#)
- [Memulihkan namespace tanpa server dari snapshot](#)
- [Berbagi snapshot kluster](#)
- [Mengonfigurasi salinan snapshot lintas wilayah untuk kluster yang tidak terenkripsi](#)
- [Konfigurasi salinan snapshot lintas wilayah untuk kluster yang AWS KMS dienkripsi](#)
- [Memodifikasi periode retensi untuk salinan snapshot lintas wilayah](#)

Membuat jadwal snapshot

Untuk mengontrol secara tepat kapan snapshot diambil, Anda dapat membuat jadwal snapshot dan melampirkannya ke satu atau lebih cluster. Anda dapat melampirkan jadwal saat membuat kluster atau dengan memodifikasi cluster. Untuk informasi selengkapnya, lihat [Jadwal snapshot otomatis](#).

Untuk membuat jadwal snapshot

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster, Snapshots, lalu pilih tab Jadwal Snapshot. Jadwal snapshot ditampilkan.
3. Pilih Tambahkan jadwal untuk menampilkan halaman untuk menambahkan jadwal.
4. Masukkan properti definisi jadwal, lalu pilih Tambahkan jadwal.
5. Pada halaman yang muncul, Anda dapat melampirkan cluster ke jadwal snapshot baru Anda, lalu pilih OK.

Membuat snapshot manual

Anda dapat membuat snapshot manual cluster dari daftar snapshot sebagai berikut. Atau, Anda dapat mengambil snapshot cluster di panel konfigurasi cluster. Untuk informasi selengkapnya, lihat [Membuat snapshot dari sebuah cluster](#).

Untuk membuat snapshot manual

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster, Snapshots, lalu pilih Buat snapshot. Halaman snapshot untuk membuat snapshot manual ditampilkan.
3. Masukkan properti definisi snapshot, lalu pilih Buat snapshot. Mungkin perlu beberapa waktu agar snapshot tersedia.

Mengubah periode retensi snapshot manual

Anda dapat mengubah periode retensi untuk snapshot manual dengan memodifikasi pengaturan snapshot.

Untuk mengubah periode retensi snapshot manual

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, Snapshots, lalu pilih snapshot manual untuk diubah.
3. Untuk Tindakan, pilih Pengaturan snapshot manual untuk menampilkan properti snapshot manual.
4. Masukkan properti yang direvisi dari definisi snapshot, lalu pilih Simpan.

Menghapus snapshot manual

Anda dapat menghapus snapshot manual dengan memilih satu atau lebih snapshot dalam daftar snapshot.

Untuk menghapus snapshot manual

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, Snapshots, lalu pilih snapshot yang akan dihapus.
3. Untuk Tindakan, pilih Hapus snapshot untuk menghapus snapshot.
4. Konfirmasikan penghapusan snapshot yang terdaftar, lalu pilih Hapus.

Menyalin snapshot otomatis

Snapshot otomatis dihapus secara otomatis saat periode retensi berakhir, saat Anda menonaktifkan snapshot otomatis, atau saat Anda menghapus klaster. Jika Anda ingin menyimpan snapshot otomatis, Anda dapat menyalinnya ke snapshot manual.

Untuk menyalin snapshot otomatis

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, Snapshots, lalu pilih snapshot yang akan disalin.
3. Untuk Tindakan, pilih Salin snapshot otomatis untuk menyalin snapshot.
4. Perbarui properti snapshot baru, lalu pilih Salin.

Memulihkan cluster dari snapshot

Saat Anda memulihkan cluster dari snapshot, Amazon Redshift membuat cluster baru dengan semua data snapshot di cluster baru.

Untuk memulihkan cluster dari snapshot

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, Snapshots, lalu pilih snapshot untuk dipulihkan.
3. Pilih Pulihkan dari snapshot untuk melihat konfigurasi Cluster dan nilai detail Cluster dari cluster baru yang akan dibuat menggunakan informasi snapshot.
4. Perbarui properti cluster baru, lalu pilih Pulihkan cluster dari snapshot.

Jika AWS Secrets Manager tidak mengelola kata sandi admin klaster Anda, Anda dapat membuatnya mengelola klaster yang dipulihkan dengan memilih Kelola kredensial admin AWS Secrets Manager di bagian konfigurasi Cluster dan menentukan kunci KSM. Jika tidak, cluster dipulihkan dengan kredensial admin yang dimilikinya pada saat snapshot diambil. Anda dapat memperbarui kredensial admin cluster di halaman detail cluster setelah memulihkannya.

Jika AWS Secrets Manager mengelola kata sandi admin klaster Anda pada saat tangkapan layar diambil, Anda harus terus menggunakan AWS Secrets Manager untuk mengelola kata sandi admin. Anda dapat memilih untuk tidak menggunakan rahasia setelah memulihkan klaster dengan memperbarui kredensial admin cluster di halaman detail cluster.

Jika Anda memiliki node cadangan, misalnya node cadangan DC2, Anda dapat meningkatkan ke node cadangan RA3. Anda dapat melakukan ini saat memulihkan dari snapshot atau melakukan pengubahan ukuran elastis. Anda dapat menggunakan konsol untuk memandu Anda melalui proses ini. Untuk informasi selengkapnya tentang memutakhirkan ke node RA3, lihat [Memutakhirkan ke tipe node RA3](#).

Memulihkan namespace tanpa server dari snapshot

Memulihkan namespace tanpa server dari snapshot menggantikan semua database namespace dengan database di snapshot. Untuk informasi selengkapnya tentang snapshot tanpa server, lihat [Bekerja dengan snapshot](#) dan titik pemulihan. Amazon Redshift secara otomatis mengonversi tabel dengan kunci interleaved menjadi kunci majemuk saat Anda memulihkan snapshot klaster yang disediakan ke namespace Amazon Redshift Tanpa Server. Untuk informasi selengkapnya tentang kunci sortir, lihat [Bekerja dengan kunci sortir](#).

Untuk memulihkan snapshot dari klaster yang disediakan ke namespace tanpa server Anda.

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Clusters, Snapshots, lalu pilih snapshot yang akan digunakan.
3. Pilih Pulihkan dari snapshot, Pulihkan ke namespace tanpa server.
4. Pilih namespace yang ingin Anda pulihkan.
5. Konfirmasikan bahwa Anda ingin memulihkan dari snapshot Anda. Pilih pulihkan. Tindakan ini menggantikan semua database di namespace tanpa server dengan data dari klaster yang disediakan.

Berbagi snapshot klaster

Anda dapat mengotorisasi pengguna lain untuk mengakses snapshot manual yang Anda miliki, dan Anda nantinya dapat mencabut akses tersebut ketika tidak lagi diperlukan.

Untuk berbagi snapshot dengan akun lain

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster, Snapshots, lalu pilih snapshot manual untuk dibagikan.
3. Untuk Tindakan, pilih Pengaturan snapshot manual untuk menampilkan properti snapshot manual.
4. Masukkan akun atau akun untuk dibagikan di bagian Kelola akses, lalu pilih Simpan.

Pertimbangan keamanan untuk berbagi snapshot terenkripsi

Saat Anda memberikan akses ke snapshot terenkripsi, Redshift mengharuskan kunci terkelola pelanggan AWS KMS yang digunakan untuk membuat snapshot dibagikan dengan akun atau akun yang melakukan pemulihan. Jika kunci tidak dibagikan, mencoba memulihkan snapshot menghasilkan kesalahan yang ditolak akses. Akun penerima tidak memerlukan izin tambahan untuk memulihkan snapshot bersama. Saat Anda mengotorisasi akses snapshot dan membagikan kunci, akses otorisasi identitas harus memiliki `kms:DescribeKey` izin pada kunci yang digunakan untuk mengenkripsi snapshot. Izin ini dijelaskan secara lebih rinci dalam [AWS KMS izin](#). Untuk informasi selengkapnya, lihat [DescribeKey](#) di dokumentasi referensi Amazon Redshift API.

Kebijakan kunci yang dikelola pelanggan dapat diperbarui secara terprogram atau di konsol. AWS Key Management Service

Mengizinkan akses ke kunci AWS KMS untuk snapshot terenkripsi

Untuk membagikan kunci terkelola pelanggan AWS KMS untuk snapshot terenkripsi, perbarui kebijakan kunci dengan melakukan langkah-langkah berikut:

1. Perbarui kebijakan kunci KMS dengan Nama Sumber Daya Amazon (ARN) akun AWS yang Anda bagikan `Principal` seperti dalam kebijakan kunci KMS.
2. Izinkan `kms:Decrypt` tindakan.

Dalam contoh kebijakan kunci berikut, pengguna `111122223333` adalah pemilik kunci KMS, dan pengguna `444455556666` adalah akun tempat kunci dibagikan. Kebijakan kunci ini memberikan akses AWS akun ke contoh kunci KMS dengan menyertakan ARN untuk identitas akun AWS root bagi `444455556666` pengguna `Principal` sebagai kebijakan, dan dengan mengizinkan `kms:Decrypt` tindakan.

```
{
  "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": "*"
    }
  ]
}
```


Setelah akses diberikan ke kunci KMS yang dikelola pelanggan, akun yang mengembalikan snapshot terenkripsi harus membuat peran AWS Identity and Access Management (IAM), atau pengguna, jika belum memilikinya. Selain itu, AWS akun tersebut juga harus melampirkan kebijakan IAM ke peran IAM atau pengguna yang memungkinkan mereka memulihkan snapshot database terenkripsi, menggunakan kunci KMS Anda.

Untuk informasi selengkapnya tentang memberikan akses ke AWS KMS kunci, lihat [Mengizinkan pengguna di akun lain menggunakan kunci KMS](#), di panduan AWS Key Management Service pengembang.

Untuk ikhtisar kebijakan utama, lihat [Cara Amazon Redshift menggunakan AWS KMS](#)

Mengonfigurasi salinan snapshot lintas wilayah untuk kluster yang tidak terenkripsi

Anda dapat mengonfigurasi Amazon Redshift untuk menyalin snapshot untuk cluster ke Wilayah lain. AWS Untuk mengonfigurasi salinan snapshot lintas wilayah, Anda perlu mengaktifkan fitur salin ini untuk setiap cluster dan mengonfigurasi tempat menyalin snapshot dan berapa lama untuk menyimpan snapshot otomatis atau manual yang disalin di Wilayah tujuan. AWS Saat salinan lintas wilayah diaktifkan untuk kluster, semua snapshot manual dan otomatis baru disalin ke Wilayah yang ditentukan. AWS Nama snapshot yang disalin diawali dengan. **copy**:

Untuk mengonfigurasi snapshot Lintas wilayah

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Clusters, lalu pilih cluster yang ingin Anda pindahkan snapshot.
3. Untuk Tindakan, pilih Konfigurasi snapshot lintas wilayah.

Kotak dialog Configure Cross-region muncul.

4. Untuk Salin snapshot, pilih Ya.
5. Di AWS Wilayah Tujuan, pilih AWS Wilayah untuk menyalin snapshot.
6. Di Periode retensi snapshot otomatis (hari), pilih jumlah hari yang Anda inginkan agar snapshot otomatis disimpan di AWS Wilayah tujuan sebelum dihapus.
7. Di Periode retensi snapshot manual, pilih nilai yang mewakili jumlah hari yang Anda inginkan snapshot manual disimpan di AWS Wilayah tujuan sebelum dihapus. Jika Anda memilih Nilai kustom, periode retensi harus antara 1 hingga 3653 hari.
8. Pilih Simpan.

Konfigurasi salinan snapshot lintas wilayah untuk kluster yang AWS KMS dienkripsi

Saat meluncurkan kluster Amazon Redshift, Anda dapat memilih untuk mengenkripsinya dengan kunci root dari (). AWS Key Management Service AWS KMS kunci khusus untuk suatu AWS Wilayah. Jika Anda ingin mengaktifkan salinan snapshot lintas wilayah untuk kluster AWS KMS —terenkripsi, Anda harus mengonfigurasi hibah salinan snapshot untuk kunci root di Wilayah tujuan. AWS Dengan melakukan ini, Anda mengaktifkan Amazon Redshift untuk melakukan operasi enkripsi di Wilayah tujuan AWS .

Prosedur berikut menjelaskan proses mengaktifkan salinan snapshot lintas wilayah untuk cluster - enkripsi. AWS KMS Untuk informasi selengkapnya tentang enkripsi di Amazon Redshift dan hibah salinan snapshot, lihat. [Menyalin AWS KMS—snapshot terenkripsi ke Wilayah lain AWS](#)

Untuk mengonfigurasi snapshot Lintas wilayah untuk kluster —terenkripsi AWS KMS

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Clusters, lalu pilih cluster yang ingin Anda pindahkan snapshot.
3. Untuk Tindakan, pilih Konfigurasi snapshot lintas wilayah.

Kotak dialog Configure Cross-region muncul.

4. Untuk Salin snapshot, pilih Ya.
5. Di AWS Wilayah Tujuan, pilih AWS Wilayah untuk menyalin snapshot.
6. Di Periode retensi snapshot otomatis (hari), pilih jumlah hari yang Anda inginkan agar snapshot otomatis disimpan di AWS Wilayah tujuan sebelum dihapus.
7. Di Periode retensi snapshot manual, pilih nilai yang mewakili jumlah hari yang Anda inginkan snapshot manual disimpan di AWS Wilayah tujuan sebelum dihapus. Jika Anda memilih Nilai kustom, periode retensi harus antara 1 hingga 3653 hari.
8. Pilih Simpan.

Memodifikasi periode retensi untuk salinan snapshot lintas wilayah

Setelah mengonfigurasi salinan snapshot lintas wilayah, Anda mungkin ingin mengubah pengaturan. Anda dapat dengan mudah mengubah periode retensi dengan memilih jumlah hari baru dan menyimpan perubahan.

⚠ Warning

Anda tidak dapat mengubah AWS Wilayah tujuan setelah salinan snapshot lintas wilayah dikonfigurasi.

Jika Anda ingin menyalin snapshot ke AWS Wilayah lain, nonaktifkan salinan snapshot lintas wilayah terlebih dahulu. Kemudian aktifkan kembali dengan AWS Wilayah tujuan baru dan periode retensi. Setiap snapshot otomatis yang disalin akan dihapus setelah Anda menonaktifkan salinan snapshot lintas wilayah. Dengan demikian, Anda harus menentukan apakah ada yang ingin Anda simpan dan menyalinnya ke snapshot manual sebelum menonaktifkan salinan snapshot lintas wilayah.

Untuk memodifikasi snapshot Lintas wilayah

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Clusters, lalu pilih cluster yang ingin Anda ubah snapshot.
3. Untuk Tindakan, pilih Konfigurasi snapshot lintas wilayah untuk menampilkan properti snapshot.
4. Masukkan properti yang direvisi dari definisi snapshot, lalu pilih Simpan.

Mengelola snapshot menggunakan API Amazon AWS CLI Redshift dan Amazon

Anda dapat menggunakan operasi Amazon Redshift CLI berikut untuk mengelola snapshot.

- [otorisasi-snapshot-akses](#)
- [copy-cluster-snapshot](#)
- [buat-kluster-snapshot](#)
- [hapus-cluster-snapshot](#)
- [jelaskan-cluster-snapshots](#)
- [nonaktifkan-snapshot-copy](#)
- [aktifkan-snapshot-copy](#)
- [memodifikasi-snapshot-copy-retensi-periode](#)
- [pulihkan-dari-cluster-snapshot](#)
- [mencabut-snapshot-akses](#)

Anda dapat menggunakan tindakan Amazon Redshift API berikut untuk mengelola snapshot.

- [AuthorizeSnapshotAkses](#)
- [CopyClusterCuplikan](#)
- [CreateClusterCuplikan](#)
- [DeleteClusterCuplikan](#)
- [DescribeClusterCuplikan](#)
- [DisableSnapshotSalin](#)
- [EnableSnapshotSalin](#)
- [ModifySnapshotCopyRetentionPeriode](#)
- [RestoreFromClusterSnapshot](#)
- [RevokeSnapshotAkses](#)

Untuk informasi selengkapnya tentang snapshot Amazon Redshift, lihat. [Cuplikan dan cadangan Amazon Redshift](#)

Bekerja dengan AWS Backup

AWS Backup adalah layanan yang dikelola sepenuhnya yang membantu Anda memusatkan dan mengotomatiskan perlindungan data di seluruh AWS layanan, di cloud, dan di tempat.

Menggunakan AWS Backup Amazon Redshift, Anda dapat mengonfigurasi kebijakan perlindungan data dan memantau aktivitas untuk sumber daya Amazon Redshift yang berbeda di satu tempat. Anda juga dapat membuat dan menyimpan snapshot di kluster yang disediakan Amazon Redshift. Ini memungkinkan Anda mengotomatiskan dan mengkonsolidasikan tugas pencadangan yang harus Anda lakukan secara terpisah sebelumnya, tanpa proses manual apa pun.

Pencadangan, atau titik pemulihan, mewakili konten sumber daya, seperti kluster Amazon Redshift, pada waktu yang ditentukan. Cadangan umumnya mengacu pada cadangan yang berbeda dalam AWS layanan, seperti snapshot Amazon Redshift. AWS Backup menyimpan cadangan di brankas cadangan, yang dapat Anda atur sesuai dengan kebutuhan bisnis Anda. Istilah titik pemulihan dan cadangan digunakan secara bergantian. Untuk informasi selengkapnya AWS Backup, lihat [Bekerja dengan cadangan](#).

Amazon Redshift terintegrasi secara native dengan AWS Backup. Hal itu memungkinkan Anda menentukan paket cadangan dan menetapkan sumber daya Amazon Redshift ke paket cadangan. AWS Backup mengotomatiskan pembuatan snapshot manual Amazon Redshift, dan menyimpan

snapshot ini dengan aman di brankas cadangan terenkripsi yang Anda tetapkan dalam paket cadangan Anda. Untuk informasi tentang brankas, lihat [Bekerja dengan vault cadangan](#). Dalam paket cadangan, Anda dapat menentukan frekuensi cadangan, jendela cadangan, siklus hidup, atau vault cadangan. Untuk informasi tentang rencana cadangan, lihat [Mengelola cadangan menggunakan paket cadangan](#).

Topik

- [Pertimbangan untuk menggunakan AWS Backup dengan Amazon Redshift](#)
- [Mengelola AWS Backup dengan Amazon Redshift](#)

Pertimbangan untuk menggunakan AWS Backup dengan Amazon Redshift

Bagian berikut menjelaskan pertimbangan dan batasan penggunaan AWS Backup dengan Amazon Redshift.

Pertimbangan untuk menggunakan AWS Backup dengan Amazon Redshift

Berikut ini adalah pertimbangan untuk digunakan AWS Backup dengan Amazon Redshift:

- AWS Backup untuk Amazon Redshift tersedia di mana keduanya AWS Backup dan Amazon Redshift tersedia dalam hal yang sama Wilayah AWS. Untuk informasi tentang di mana AWS Backup tersedia, lihat [Ketersediaan fitur oleh Wilayah AWS](#).
- Untuk mulai menggunakan AWS Backup, verifikasi bahwa Anda telah memenuhi semua prasyarat. Untuk informasi selengkapnya, lihat [Prasyarat](#).
- Afirmasi memilih untuk AWS Backup layanan. Pilihan keikutsertaan berlaku untuk akun tertentu dan Wilayah AWS. Anda mungkin harus memilih masuk ke beberapa Wilayah menggunakan akun yang sama. Untuk informasi selengkapnya, lihat [Memulai 1: Penyisihan Layanan](#).
- Dari konsol Amazon Redshift, Anda dapat membuat snapshot manual dan otomatis. AWS Backupnya mendukung snapshot manual saat ini.
- Setelah Anda menggunakan AWS Backup untuk mengelola pengaturan snapshot, Anda tidak dapat terus mengelola pengaturan snapshot manual menggunakan Amazon Redshift. Sebagai gantinya, Anda dapat terus mengelola pengaturan menggunakan AWS Backup paket. Untuk informasi selengkapnya, lihat [Mengelola backup menggunakan rencana cadangan](#).
- Untuk menghemat biaya penyimpanan saat Anda memiliki bucket Amazon S3 yang diaktifkan versi untuk dicadangkan, sebaiknya tetapkan aturan kedaluwarsa siklus hidup. Untuk informasi selengkapnya tentang menentukan aturan siklus hidup, lihat [Contoh 6: Menentukan aturan siklus hidup untuk bucket yang diaktifkan versioning-nya](#). Jika Anda tidak menetapkan periode

kedaluwarsa siklus hidup, biaya penyimpanan Amazon Redshift Anda mungkin meningkat, karena AWS Backup menyimpan semua versi data Amazon Redshift Anda.

Keterbatasan:

Berikut ini adalah batasan untuk menggunakan AWS Backup di Amazon Redshift:

- Anda tidak dapat menggunakan AWS Backup untuk mengelola snapshot otomatis Amazon Redshift. Untuk mengelola snapshot otomatis, gunakan tag. Untuk informasi tentang pemberian tag sumber daya, lihat [Menandai sumber daya di Amazon Redshift](#).
- AWS Backup tidak mendukung Amazon Redshift Tanpa Server.

Mengelola AWS Backup dengan Amazon Redshift

Untuk melindungi sumber daya pada kluster yang disediakan Amazon Redshift, Anda dapat menggunakan AWS Backup konsol, atau menggunakan AWS Backup API atau AWS Command Line Interface (AWS CLI) secara terprogram. Bila Anda perlu memulihkan sumber daya, Anda dapat menggunakan AWS Backup konsol atau AWS CLI untuk menemukan dan memulihkan sumber daya yang Anda butuhkan. Untuk informasi selengkapnya, lihat [AWS Command Line Interface](#).

Saat menggunakan AWS Backup untuk Amazon Redshift, Anda dapat melakukan tindakan berikut:

- Buat cadangan berkala yang secara otomatis memulai snapshot Amazon Redshift. Backup berkala berguna untuk memenuhi kebutuhan retensi data jangka panjang Anda. Untuk informasi selengkapnya, lihat [backup Amazon Redshift](#).
- Otomatiskan penjadwalan dan retensi cadangan dengan mengonfigurasi rencana cadangan secara terpusat.
- Kembalikan cluster ke cadangan tersimpan yang Anda pilih. Anda mengatur seberapa sering mencadangkan sumber daya Anda. Untuk informasi selengkapnya, lihat [Mengembalikan kluster Amazon Redshift](#).

Mengkonfigurasi penyebaran Multi-AZ

Amazon Redshift mendukung beberapa penerapan Availability Zones (Multi-AZ) untuk kluster RA3 yang disediakan. Dengan menggunakan penerapan Multi-AZ, gudang data Amazon Redshift Anda dapat terus beroperasi dalam skenario kegagalan saat peristiwa tak terduga terjadi di Availability Zone. Penerapan multi-AZ menyebarkan sumber daya komputasi di dua Availability Zones (AZ)

dan sumber daya komputasi ini dapat diakses melalui satu titik akhir. Jika terjadi kegagalan seluruh Availability Zone, sumber daya komputasi yang tersisa di Availability Zone kedua tersedia untuk melanjutkan pemrosesan beban kerja. Amazon Redshift mengenakan tarif komputasi per jam yang sama untuk RA3 saat menjalankan gudang data Multi-AZ. Biaya penyimpanan tetap sama seperti yang dibagikan di semua Availability Zone di dalam dan Wilayah AWS.

Saat ini, Amazon Redshift mendukung nol Recovery Point Objective (RPO) yang memungkinkan data menjadi terkini dan up-to-date jika terjadi kegagalan. Dengan penerapan Multi-AZ, Amazon Redshift semakin meningkatkan kemampuan pemulihan yang ada dan mengurangi Recovery Time Objective (RTO). Hal ini dimungkinkan karena penerapan Multi-AZ dapat pulih lebih cepat dari kegagalan atau bencana sehingga meningkatkan Perjanjian Tingkat Layanan Amazon Redshift (SLA) menjadi 99,99% dibandingkan dengan 99,9% dengan gudang data AZ tunggal.

Menyiapkan penyebaran Multi-AZ

Untuk mengatur penyebaran Multi-AZ, pilih opsi Multi-AZ dan tentukan jumlah node komputasi yang akan disediakan di setiap Availability Zone. Amazon Redshift secara otomatis menyebarkan sumber daya komputasi yang sama di dua Availability Zone dan semua sumber daya komputasi selalu tersedia untuk pemrosesan baca dan tulis selama operasi normal. Hal ini memungkinkan penyebaran multi-AZ untuk bertindak sebagai gudang data tunggal dengan titik akhir tunggal, menghilangkan kebutuhan untuk perubahan aplikasi ketika bencana terjadi. Meskipun penerapan Multi-AZ memproses kueri individual menggunakan sumber daya komputasi yang hanya berada di satu Availability Zone, ia dapat secara otomatis mendistribusikan pemrosesan beberapa kueri simultan ke kedua Availability Zone untuk meningkatkan throughput keseluruhan untuk beban kerja konkurensi yang tinggi.

Anda juga dapat mengonversi gudang data Single-AZ yang ada menjadi gudang data multi-AZ atau sebaliknya. Semuanya tetap sama kecuali sumber daya komputasi tambahan disediakan di Availability Zone kedua. Saat bermigrasi ke Multi-AZ dari cluster single-AZ yang ada, Anda mungkin diminta untuk menggandakan jumlah node cluster yang dibutuhkan, untuk memfasilitasi performa kueri tunggal yang dipertahankan. Sebagian besar beban kerja mengamati peningkatan throughput pemrosesan kueri secara keseluruhan dengan gudang data multi-AZ karena ada dua kali jumlah sumber daya komputasi yang tersedia.

Jika terjadi kegagalan di Availability Zone, Amazon Redshift terus beroperasi dengan menggunakan sumber daya di Availability Zone yang tersisa secara otomatis. Namun, koneksi pengguna mungkin terputus dan harus dibangun kembali. Selain itu, kueri yang berjalan di Availability Zone yang gagal dapat gagal dan harus dicoba ulang. Namun, Anda dapat menyambung kembali ke klaster dan

menjadwal ulang kueri dengan segera, dan Amazon Redshift akan memproses kueri di Availability Zone yang tersisa. Kueri yang dikeluarkan pada atau setelah kegagalan terjadi mungkin mengalami penundaan runtime saat gudang data multi-AZ pulih.

Note

Untuk mencapai kinerja yang lebih baik dan ketersediaan yang lebih tinggi, kami sarankan Anda menggunakan ISOLASI SNAPSHOT dengan cluster multi-AZ Anda. Untuk informasi selengkapnya, lihat [MEMBUAT DATABASE](#).

Batasan

Gudang data multi-AZ memiliki kemampuan fungsional yang sama dengan gudang data Single-AZ, kecuali untuk batasan berikut yang berlaku untuk gudang data multi-AZ:

- Anda tidak dapat membuat gudang data Multi-AZ yang tidak terenkripsi. Pastikan untuk menambahkan enkripsi saat membuat gudang data multi-AZ baru, mengubah gudang data Single-AZ menjadi gudang data multi-AZ, atau mengubah gudang data Single-AZ menjadi gudang data multi-AZ.
- Anda tidak dapat membuat penerapan multi-AZ node tunggal untuk salah satu jenis instans RA3. Pilih 2 atau lebih node per Availability Zone saat membuat penerapan Multi-AZ.
- Amazon Redshift tidak mendukung konfigurasi subnet yang dapat mendukung kurang dari tiga Availability Zone. Dengan kata lain, grup subnet yang dikonfigurasi membutuhkan tiga subnet lagi.
- Anda tidak dapat memindahkan penerapan Multi-AZ ke Availability Zone lain. Relokasi akan ditentukan dan dilakukan secara otomatis oleh Amazon Redshift saat menggunakan penerapan Multi-AZ.
- Anda tidak dapat menjeda atau melanjutkan penerapan Multi-AZ.
- Anda tidak dapat menjalankan penerapan Multi-AZ di luar rentang port yang didukung 5431 hingga 5455 dan 8191 hingga 8215.
- Anda tidak dapat menggunakan tampilan STL, SVCS, SVL, SVV, STV dengan penerapan multi-AZ karena hanya mendukung tampilan pemantauan sistem (tampilan SYS_*). Ubah kueri pemantauan Anda untuk menggunakan tampilan pemantauan sistem (tampilan SYS_*).
- Anda tidak dapat melampirkan alamat IP Elastis ke cluster yang ada dengan Multi-AZ diaktifkan.
- Anda tidak dapat mengonversi cluster dengan alamat IP Elastis terlampir dari Single-AZ ke Multi-AZ.

- Penyebaran Multi-AZ Amazon Redshift tersedia dalam hal berikut: Wilayah AWS
 - AS Timur (Ohio) (us-east-2)
 - US East (N. Virginia) (us-east-1)
 - US West (Oregon) (us-west-2)
 - Africa (Cape Town) (af-south-1)
 - Asia Pacific (Hong Kong) (ap-east-1)
 - Asia Pasifik (Hyderabad) (ap-south-2)
 - Asia Pasifik (Jakarta) (ap-southeast-3)
 - Asia Pasifik (Melbourne) (ap-southeast-4)
 - Asia Pasifik (Mumbai) (ap-south-1)
 - Asia Pasifik (Osaka) (ap-northeast-3)
 - Asia Pasifik (Seoul) (ap-northeast-2)
 - Asia Pasifik (Singapura) (ap-southeast-1)
 - Asia Pacific (Sydney) (ap-southeast-2)
 - Asia Pacific (Tokyo) (ap-northeast-1)
 - Kanada (Pusat) (ca-central-1)
 - Eropa (Frankfurt) (eu-central-1)
 - Eropa (Irlandia) (eu-west-1)
 - Europe (Milan) (eu-south-1)
 - Eropa (Paris) (eu-west-3)
 - Eropa (Spanyol) (eu-south-2)
 - Eropa (Stockholm) (eu-north-1)
 - Eropa (Zurich) (eu-central-2)
 - Israel (Tel Aviv) (il-central-1)
 - Middle East (Bahrain) (me-south-1)
 - Timur Tengah (UEA) (me-central-1)

Topik

- [Mengelola penyebaran Multi-AZ](#)
- [Gagal dalam penerapan Multi-AZ](#)
- [Pemantauan kueri untuk Multi-AZ](#)

Mengelola penyebaran Multi-AZ

Amazon Redshift Multi-AZ mendukung dua Availability Zone sekaligus. Amazon Redshift secara otomatis memilih Availability Zones berdasarkan konfigurasi grup subnet yang dipilih. Anda dapat mengonversi gudang data Availability Zone tunggal yang ada menjadi gudang data Multi-AZ atau memulihkan dari snapshot untuk mengonfigurasinya menjadi gudang data Multi-AZ.

Menggunakan konsol Amazon Redshift, Anda dapat dengan mudah membuat penerapan Multi-AZ baru. Untuk membuat penyebaran Multi-AZ baru menggunakan konsol Amazon Redshift, pilih opsi Multi-AZ saat membuat gudang data. Tentukan jumlah node komputasi yang diperlukan dalam satu Availability Zone, dan Amazon Redshift akan menerapkan jumlah node tersebut di masing-masing dari dua Availability Zone. Semua node akan digunakan untuk membaca dan menulis pemrosesan beban kerja selama operasi normal. Anda juga dapat menggunakan AWS CLI `create-cluster` perintah untuk membuat gudang data Multi-AZ baru menggunakan `multi-az` parameter.

Anda dapat mengonversi gudang data Single-AZ yang ada menjadi gudang data multi-AZ, Anda dapat menggunakan konsol Amazon Redshift atau perintah menggunakan AWS CLI `modify-cluster` parameter. `multi-az` Atau, Anda dapat memulihkan dari snapshot untuk mengonfigurasi gudang data Single-AZ ke gudang data multi-AZ baik menggunakan konsol Amazon Redshift atau perintah menggunakan parameter. AWS CLI `restore-from-cluster-snapshot` `multi-az`

Penerapan multi-AZ hanya mendukung tipe node RA3 yang menggunakan Amazon Redshift Managed Storage (RMS). Amazon Redshift menyimpan data dalam RMS, yang menggunakan Amazon S3 dan dapat diakses di semua Availability Zone di Wilayah AWS, tanpa harus mereplikasi data di tingkat Amazon Redshift.

Menyiapkan Multi-AZ saat membuat cluster baru

Anda dapat mengatur penerapan Multi-AZ saat membuat klaster baru baik menggunakan konsol Amazon Redshift atau. AWS Command Line Interface

Menggunakan konsol

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Dasbor cluster yang disediakan, dan pilih Cluster. Cluster untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih tombolnya Buat cluster untuk membuka halaman buat cluster.

4. Masukkan properti untuk cluster Anda. Untuk informasi umum tentang membuat cluster, lihat [Membuat klaster](#).
5. Pilih salah satu tipe node RA3 dari daftar drop-down tipe Node. Opsi konfigurasi AZ hanya tersedia ketika Anda memilih tipe simpul RA3.
6. Di bawah konfigurasi AZ, pilih Multi-AZ.
7. Di bawah Jumlah node per AZ, masukkan setidaknya dua node untuk cluster Anda.
8. Anda memiliki opsi untuk memuat data sampel atau membawa data Anda sendiri:
 - Dalam Data sampel, pilih Muat data sampel untuk memuat kumpulan data sampel ke dalam klaster Amazon Redshift Anda. Amazon Redshift memuat kumpulan data sampel Tikit ke dalam database dev default dan skema publik. Amazon Redshift secara otomatis memuat kumpulan data sampel ke cluster Amazon Redshift Anda. Anda dapat mulai menggunakan editor kueri v2 untuk menanyakan data.
 - Untuk membawa data Anda sendiri ke cluster Amazon Redshift, ikuti langkah-langkah dalam [Membawa data Anda sendiri ke Amazon Redshift](#).
9. Gulir ke bawah ke Konfigurasi tambahan, perluas Jaringan dan keamanan, dan pastikan Anda menerima grup subnet Cluster default atau memilih yang lain. Jika Anda memilih grup subnet cluster lain, pastikan ada 3 Availability Zones di grup subnet yang Anda pilih.
10. Di bawah Konfigurasi tambahan, perluas konfigurasi Database.
11. Untuk menggunakan kunci kustom alih-alih AWS KMS AWS Key Management Service kunci default, klik Sesuaikan pengaturan enkripsi di bawah Enkripsi basis data.
12. Di bawah Pilih tombol KMS, Anda dapat memilih AWS Key Management Service kunci atau memasukkan ARN. Atau, Anda dapat mengklik Buat AWS Key Management Service kunci di AWS Key Management Service konsol. Untuk informasi selengkapnya tentang membuat kunci KMS, lihat [Membuat Kunci](#) di Panduan AWS Key Management Service Pengembang.
13. Klik Buat klaster. Ketika pembuatan cluster berhasil, Anda dapat melihat detail di halaman detail cluster. Anda dapat menggunakan klien SQL Anda untuk memuat dan menanyakan data.

Menggunakan AWS Command Line Interface

Untuk mengatur Multi-AZ saat membuat cluster menggunakan AWS Command Line Interface

- Dari AWS CLI gunakan `create-cluster` perintah dan `multi-az` parameter sebagai berikut.

```
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
```

Mengonversi gudang data AZ tunggal menjadi gudang data multi-AZ

Dengan mengonversi gudang data AZ tunggal menjadi gudang data multi-AZ, gudang data Anda akan sangat tersedia dengan jaminan SLA 99,99%. Kinerja kueri individu akan tetap sama bahkan dengan gudang data multi-AZ. Untuk beban kerja konkurensi yang lebih tinggi, Anda akan melihat peningkatan dalam throughput keseluruhan karena Amazon Redshift dapat mengeksekusi permintaan menggunakan sumber daya komputasi di dua Availability Zone.

Note

Amazon Redshift tidak akan memungkinkan Anda untuk membagi sumber daya komputasi yang ada saat mengonversi dari Single-AZ ke Multi-AZ, atau sebaliknya. Operasi ini tidak didukung untuk mempertahankan kinerja kueri individual yang konsisten.

Menggunakan konsol

Untuk mengonversi cluster Single-AZ ke gudang data multi-AZ menggunakan konsol

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Dasbor cluster yang disediakan, dan pilih Cluster. Cluster untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih cluster yang ingin Anda konversi ke penyebaran multi-AZ. Halaman detail cluster muncul.
4. Untuk Tindakan, pilih Aktifkan Multi-AZ. Ringkasan modifikasi muncul. Klik Aktifkan Multi-AZ.

5. Ketika ada kesalahan, lakukan salah satu hal berikut, lalu klik Aktifkan Multi-AZ.
 - Enkripsi cluster - Pilih Properti untuk mengedit pengaturan enkripsi di bagian konfigurasi Database di bawah tab Properties pada halaman detail cluster.
 - Grup subnet - Pilih grup Subnet untuk mengedit pengaturan grup subnet cluster dengan mengklik tautan grup subnet. Jika Anda memilih grup subnet cluster lain, pastikan ada 3 Availability Zones di grup subnet yang Anda pilih.
 - Pengaturan port - Pilih Properti untuk mengedit pengaturan port di bagian konfigurasi Database di bawah tab Properties pada halaman detail cluster.
6. Anda dapat menggunakan klien SQL Anda untuk memuat dan menanyakan data.

Menggunakan AWS Command Line Interface

- Dari AWS CLI, gunakan `modify-cluster` perintah dan `multi-az` parameter sebagai berikut.

```
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
```

Mengonversi gudang data Multi-AZ menjadi gudang data AZ tunggal

Dengan mengonversi gudang data Multi-AZ menjadi gudang data AZ tunggal, gudang data Anda tidak akan mendapatkan jaminan SLA 99,99% yang ditawarkan Multi-AZ. Kinerja kueri individual akan tetap sama tetapi throughput keseluruhan akan terpengaruh karena sumber daya komputasi di Availability Zone kedua tidak akan tersedia. Anda memiliki opsi untuk mengaktifkan penskalaan konkurensi untuk menskalakan throughput secara otomatis untuk kinerja yang konsisten bahkan dengan AZ tunggal.

Note

Amazon Redshift tidak akan memungkinkan Anda untuk membagi sumber daya komputasi yang ada saat mengonversi dari Single-AZ ke Multi-AZ, atau sebaliknya. Operasi ini tidak didukung untuk mempertahankan kinerja kueri individual yang konsisten.

Menggunakan konsol

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Dasbor cluster yang disediakan, dan pilih Cluster. Cluster untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih cluster yang ingin Anda konversi ke penyebaran multi-AZ. Halaman detail cluster muncul.
4. Untuk Tindakan, pilih Nonaktifkan Multi-AZ. Ringkasan modifikasi muncul. Klik Nonaktifkan Multi-AZ.

Menggunakan AWS Command Line Interface

- Dari AWS CLI, gunakan `modify-cluster` perintah dan `no-multi-az` parameter sebagai berikut.

```
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
```

Setelah gudang data Anda dikonversi ke Single-AZ, itu akan kehilangan jaminan SLA 99,99. Secara keseluruhan throughput juga akan terpengaruh. Saat perubahan disimpan, Anda dapat melihat detailnya di halaman detail cluster.

Mengubah ukuran gudang data Multi-AZ

Anda dapat mengubah ukuran gudang data Multi-AZ dan menentukan sejumlah node atau tipe node yang berbeda dari konfigurasi gudang data saat ini.

Menggunakan konsol

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Pada menu navigasi, pilih Dasbor cluster yang disediakan, dan pilih Cluster. Cluster untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih cluster yang ingin Anda ubah ukuran gudang data Multi-AZ. Halaman detail cluster muncul.
4. Untuk Tindakan, pilih Ubah Ukuran. Halaman cluster Resize muncul.
5. Ikuti instruksi di halaman. Anda dapat mengubah ukuran cluster sekarang, sekali pada waktu tertentu, atau menambah dan mengurangi ukuran cluster Anda sesuai jadwal.
6. Di bawah Konfigurasi baru, pilih salah satu tipe node RA3 dari daftar drop-down tipe Node.
7. Klik Ubah ukuran cluster.

Menggunakan AWS Command Line Interface

Untuk mengubah ukuran gudang data Multi-AZ menggunakan AWS Command Line Interface

- Dari AWS CLI, gunakan `resize-cluster` perintah untuk mengubah jumlah node untuk Availability Zone tunggal sebagai berikut.

```
aws redshift resize-cluster \  
  --cluster-identifier test-maz-11 \  
  --cluster-type multi-node \  
  --node-type ra3.4xlarge \  
  --number-of-nodes 6
```

Menyiapkan Multi-AZ untuk gudang data yang dipulihkan dari snapshot

Anda juga dapat membuat cluster Multi-AZ baru dengan memulihkannya dari snapshot.

Menggunakan konsol

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Clusters, Snapshots, lalu pilih snapshot yang akan digunakan.
3. Pilih Pulihkan snapshot, Pulihkan ke klaster yang disediakan.
4. Masukkan properti untuk cluster Anda. Untuk informasi umum tentang membuat cluster, lihat [Membuat klaster](#).

5. Pilih salah satu tipe node RA3 dari daftar drop-down tipe Node. Opsi konfigurasi AZ hanya tersedia ketika Anda memilih tipe simpul RA3.
6. Di bawah konfigurasi AZ, pilih Multi-AZ.
7. Di bawah Jumlah node per AZ, masukkan setidaknya dua node untuk cluster Anda.
8. Anda memiliki opsi untuk memuat data sampel atau membawa data Anda sendiri:
 - Dalam Data sampel, pilih Muat data sampel untuk memuat kumpulan data sampel ke dalam kluster Amazon Redshift Anda. Amazon Redshift memuat kumpulan data sampel Tikit ke dalam database dev default dan skema publik. Amazon Redshift secara otomatis memuat kumpulan data sampel ke cluster Amazon Redshift Anda. Anda dapat mulai menggunakan editor kueri v2 untuk menanyakan data.
 - Untuk membawa data Anda sendiri ke cluster Amazon Redshift, ikuti langkah-langkah di [Muat data dari Amazon S3 ke Amazon Redshift](#).
9. Gulir ke bawah ke Konfigurasi tambahan, perluas Jaringan dan keamanan, dan pastikan Anda menerima grup subnet Cluster default atau memilih yang lain. Jika Anda memilih grup subnet cluster lain, pastikan ada 3 Availability Zones di grup subnet yang Anda pilih.
10. Di bawah Konfigurasi tambahan, perluas konfigurasi Database.
11. Di bawah Enkripsi basis data, untuk menggunakan kunci KMS khusus selain AWS Key Management Service kunci default, klik Sesuaikan pengaturan enkripsi. Opsi ini tidak dipilih secara default.
12. Di bawah Pilih tombol KMS, Anda dapat memilih AWS Key Management Service kunci atau memasukkan ARN. Atau, Anda dapat mengklik Buat AWS Key Management Service kunci di AWS Key Management Service konsol. Untuk informasi selengkapnya tentang membuat kunci KMS, lihat [Membuat Kunci](#) di Panduan AWS Key Management Service Pengembang.
13. Klik Pulihkan cluster dari snapshot. Ketika restorasi cluster berhasil, Anda dapat melihat detailnya di halaman detail cluster.

Menggunakan AWS Command Line Interface

- Dari AWS CLI, gunakan `restore-from-cluster-snapshot` perintah sebagai berikut.

```
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/
```

Gagal dalam penerapan Multi-AZ

Gudang data Multi-AZ Anda adalah sumber daya komputasi koleksi yang digunakan secara bersamaan di dua Availability Zone. Sumber daya komputasi yang digunakan di Availability Zone primer disebut sebagai komputasi primer dan yang ada di Availability Zone sekunder disebut sebagai komputasi sekunder. Gudang data multi-AZ dapat pulih secara otomatis tanpa campur tangan pengguna selama peristiwa yang tidak mungkin terjadi seperti Availability Zone atau kegagalan infrastruktur. Proses pemulihan melibatkan kegagalan dari komputasi primer ke komputasi sekunder dan menunjuk sumber daya komputasi sekunder sebagai primer. Selain itu, sumber daya komputasi sekunder baru disediakan di Availability Zone ketiga. Proses pemulihan otomatis diukur dalam hal RTO dan RPO.

- Tujuan waktu pemulihan (RTO) — Waktu yang dibutuhkan sistem untuk kembali ke kondisi kerja setelah bencana. Dengan kata lain, RTO mengukur waktu henti.
- Tujuan titik pemulihan (RPO) — Jumlah data yang dapat hilang (diukur dalam waktu). Untuk gudang data Amazon Redshift Multi-AZ, RPO biasanya nol karena semua data disimpan di Amazon Redshift Managed Storage (RMS), didukung oleh Amazon Simple Storage Service, yang sangat tahan lama dan tersedia secara default.

Note

Kinerja kinerja kueri individu tidak akan berubah setelah failover terjadi. Output keseluruhan gudang data Anda akan berkurang untuk waktu yang singkat karena tidak tersedianya sumber daya komputasi di salah satu Availability Zone. Namun, Amazon Redshift akan secara otomatis memperoleh kapasitas di Availability Zone lain untuk memastikan kapasitas pemrosesan gudang data yang sama dipulihkan.

Selain proses pemulihan otomatis, Anda juga dapat memicu proses ini secara manual untuk gudang data Anda menggunakan opsi komputasi utama Failover. Anda dapat menggunakan pendekatan ini untuk menguji bagaimana Multi-AZ akan membantu aplikasi Anda untuk ketersediaan tinggi yang lebih tinggi dan kontinuitas yang lebih baik.

Menggunakan konsol

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Lakukan salah satu hal berikut ini:
 - Pada menu navigasi, pilih Cluster. Di bawah Cluster, pilih cluster. Halaman detail cluster muncul.
 - Dari dasbor cluster, pilih cluster.
3. Dari Actions, pilih Failover primary compute.
4. Saat diminta, klik Konfirmasi.

Menggunakan AWS Command Line Interface

- Dari AWS CLI, gunakan `failover-primary-compute` perintah sebagai berikut.

```
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
```

Setelah operasi di atas dikonfirmasi, Amazon Redshift akan melakukan langkah yang sama seperti pemulihan otomatis dari Availability Zone atau kegagalan infrastruktur. Proses ini akan menyebabkan node komputasi di Availability Zone primer menjadi tidak tersedia dan sumber daya komputasi di Availability Zone sekunder akan ditetapkan sebagai komputasi utama. Ketika pemulihan cluster berhasil diselesaikan, penyebaran multi-AZ menjadi tersedia. Gudang data Multi-AZ Anda juga akan secara otomatis menyediakan komputasi sekunder baru di Availability Zone ketiga lainnya segera setelah tersedia.

Selama proses ini, status cluster di konsol ditampilkan sebagai modifikasi sepanjang waktu, karena cluster secara otomatis pulih dan mengkonfigurasi ulang kembali ke pengaturan penyebaran multi-AZ. Cluster dapat menerima koneksi baru dengan segera. Koneksi yang ada dan kueri dalam pesawat mungkin dibatalkan. Anda dapat mencobanya kembali segera.

Pemantauan kueri untuk Multi-AZ

Anda dapat melihat informasi tentang kueri yang berjalan dalam 7 hari terakhir terlepas dari jenis, ukuran, dan status (jeda atau lanjutkan) klaster Anda.

Melihat kueri dan beban untuk gudang data multi-AZ

Informasi yang ditampilkan pada halaman Kueri dan pemuatan diisi dengan informasi dari tabel sistem Amazon Redshift (tampilan SYS_*). Informasi ini memungkinkan Anda menampilkan informasi tambahan tentang kueri dan penawaran penyimpanan selama 7 hari. Diagnostik kueri menjadi lebih cepat, memungkinkan Anda memfilter data berdasarkan database, nama pengguna, atau jenis pernyataan SQL. Untuk melihat filter dan informasi tambahan ini tentang semua kueri yang dijalankan, perhatikan prasyarat berikut:

- Anda harus terhubung ke database dengan memilih Connect to database.
- Pengguna database Anda harus memiliki peran dan izin sys:operator atau sys:monitor untuk melakukan pemantauan kueri. Untuk informasi tentang peran sistem, lihat peran yang [ditetapkan sistem Amazon Redshift di Panduan Pengembang](#) Database Amazon Redshift.

Anda akan melihat filter tambahan dan informasi kueri setelah Anda terhubung ke database.

Untuk menampilkan data kinerja kueri dari Kueri dan beban

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Kueri dan beban untuk menampilkan daftar kueri untuk akun Anda.
3. Anda mungkin harus terhubung ke database untuk melihat filter tambahan. Jika diperlukan, klik Connect to database dan ikuti petunjuk untuk menyambung ke database.

Secara default, daftar menampilkan kueri untuk semua cluster Anda selama 24 jam terakhir. Anda dapat mengubah cakupan tanggal yang ditampilkan di konsol.

Untuk menampilkan data kinerja kueri dari pemantauan Query

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster. Di bawah Cluster, pilih cluster.

3. Pilih Pemantauan kueri.
4. Bergantung pada konfigurasi atau versi kluster Anda, Anda mungkin harus terhubung ke database untuk melihat filter tambahan. Jika diperlukan, klik Connect to database dan ikuti petunjuk untuk menyambung ke database.

Memantau kueri dalam penerapan Multi-AZ

Penerapan multi-AZ menggunakan sumber daya komputasi yang digunakan di kedua Availability Zone dan dapat terus beroperasi jika sumber daya di Availability Zone tertentu tidak tersedia. Semua sumber daya komputasi akan digunakan setiap saat. Hal ini memungkinkan operasi penuh di dua Availability Zone secara aktif-aktif untuk operasi baca dan tulis.

Anda dapat menanyakan tampilan SYS_ dalam skema pg_catalog untuk memantau runtime kueri dalam penerapan multi-AZ. Tampilan SYS_ menampilkan aktivitas runtime kueri atau statistik dari cluster primer dan sekunder. Untuk daftar tampilan pemantauan, lihat [Memantau tampilan](#).

Ikuti langkah-langkah berikut untuk memantau runtime kueri untuk setiap Availability Zone dalam penerapan Multi-AZ:

1. Arahkan ke konsol Amazon Redshift dan sambungkan ke database dalam penerapan Multi-AZ Anda dan jalankan kueri melalui editor kueri.
2. Jalankan kueri sampel apa pun pada penerapan Amazon Redshift Multi-AZ.
3. Untuk penerapan Multi-AZ, Anda dapat mengidentifikasi kueri dan Availability Zone di mana ia dijalankan dengan menggunakan kolom compute_type dalam tabel SYS_QUERY_HISTORY. primary adalah singkatan dari query yang dijalankan pada cluster primer dalam penyebaran multi-AZ, dan singkatan sekunder untuk query yang dijalankan pada cluster sekunder dalam penyebaran multi-AZ.

Query berikut menggunakan kolom compute_type untuk memantau query.

```
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;
```

Mengakhiri kueri untuk cluster

Mengakhiri kueri untuk cluster

Prosedur ini berlaku untuk cluster multi-AZ dan Single-AZ.

Untuk mengakhiri kueri

Anda juga dapat menggunakan halaman Kueri untuk mengakhiri kueri yang sedang berlangsung.

Pengguna database Anda harus memiliki peran dan izin sys:operator untuk mengakhiri kueri yang sedang berjalan. Untuk informasi tentang peran sistem, lihat peran yang [ditetapkan sistem Amazon Redshift di Panduan Pengembang](#) Database Amazon Redshift.

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Kueri dan beban untuk menampilkan daftar kueri untuk akun Anda.
3. Pilih kueri berjalan yang ingin Anda akhiri dalam daftar, lalu pilih Hentikan kueri.

Mengelola cluster menggunakan konsol

Untuk membuat, memodifikasi, mengubah ukuran, menghapus, reboot, dan mencadangkan cluster, gunakan bagian Clusters di konsol Amazon Redshift.

Untuk melihat cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster. Cluster untuk akun Anda di AWS Wilayah saat ini terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar. Jika Anda tidak memiliki cluster apa pun, pilih Buat cluster untuk membuatnya.
3. Pilih nama cluster dalam daftar untuk melihat detail selengkapnya tentang sebuah cluster.

Topik

- [Membuat klaster](#)
- [Membuat klaster pratinjau](#)

- [Mengubah klaster](#)
- [Menghapus klaster](#)
- [Melakukan boot ulang klaster](#)
- [Mengubah ukuran cluster](#)
- [Memutakhirkan versi rilis cluster](#)
- [Mendapatkan informasi tentang konfigurasi cluster](#)
- [Mendapatkan ikhtisar status cluster](#)
- [Membuat snapshot dari sebuah cluster](#)
- [Membuat atau mengedit alarm ruang disk](#)
- [Bekerja dengan data kinerja cluster](#)

Membuat klaster

Sebelum Anda membuat cluster, baca [Ikhtisar Amazon Redshift](#) dan [Cluster dan node di Amazon Redshift](#).

Untuk membuat klaster DB

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster. Cluster untuk akun Anda di AWS Wilayah saat ini terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih Buat cluster untuk membuat cluster.
4. Ikuti petunjuk di halaman konsol untuk memasukkan properti untuk konfigurasi Cluster.

Langkah berikut menjelaskan konsol Amazon Redshift yang berjalan di konsol Wilayah AWS yang mendukung tipe node RA3. Untuk daftar tipe node RA3 Wilayah AWS yang mendukung, lihat [Ringkasan jenis node RA3](#) di Panduan Manajemen Pergeseran Merah Amazon.

Jika Anda tidak tahu seberapa besar ukuran cluster Anda, pilih Bantu saya pilih. Melakukan hal ini memulai kalkulator ukuran yang menanyakan pertanyaan tentang ukuran dan karakteristik kueri data yang Anda rencanakan untuk disimpan di gudang data Anda. Jika Anda mengetahui ukuran cluster Anda yang diperlukan (yaitu, jenis node dan jumlah node), pilih yang akan saya pilih. Kemudian pilih jenis Node dan jumlah Node untuk mengukur cluster Anda untuk bukti konsep.

Note

Jika organisasi Anda memenuhi syarat dan klaster Anda sedang dibuat di Wilayah AWS tempat Amazon Redshift Tanpa Server tidak tersedia, Anda mungkin dapat membuat klaster di bawah program uji coba gratis Amazon Redshift. Pilih salah satu Produksi atau Uji coba gratis untuk menjawab pertanyaan Untuk apa Anda berencana menggunakan cluster ini? Saat Anda memilih Uji coba gratis, Anda membuat konfigurasi dengan tipe simpul dc2.large. Untuk informasi selengkapnya tentang memilih uji coba gratis, lihat uji coba [gratis Amazon Redshift](#). [Untuk daftar Wilayah AWS tempat Amazon Redshift Serverless tersedia, lihat titik akhir yang terdaftar untuk Redshift Serverless API di Referensi Umum Amazon Web Services](#)

5. Di bagian konfigurasi Database, tentukan nilai untuk nama pengguna Admin. Untuk kata sandi Admin, Anda dapat memilih dari opsi berikut:
 - Buat kata sandi — Gunakan kata sandi yang dihasilkan oleh Amazon Redshift.
 - Tambahkan kata sandi admin secara manual — Gunakan kata sandi Anda sendiri.
 - Kelola kredensi admin di AWS Secrets Manager — Amazon Redshift AWS Secrets Manager menggunakan untuk membuat dan mengelola kata sandi admin Anda. Menggunakan AWS Secrets Manager untuk menghasilkan dan mengelola rahasia kata sandi Anda menimbulkan biaya. Untuk informasi tentang AWS Secrets Manager harga, lihat [AWS Secrets Manager Harga](#).
6. (Opsional) Ikuti petunjuk di halaman konsol untuk memasukkan properti untuk izin Cluster. Berikan izin klaster jika klaster Anda perlu mengakses AWS layanan lain untuk Anda, misalnya untuk memuat data dari Amazon S3.
7. Pilih Buat cluster untuk membuat cluster. Cluster mungkin membutuhkan waktu beberapa menit untuk siap digunakan.

Konfigurasi tambahan

Saat membuat cluster, Anda dapat menentukan properti tambahan untuk menyesuaikannya. Anda dapat menemukan detail lebih lanjut tentang beberapa properti ini dalam daftar berikut.

Jenis alamat IP

Pilih jenis alamat IP untuk cluster Anda. Anda dapat memilih agar sumber daya Anda berkomunikasi hanya melalui protokol pengalamatan IPv4, atau memilih mode dual-stack, yang memungkinkan sumber daya Anda berkomunikasi melalui IPv4 dan IPv6. Fitur ini hanya tersedia di Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat). Untuk informasi selengkapnya tentang AWS Wilayah, lihat [Wilayah dan Zona Ketersediaan](#).

Cloud privat virtual (VPC)

Pilih VPC yang memiliki grup subnet cluster. Setelah cluster dibuat, grup subnet cluster tidak dapat diubah.

Grup parameter

Pilih grup parameter cluster untuk mengasosiasikan dengan cluster. Jika Anda tidak memilih salah satu, cluster menggunakan grup parameter default.

Enkripsi

Pilih apakah Anda ingin mengenkripsi semua data dalam cluster dan snapshot-nya. Jika Anda meninggalkan pengaturan default, None, enkripsi tidak diaktifkan. Jika Anda ingin mengaktifkan enkripsi, pilih apakah Anda ingin menggunakan AWS Key Management Service (AWS KMS) atau modul keamanan perangkat keras (HSM), lalu konfigurasi pengaturan terkait. Untuk informasi selengkapnya tentang enkripsi di Amazon Redshift, lihat [Enkripsi basis data Amazon Redshift](#)

- KMS

Pilih Use AWS Key Management Service (AWS KMS) jika Anda ingin mengaktifkan enkripsi dan gunakan AWS KMS untuk mengelola kunci enkripsi Anda. Juga, pilih kunci yang akan digunakan. Anda dapat memilih kunci default, kunci dari akun saat ini, atau kunci dari akun lain.

Note

Jika Anda ingin menggunakan kunci dari AWS akun lain, masukkan Nama Sumber Daya Amazon (ARN) untuk kunci yang akan digunakan. Anda harus memiliki izin untuk menggunakan kunci. Untuk informasi selengkapnya tentang akses ke kunci AWS KMS, lihat [Mengontrol akses ke kunci Anda](#) di Panduan AWS Key Management Service Pengembang.

Untuk informasi selengkapnya tentang menggunakan kunci AWS KMS enkripsi di Amazon Redshift, lihat. [Enkripsi database untuk Amazon Redshift menggunakan AWS KMS](#)

- HSM

Pilih HSM jika Anda ingin mengaktifkan enkripsi dan menggunakan modul keamanan perangkat keras (HSM) untuk mengelola kunci enkripsi Anda.

Jika Anda memilih HSM, pilih nilai dari Koneksi HSM dan Sertifikat Klien HSM. Nilai-nilai ini diperlukan untuk Amazon Redshift dan HSM untuk membentuk koneksi tepercaya di mana kunci cluster dapat diteruskan. Koneksi HSM dan sertifikat klien harus diatur di Amazon Redshift sebelum Anda meluncurkan klaster. Untuk informasi selengkapnya tentang pengaturan koneksi HSM dan sertifikat klien, lihat [Enkripsi untuk Amazon Redshift menggunakan modul keamanan perangkat keras](#).

Jalur pemeliharaan

Anda dapat memilih apakah versi cluster yang digunakan adalah trek Current, Trailing, atau terkadang Preview.

Pemantauan

Anda dapat memilih apakah akan membuat CloudWatch alarm.

Konfigurasi snapshot lintas wilayah

Anda dapat memilih apakah akan mengaktifkan snapshot lintas wilayah.

Periode retensi snapshot otomatis

Anda dapat memilih jumlah hari untuk menyimpan snapshot ini dalam waktu 35 hari. Jika tipe node adalah DC2, Anda dapat memilih nol (0) hari untuk tidak membuat snapshot otomatis.

Periode retensi snapshot manual

Anda dapat memilih jumlah hari atau *Indefinitely* untuk mempertahankan snapshot ini.

Membuat klaster pratinjau

Anda dapat membuat klaster Amazon Redshift di Pratinjau untuk menguji fitur baru Amazon Redshift. Anda tidak dapat menggunakan fitur tersebut dalam produksi atau memindahkan klaster Pratinjau Anda ke klaster produksi atau klaster di trek lain. Untuk syarat dan ketentuan pratinjau, lihat Beta dan Pratinjau di [Ketentuan AWS Layanan](#).

Untuk membuat cluster di Pratinjau

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Dasbor cluster yang disediakan, dan pilih Cluster. Cluster untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Spanduk ditampilkan pada halaman daftar Clusters yang memperkenalkan pratinjau. Pilih tombolnya Buat klaster pratinjau untuk membuka halaman buat cluster.
4. Masukkan properti untuk cluster Anda. Pilih trek Pratinjau yang berisi fitur yang ingin Anda uji. Sebaiknya masukkan nama untuk cluster yang menunjukkan bahwa itu ada di trek pratinjau. Pilih opsi untuk klaster Anda, termasuk opsi berlabel -preview, untuk fitur yang ingin Anda uji. Untuk informasi umum tentang membuat klaster, lihat [Membuat klaster](#) di Panduan Manajemen Pergeseran Merah Amazon.
5. Pilih Buat cluster untuk membuat klaster dalam pratinjau.

Note

preview_2023Lagu ini adalah trek pratinjau terbaru yang tersedia. Track ini mendukung pembuatan cluster dengan tipe node RA3 saja. Tipe node DC2 dan tipe node yang lebih lama tidak didukung.

6. Saat klaster pratinjau Anda tersedia, gunakan klien SQL Anda untuk memuat dan menanyakan data.

Untuk informasi tentang pratinjau di grup kerja Redshift Tanpa Server, lihat. [Membuat workgroup pratinjau](#)

Mengubah klaster

Saat Anda memodifikasi klaster, perubahan pada opsi berikut akan segera diterapkan:

- Grup keamanan VPC
- Dapat diakses publik
- Kata sandi pengguna admin
- Koneksi HSM

- Sertifikat Klien HSM
- Detail pemeliharaan
- Preferensi snapshot

Perubahan pada opsi berikut berlaku hanya setelah cluster dimulai ulang:

- Pengidentifikasi cluster

Amazon Redshift memulai ulang cluster secara otomatis saat Anda mengubah pengenal Cluster.

- Perutean VPC yang ditingkatkan

Amazon Redshift memulai ulang cluster secara otomatis saat Anda mengubah perutean VPC yang Ditingkatkan.

- Kelompok parameter cluster
- Jenis alamat IP

Fitur ini hanya tersedia di Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat). Untuk informasi selengkapnya tentang AWS Wilayah, lihat [Wilayah dan Zona Ketersediaan](#).

Jika Anda mengurangi periode retensi snapshot otomatis, snapshot otomatis yang ada yang pengaturannya berada di luar periode retensi baru akan dihapus. Untuk informasi selengkapnya, lihat [Cuplikan dan cadangan Amazon Redshift](#).

Untuk informasi selengkapnya tentang properti cluster, lihat [Konfigurasi tambahan](#).

Untuk mengubah klaster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster.
3. Pilih cluster yang akan dimodifikasi.
4. Pilih Edit. Halaman Edit cluster muncul.
5. Perbarui properti cluster. Beberapa properti yang dapat Anda modifikasi adalah:
 - Pengidentifikasi klaster
 - Retensi snapshot

- Relokasi cluster

Untuk mengedit pengaturan untuk konfigurasi Jaringan dan keamanan, Pemeliharaan, dan Database, konsol menyediakan tautan ke tab detail klaster yang sesuai.

6. Pilih Simpan perubahan.

Menghapus klaster

Jika Anda tidak lagi membutuhkan cluster Anda, Anda dapat menghapusnya. Jika Anda berencana untuk menyediakan cluster baru dengan data dan konfigurasi yang sama dengan yang Anda hapus, Anda memerlukan snapshot manual. Dengan menggunakan snapshot manual, Anda dapat memulihkan snapshot nanti dan melanjutkan menggunakan cluster. Jika Anda menghapus klaster tetapi tidak membuat snapshot manual akhir, data cluster akan dihapus. Dalam kedua kasus, snapshot otomatis dihapus setelah cluster dihapus, tetapi setiap snapshot manual dipertahankan sampai Anda menghapusnya. Anda mungkin dikenakan tarif penyimpanan Amazon Simple Storage Service untuk snapshot manual, tergantung pada jumlah penyimpanan yang tersedia untuk snapshot Amazon Redshift untuk cluster Anda. Untuk informasi selengkapnya, lihat [Mematikan dan menghapus cluster](#).

Menghapus cluster juga menghapus rahasia terkait AWS Secrets Manager .

Untuk menghapus klaster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster.
3. Pilih cluster yang akan dihapus.
4. Untuk Tindakan, pilih Hapus. Halaman Delete cluster muncul.
5. Pilih Hapus klaster.

Note

Saat Anda menghapus klaster dan memilih untuk membuat snapshot akhir, Amazon Redshift akan menghentikan permintaan penghapusan jika operasi pemulihan sedang berlangsung di

cluster. Jika ini terjadi, Anda dapat menghapus cluster tanpa snapshot akhir, atau Anda dapat menghapusnya dengan snapshot terakhir setelah pemulihan selesai.

Melakukan boot ulang klaster

Saat Anda me-reboot cluster, status cluster disetel ke `rebooting` dan acara cluster dibuat saat reboot selesai. Setiap modifikasi cluster yang tertunda diterapkan pada reboot ini.

Untuk me-reboot sebuah cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster.
3. Pilih cluster untuk reboot.
4. Untuk Tindakan, pilih Reboot cluster. Halaman cluster Reboot muncul.
5. Pilih Reboot cluster.

Mengubah ukuran cluster

Saat Anda mengubah ukuran cluster, Anda menentukan sejumlah node atau tipe node yang berbeda dari konfigurasi cluster saat ini. Saat cluster sedang dalam proses mengubah ukuran, Anda tidak dapat menjalankan kueri tulis atau baca/tulis apa pun di cluster; Anda hanya dapat menjalankan kueri baca.

Untuk informasi lebih lanjut tentang mengubah ukuran cluster, termasuk berjalan melalui proses mengubah ukuran cluster menggunakan pendekatan yang berbeda, lihat [Mengubah ukuran cluster](#)

Untuk mengubah ukuran cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster.
3. Pilih cluster untuk mengubah ukuran.
4. Untuk Tindakan, pilih Ubah Ukuran. Halaman cluster Resize muncul.
5. Ikuti instruksi di halaman. Anda dapat mengubah ukuran cluster sekarang, sekali pada waktu tertentu, atau menambah dan mengurangi ukuran cluster Anda sesuai jadwal.

6. Tergantung pada pilihan Anda, pilih Ubah ukuran sekarang atau Jadwalkan Ubah ukuran.

Jika Anda memiliki node cadangan, Anda dapat meningkatkan ke node cadangan RA3. Anda dapat melakukan ini ketika Anda menggunakan konsol untuk memulihkan dari snapshot atau untuk melakukan perubahan ukuran elastis. Anda dapat menggunakan konsol untuk memandu Anda melalui proses ini. Untuk informasi selengkapnya tentang memutakhirkan ke node RA3, lihat [Memutakhirkan ke tipe node RA3](#).

Memutakhirkan versi rilis cluster

Anda dapat memutakhirkan versi pemeliharaan rilis klaster yang memiliki nilai Status Rilis rilis Baru yang tersedia. Saat Anda memutakhirkan versi pemeliharaan, Anda dapat memilih untuk segera memutakhirkan atau meningkatkan di jendela pemeliharaan berikutnya.

Important

Jika Anda segera memutakhirkan, klaster Anda offline hingga pemutakhiran selesai.

Untuk meng-upgrade cluster ke versi rilis baru

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster.
3. Pilih cluster untuk meng-upgrade.
4. Untuk Tindakan, pilih Upgrade versi cluster. Halaman versi klaster Upgrade muncul.
5. Ikuti instruksi di halaman.
6. Pilih Upgrade versi cluster.

Mendapatkan informasi tentang konfigurasi cluster

Untuk menampilkan informasi tentang cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).

2. Pada menu navigasi, pilih Cluster, lalu pilih nama cluster dari daftar untuk membuka detailnya. Rincian cluster ditampilkan, yang dapat mencakup kinerja Cluster, pemantauan Kueri, Database, Datashares, Jadwal, Pemeliharaan, dan tab Properti.
3. Pilih setiap tab untuk melihat detail lebih lanjut.

Mendapatkan ikhtisar status cluster

Untuk melihat status klaster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster.
3. Melihat status klaster di kolom Status.

Membuat snapshot dari sebuah cluster

Untuk membuat snapshot dari sebuah cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster.
3. Pilih cluster untuk membuat snapshot.
4. Untuk Tindakan, pilih Buat snapshot. Halaman Buat snapshot muncul.
5. Ikuti instruksi di halaman.
6. Pilih Buat snapshot.

Membuat atau mengedit alarm ruang disk

Untuk membuat alarm penggunaan ruang disk untuk cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Alarm.
3. Untuk Tindakan, pilih Buat alarm. Halaman Create alarm muncul.

4. Ikuti instruksi di halaman.
5. Pilih Buat alarm.

Bekerja dengan data kinerja cluster

Di konsol, Anda dapat bekerja dengan kinerja klaster pada tab Kinerja cluster pada halaman detail cluster.

Mengelola cluster menggunakan API Amazon AWS CLI Redshift dan Amazon

Anda dapat menggunakan AWS CLI operasi berikut untuk mengelola cluster di Amazon Redshift.

- [batalkan-mengubah ukuran](#)
- [buat-cluster](#)
- [hapus-cluster](#)
- [jelaskan-cluster](#)
- [jelaskan-cluster-versi](#)
- [jelaskan-node-konfigurasi-opsi](#)
- [jelaskan-orderable-cluster-options](#)
- [deskripsikan-mengubah ukuran](#)
- [memodifikasi-cluster](#)
- [jeda-cluster](#)
- [reboot-cluster](#)
- [mengubah ukuran-cluster](#)
- [lanjutkan-cluster](#)

Anda dapat menggunakan operasi Amazon Redshift API berikut untuk mengelola cluster.

- [CancelResize](#)
- [CreateCluster](#)
- [DeleteCluster](#)
- [DescribeClusters](#)

- [DescribeClusterVersi](#)
- [DescribeNodeConfigurationOptions](#)
- [DescribeResize](#)
- [DescribeOrderableClusterOptions](#)
- [ModifyCluster](#)
- [PauseCluster](#)
- [RebootCluster](#)
- [ResizeCluster](#)
- [ResumeCluster](#)

Mengelola cluster dalam VPC

Topik

- [Gambaran Umum](#)
- [Membuat cluster di VPC](#)
- [Mengelola grup keamanan VPC untuk sebuah cluster](#)
- [Mengonfigurasi setelan komunikasi grup keamanan untuk klaster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server](#)
- [Bagaimana Amazon Redshift bekerja dengan berbagi VPC untuk sumber daya AWS](#)
- [Grup subnet klaster Amazon Redshift](#)

Gambaran Umum

Amazon Redshift mendukung platform EC2-VPC dan EC2-Classic untuk meluncurkan cluster di cloud pribadi virtual (VPC) berdasarkan layanan Amazon VPC. Untuk informasi selengkapnya, lihat [Gunakan EC2-VPC saat Anda membuat cluster](#).

Note

Amazon Redshift tidak mendukung peluncuran cluster ke VPC penyewaan khusus. Untuk informasi selengkapnya, lihat [Instans khusus](#) di Panduan Pengguna Amazon VPC.

Saat menyediakan cluster di VPC, Anda perlu melakukan hal berikut:

- Berikan informasi VPC.

Saat Anda meminta Amazon Redshift untuk membuat klaster di VPC, Anda harus memberikan informasi VPC Anda dengan membuat grup subnet cluster. Informasi ini mencakup ID VPC dan daftar subnet di VPC Anda. Saat meluncurkan klaster, Anda menyediakan grup subnet klaster sehingga Amazon Redshift dapat menyediakan klaster Anda di salah satu subnet di VPC. Untuk informasi selengkapnya tentang membuat grup subnet di Amazon Redshift, lihat [Grup subnet klaster Amazon Redshift](#) Untuk informasi selengkapnya tentang pengaturan VPC, lihat [Memulai Amazon VPC di](#) Panduan Memulai VPC Amazon.

- Secara opsional, konfigurasi opsi yang dapat diakses publik.

Jika Anda mengonfigurasi klaster agar dapat diakses publik, Amazon Redshift menggunakan alamat IP elastis untuk alamat IP eksternal. Alamat IP elastis adalah alamat IP statis. Dengan itu, Anda dapat mengubah konfigurasi dasar Anda tanpa mempengaruhi alamat IP yang digunakan klien untuk terhubung ke cluster Anda. Pendekatan ini dapat membantu untuk situasi seperti pemulihan setelah kegagalan. Apakah Anda membuat alamat IP elastis tergantung pada pengaturan relokasi zona ketersediaan Anda. Ada dua opsi:

1. Jika relokasi zona ketersediaan diaktifkan dan ingin mengaktifkan akses publik, Anda tidak menentukan alamat IP elastis. Alamat IP elastis yang dikelola oleh Amazon Redshift ditetapkan. Ini terkait dengan AWS akun Anda.
2. Jika relokasi zona ketersediaan dimatikan dan ingin mengaktifkan akses publik, Anda dapat memilih untuk membuat alamat IP elastis untuk VPC di Amazon EC2, sebelum meluncurkan klaster Amazon Redshift Anda. Jika Anda tidak membuat alamat IP, Amazon Redshift menyediakan alamat IP elastis yang dikonfigurasi untuk digunakan untuk VPC. Alamat IP elastis ini dikelola oleh Amazon Redshift dan tidak terkait dengan akun Anda AWS .

Untuk informasi selengkapnya, lihat [Alamat IP Elastis](#) di Panduan Pengguna Amazon EC2.

Dalam beberapa kasus, Anda mungkin memiliki cluster yang dapat diakses publik di VPC yang ingin Anda sambungkan dengan menggunakan alamat IP pribadi dari dalam VPC. Jika demikian, atur parameter VPC berikut ke: `true`

- `DNS resolution`
- `DNS hostnames`

Misalkan Anda memiliki cluster yang dapat diakses publik di VPC tetapi tidak menyetel parameter tersebut `true` ke dalam VPC. Dalam kasus ini, koneksi yang dibuat dari dalam VPC menyelesaikan ke alamat IP elastis cluster, bukan alamat IP pribadi. Kami menyarankan Anda

mengatur parameter ini `true` dan menggunakan alamat IP pribadi untuk cluster yang dapat diakses publik saat menghubungkan dari dalam VPC. Untuk informasi selengkapnya, lihat [Menggunakan DNS dengan VPC Anda](#) dalam Panduan Pengguna Amazon VPC.

Note

Jika Anda memiliki klaster yang dapat diakses publik di VPC, koneksi dari dalam VPC terus menggunakan alamat IP elastis untuk terhubung ke cluster hingga Anda mengubah ukuran cluster. Ini terjadi bahkan dengan parameter sebelumnya ditetapkan. Setiap cluster baru mengikuti perilaku baru menggunakan alamat IP pribadi saat menghubungkan ke cluster yang dapat diakses publik dari dalam VPC yang sama.

Alamat IP elastis adalah alamat IP eksternal untuk mengakses cluster di luar VPC. Ini tidak terkait dengan alamat IP publik node cluster dan alamat IP pribadi yang ditampilkan di konsol Amazon Redshift di bawah Detail koneksi. Alamat IP node cluster publik dan pribadi muncul terlepas dari apakah cluster dapat diakses publik atau tidak. Mereka hanya digunakan dalam keadaan tertentu untuk mengkonfigurasi aturan masuk pada host jarak jauh. Keadaan ini terjadi saat Anda memuat data dari instans Amazon EC2 atau host jarak jauh lainnya menggunakan koneksi Secure Shell (SSH). Untuk informasi selengkapnya, lihat [Langkah 1: Ambil kunci publik klaster dan alamat IP node cluster](#) di Panduan Pengembang Database Amazon Redshift.

Opsi untuk mengaitkan cluster dengan alamat IP elastis tersedia saat Anda membuat cluster atau mengembalikan cluster dari snapshot. Dalam beberapa kasus, Anda mungkin ingin mengaitkan cluster dengan alamat IP elastis atau mengubah alamat IP elastis yang terkait dengan cluster. Untuk melampirkan alamat IP elastis setelah cluster dibuat, pertama-tama perbarui cluster sehingga tidak dapat diakses publik, kemudian membuatnya dapat diakses publik dan menambahkan alamat IP Elastis dalam operasi yang sama.

- Kaitkan grup keamanan VPC.

Anda kemudian memberikan akses masuk menggunakan grup keamanan VPC. Grup keamanan VPC ini harus mengizinkan akses melalui port database untuk cluster sehingga Anda dapat terhubung dengan menggunakan alat klien SQL. Anda dapat mengonfigurasi ini terlebih dahulu, atau menambahkan aturan ke dalamnya setelah Anda meluncurkan cluster. Untuk informasi selengkapnya, lihat [Mengonfigurasi setelah komunikasi grup keamanan untuk klaster Amazon Redshift](#), yang memberikan panduan tentang mengonfigurasi aturan masuk dan keluar antara klien dan klaster yang disediakan atau grup kerja Amazon Redshift Tanpa Server. Sumber daya lain

yang membantu Anda memahami grup keamanan adalah [Keamanan di VPC Anda di Panduan Pengguna Amazon VPC](#). Perhatikan bahwa Anda tidak dapat menggunakan grup keamanan klaster Amazon Redshift untuk memberikan akses masuk ke klaster.

Untuk informasi selengkapnya tentang bekerja dengan cluster di VPC, lihat [Membuat cluster di VPC](#)

Memulihkan snapshot cluster di VPC

Cuplikan cluster di VPC hanya dapat dipulihkan dalam VPC, bukan di luar VPC. Anda dapat mengembalikannya di VPC yang sama atau VPC lain di akun Anda. Untuk informasi selengkapnya tentang snapshot, lihat [Cuplikan dan cadangan Amazon Redshift](#).

Membuat cluster di VPC

Berikut ini adalah langkah-langkah umum bagaimana Anda dapat menyebarkan cluster di virtual private cloud (VPC) Anda.

Untuk membuat cluster di VPC

1. Siapkan VPC.

Anda dapat membuat klaster baik di VPC default untuk akun Anda, jika akun Anda memilikinya, atau VPC yang telah Anda buat. Untuk informasi selengkapnya, lihat [Gunakan EC2-VPC saat Anda membuat cluster](#). Untuk membuat VPC, lihat [Membuat VPC di Panduan Pengguna Amazon VPC](#). Catat pengenal VPC, subnet, dan Availability Zone subnet. Anda memerlukan informasi ini saat meluncurkan cluster Anda.

Note

Anda harus memiliki setidaknya satu subnet yang ditentukan dalam VPC Anda sehingga Anda dapat menambahkannya ke grup subnet cluster di langkah berikutnya. Untuk informasi selengkapnya tentang menambahkan subnet ke VPC Anda, [lihat Menambahkan subnet ke VPC Anda di Panduan Pengguna Amazon VPC](#).

2. Buat grup subnet klaster Amazon Redshift untuk menentukan subnet mana yang dapat digunakan cluster Amazon Redshift Anda di VPC.

Anda dapat membuat grup subnet cluster menggunakan konsol Amazon Redshift atau secara terprogram. Untuk informasi selengkapnya, lihat [Grup subnet klaster Amazon Redshift](#).

3. Otorisasi akses untuk koneksi masuk dalam grup keamanan VPC yang Anda kaitkan dengan cluster.

Anda dapat mengaktifkan klien di luar VPC (di internet publik) untuk terhubung ke cluster.

Untuk melakukan ini, Anda mengaitkan cluster dengan grup keamanan VPC yang memberikan akses masuk ke port yang Anda gunakan saat meluncurkan cluster. Untuk contoh aturan grup keamanan, lihat [Aturan grup keamanan](#) di Panduan Pengguna Amazon VPC.

4. Ikuti langkah-langkah di [cluster yang disediakan Amazon Redshift di Panduan Memulai Amazon Redshift](#) untuk membuat klaster. Lakukan modifikasi berikut saat membuat cluster Anda:
 - Untuk menampilkan bagian Konfigurasi tambahan, matikan Gunakan default.
 - Di bagian Jaringan dan keamanan, tentukan grup keamanan Virtual Private Cloud (VPC), Cluster subnet, dan grup keamanan VPC yang Anda atur.

Sekarang Anda siap menggunakan cluster. Anda dapat mengikuti langkah-langkah Memulai untuk menguji klaster dengan mengunggah data sampel dan mencoba contoh kueri.

Mengelola grup keamanan VPC untuk sebuah cluster

Saat Anda menyediakan klaster Amazon Redshift, klaster tersebut dikunci secara default sehingga tidak ada yang memiliki akses ke sana. Untuk memberi pengguna lain akses masuk ke klaster Amazon Redshift, Anda mengaitkan klaster dengan grup keamanan. Jika Anda menggunakan platform EC2-VPC, Anda dapat menggunakan grup keamanan Amazon VPC yang ada atau menentukan yang baru. Anda kemudian mengaitkannya dengan cluster seperti yang dijelaskan berikut. Jika Anda menggunakan platform EC2-Classic, Anda menentukan grup keamanan cluster dan mengaitkannya dengan cluster. Untuk informasi selengkapnya tentang penggunaan grup keamanan klaster di platform EC2-Classic, lihat [Grup keamanan klaster Amazon Redshift](#)

Grup keamanan VPC terdiri dari seperangkat aturan yang mengontrol akses ke instance di VPC, seperti cluster Anda. Aturan individu menetapkan akses berdasarkan rentang alamat IP atau pada grup keamanan VPC lainnya. Saat Anda mengaitkan grup keamanan VPC dengan klaster, aturan yang ditentukan dalam grup keamanan VPC mengontrol akses ke klaster.

Setiap cluster yang Anda sediakan di platform EC2-VPC memiliki satu atau lebih grup keamanan Amazon VPC yang terkait dengannya. Amazon VPC menyediakan grup keamanan VPC yang disebut default, yang dibuat secara otomatis saat Anda membuat VPC. Setiap cluster yang Anda luncurkan di VPC secara otomatis dikaitkan dengan grup keamanan VPC default jika Anda tidak menentukan grup keamanan VPC yang berbeda saat membuat cluster. Anda dapat mengaitkan grup keamanan

VPC dengan klaster saat membuat klaster, atau Anda dapat mengaitkan grup keamanan VPC nanti dengan memodifikasi klaster.

Tabel berikut menjelaskan aturan default untuk grup keamanan VPC default.

Inbound			
Source	Protocol	Port Range	Comments
The security group ID (sg-xxxxxxx)	All	All	Allow inbound traffic from instances assigned to the same security group
Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	All	All	Allow all outbound traffic

Anda dapat mengubah aturan untuk grup keamanan VPC default sesuai kebutuhan untuk klaster Amazon Redshift Anda.

Jika grup keamanan VPC default cukup untuk Anda, Anda tidak perlu membuat lebih banyak. Namun, Anda dapat secara opsional membuat grup keamanan VPC tambahan untuk mengelola akses masuk ke cluster Anda dengan lebih baik. Misalnya, Anda menjalankan layanan di klaster Amazon Redshift, dan Anda memiliki beberapa tingkat layanan berbeda yang Anda berikan kepada pelanggan Anda. Jika Anda tidak ingin menyediakan akses yang sama di semua tingkat layanan, Anda mungkin ingin membuat grup keamanan VPC terpisah, satu untuk setiap tingkat layanan. Anda kemudian dapat mengaitkan grup keamanan VPC ini dengan cluster Anda.

Anda dapat membuat hingga 100 grup keamanan VPC untuk VPC dan mengaitkan grup keamanan VPC dengan banyak cluster. Namun, Anda hanya dapat mengaitkan hingga lima grup keamanan VPC dengan cluster tertentu.

Amazon Redshift segera menerapkan perubahan ke grup keamanan VPC. Jadi, jika Anda telah mengaitkan grup keamanan VPC dengan klaster, aturan akses cluster masuk dalam grup keamanan VPC yang diperbarui segera berlaku.

[Anda dapat membuat dan memodifikasi grup keamanan VPC di https://console.aws.amazon.com/vpc/](https://console.aws.amazon.com/vpc/). Anda juga dapat mengelola grup keamanan VPC secara terprogram dengan menggunakan, AWS CLI Amazon EC2 CLI, dan file. AWS Tools for Windows PowerShell Untuk informasi selengkapnya tentang bekerja dengan grup keamanan VPC, lihat [Grup keamanan untuk VPC Anda di Panduan Pengguna](#) Amazon VPC.

Mengonfigurasi setelan komunikasi grup keamanan untuk kluster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server

Topik ini membantu Anda mengonfigurasi grup keamanan untuk merutekan dan menerima lalu lintas jaringan dengan tepat. Berikut ini adalah beberapa kasus penggunaan umum:

- Anda mengaktifkan aksesibilitas publik untuk kluster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server, tetapi tidak menerima lalu lintas. Untuk ini, Anda harus mengonfigurasi aturan masuk untuk memungkinkan lalu lintas mencapainya dari internet.
- Cluster atau grup kerja Anda tidak dapat diakses publik, dan Anda menggunakan grup keamanan VPC default Redshift yang telah dikonfigurasi sebelumnya untuk mengizinkan lalu lintas masuk. Tetapi Anda memiliki persyaratan untuk menggunakan grup keamanan selain default, dan grup keamanan khusus ini tidak mengizinkan lalu lintas masuk. Anda harus mengkonfigurasinya untuk memungkinkan komunikasi.

Bagian berikut membantu Anda memilih respons yang benar untuk setiap kasus penggunaan dan menunjukkan cara mengonfigurasi lalu lintas jaringan sesuai kebutuhan Anda. Anda dapat secara opsional menggunakan langkah-langkah untuk mengatur komunikasi dari grup keamanan swasta lainnya.

Note

Pengaturan lalu lintas jaringan dalam banyak kasus tidak dikonfigurasi secara otomatis di Amazon Redshift. Ini karena mereka dapat bervariasi pada tingkat granular, tergantung pada apakah sumber lalu lintas adalah internet atau grup keamanan swasta, dan karena persyaratan keamanan bervariasi.

Aksesibilitas publik dengan konfigurasi grup keamanan default atau kustom

Jika Anda membuat atau Anda sudah memiliki cluster atau workgroup, lakukan langkah-langkah konfigurasi berikut untuk membuatnya dapat diakses publik. Ini berlaku baik ketika Anda memilih grup keamanan default atau grup keamanan khusus:

1. Temukan pengaturan jaringan:

- Untuk klaster Amazon Redshift yang disediakan, pilih tab Properties, lalu di bawah Pengaturan jaringan dan keamanan, pilih VPC untuk klaster Anda.
 - Untuk grup kerja Amazon Redshift Tanpa Server, pilih konfigurasi Workgroup. Pilih workgroup dari daftar. Kemudian, di bawah Akses data, di panel Jaringan dan keamanan, pilih edit.
2. Konfigurasi gateway Internet dan tabel rute untuk VPC Anda. Anda memulai konfigurasi dengan memilih VPC berdasarkan nama. Ini membuka dasbor VPC. Untuk terhubung ke cluster atau workgroup yang dapat diakses publik dari internet, gateway internet harus dilampirkan ke tabel rute. Anda dapat mengonfigurasinya dengan memilih tabel Route di dasbor VPC. Konfirmasikan bahwa target gateway internet ditetapkan dengan sumber 0.0.0.0/0 atau IP CIDR publik. Tabel rute harus dikaitkan dengan VPC tempat klaster Anda berada. Untuk informasi selengkapnya mengenai pengaturan akses internet untuk VPC, seperti yang dijelaskan di sini, lihat [Mengaktifkan akses internet di dokumentasi](#) Amazon VPC. Untuk informasi selengkapnya tentang mengonfigurasi tabel rute, lihat [Mengonfigurasi tabel rute](#).
 3. Setelah Anda mengkonfigurasi gateway internet dan tabel rute, kembali ke pengaturan jaringan untuk Redshift. Buka akses masuk dengan memilih grup keamanan dan kemudian memilih aturan Inbound. Pilih Edit aturan masuk.
 4. Pilih Protokol dan Port untuk aturan masuk, atau aturan, sesuai kebutuhan Anda, untuk mengizinkan lalu lintas dari klien. Untuk cluster RA3, pilih port dalam rentang 5431-5455 atau 8191-8215. Setelah selesai, simpan setiap aturan.
 5. Edit pengaturan yang dapat diakses publik untuk mengaktifkannya. Anda dapat melakukan ini dari menu Tindakan klaster atau grup kerja Anda.

Saat Anda mengaktifkan pengaturan yang dapat diakses publik, Redshift membuat alamat IP Elastis. Ini adalah alamat IP statis yang terkait dengan AWS akun Anda. Klien di luar VPC dapat menggunakannya untuk terhubung.

Untuk informasi selengkapnya tentang mengonfigurasi grup keamanan Anda, lihat [Grup keamanan klaster Amazon Redshift](#).

Anda dapat menguji aturan Anda dengan menghubungkan dengan klien, lakukan hal berikut jika Anda terhubung ke Amazon Redshift Tanpa Server. Setelah Anda menyelesaikan konfigurasi jaringan, sambungkan dengan alat klien Anda, seperti [Amazon Redshift](#) RSQL. Menggunakan domain Amazon Redshift Tanpa Server sebagai host, masukkan yang berikut ini:

```
rsql -h workgroup-name.account-id.region.amazonaws.com -U admin -d dev -p 5439
```


Aksesibilitas pribadi dengan konfigurasi grup keamanan default atau kustom

Ketika Anda tidak berkomunikasi melalui internet ke cluster atau kelompok kerja Anda, itu disebut sebagai dapat diakses secara pribadi. Jika Anda memilih grup keamanan default saat membuatnya, grup keamanan menyertakan aturan komunikasi default berikut:

- Aturan masuk yang memungkinkan lalu lintas dari semua sumber daya yang ditetapkan ke grup keamanan.
- Aturan keluar yang memungkinkan semua lalu lintas keluar. Tujuan untuk aturan ini adalah 0.0.0.0/0. Dalam notasi routing antar domain tanpa kelas (CIDR), ini mewakili semua alamat IP yang mungkin.

Anda dapat melihat aturan di konsol dengan memilih grup keamanan untuk klaster atau grup kerja Anda.

Jika klaster atau grup kerja dan klien Anda menggunakan grup keamanan default, tidak ada konfigurasi tambahan yang diperlukan untuk mengizinkan lalu lintas jaringan. Tetapi jika Anda menghapus atau mengubah aturan apa pun di grup keamanan default untuk Redshift atau klien, ini tidak lagi berlaku. Dalam hal ini, Anda harus mengonfigurasi aturan untuk memungkinkan komunikasi masuk dan keluar. Konfigurasi grup keamanan umum adalah sebagai berikut:

- Untuk instans Amazon EC2 klien:
 - Aturan inbound yang memungkinkan alamat IP klien.
 - Aturan keluar yang memungkinkan rentang alamat IP (blok CIDR) dari semua subnet yang disediakan untuk penggunaan Redshift. Atau Anda dapat menentukan 0.0.0.0/0, yang merupakan semua rentang alamat IP.
- Untuk klaster atau grup kerja Redshift Anda:
 - Aturan masuk yang memungkinkan grup keamanan klien.
 - Aturan keluar yang memungkinkan lalu lintas ke 0.0.0.0/0. Biasanya, aturan keluar memungkinkan semua lalu lintas keluar. Secara opsional, Anda dapat menambahkan aturan keluar untuk mengizinkan lalu lintas ke grup keamanan klien. Dalam kasus opsional ini, aturan keluar tidak selalu diperlukan, karena lalu lintas respons untuk setiap permintaan diizinkan untuk mencapai instance. Untuk detail selengkapnya mengenai perilaku permintaan dan respons, lihat [Grup keamanan](#) di panduan pengguna Amazon VPC.

Jika Anda mengubah konfigurasi untuk subnet atau grup keamanan yang ditentukan untuk penggunaan Redshift, Anda mungkin perlu mengubah aturan lalu lintas yang sesuai untuk menjaga komunikasi tetap terbuka. Untuk informasi selengkapnya tentang membuat aturan masuk dan keluar, lihat [pemblokiran CIDR VPC di](#) panduan pengguna Amazon VPC. Untuk informasi selengkapnya tentang menghubungkan ke Amazon Redshift dari klien, lihat [Mengonfigurasi koneksi di Amazon Redshift](#).

Bagaimana Amazon Redshift bekerja dengan berbagi VPC untuk sumber daya AWS

Berbagi VPC membuatnya sehingga Anda dapat membuat sumber daya AWS aplikasi, seperti instans Amazon EC2 dan layanan AWS lainnya, di cloud pribadi virtual (VPC) bersama yang dikelola secara terpusat. Akun yang memiliki VPC (pemilik) berbagi satu atau lebih subnet dengan akun lain (peserta) yang termasuk dalam organisasi yang sama. AWS Ini menjelaskan cara membuat dan menggunakan kluster Amazon Redshift atau workgroup Amazon Redshift Tanpa Server di VPC bersama.

Manfaat berbagi VPC termasuk bahwa Anda tidak perlu mengelola banyak VPC dan dapat membantu Anda menyederhanakan jaringan Anda. Manfaat khusus untuk administrator dan pengguna Amazon Redshift adalah sumber daya Redshift dapat beroperasi secara produktif di VPC bersama. Untuk informasi selengkapnya tentang berbagi VPC, lihat [Bagikan VPC Anda dengan akun lain](#), yang membahas lebih detail mengenai manfaat berbagi VPC dan cara kerjanya.

Cara menggunakan sumber daya gudang data Amazon Redshift di VPC bersama

Pertama, penting untuk dipahami bahwa kluster Amazon Redshift atau workgroup Amazon Redshift Tanpa Server tidak dapat dibuat terlihat oleh peserta dalam subnet bersama. Tetapi ini tidak menghalangi peserta untuk bekerja dengan database pemilik di VPC bersama. Ini dirinci lebih lengkap dalam langkah-langkah berikut.

Sebelum membuat kluster Amazon Redshift yang disediakan di VPC bersama, Anda harus membuat grup subnet yang ingin Anda gunakan untuk Amazon Redshift. Ini harus mencakup subnet dari VPC bersama yang ingin Anda gunakan. Saat membuat kluster Amazon Redshift, Anda harus memilih subnet ini dan juga menentukan grup keamanan VPC bersama. Demikian pula, Anda harus menentukan subnet bersama dan grup keamanan yang Anda buat di VPC bersama saat Anda membuat grup kerja dan database Amazon Redshift Tanpa Server. Setelah menyiapkan subnet, lakukan langkah-langkah berikut untuk menyiapkan sumber daya Redshift di lingkungan bersama:

1. Pemilik VPC membuat cluster Amazon Redshift atau workgroup Amazon Redshift Tanpa Server, menggunakan subnet di VPC bersama.
2. Pemilik VPC membuat cluster atau workgroup tersedia dalam skenario cross-VPC. Langkah-langkahnya dijelaskan dalam [Bekerja dengan titik akhir VPC yang dikelola RedShift di Amazon Redshift](#) untuk klaster yang disediakan [atau di Menghubungkan ke Amazon Redshift Tanpa Server dari titik akhir VPC yang dikelola Amazon Redshift untuk Amazon Redshift Tanpa Server](#). Dengan mengaktifkan ketersediaan lintas-VPC, mereka dapat membuat database tersedia untuk pengguna di AWS akun yang sama atau di akun lain.
3. Sebaliknya, melalui berbagi VPC, pemilik dapat berbagi subnet dengan peserta, dan peserta dapat membuat cluster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server di subnet. Namun, pemilik dalam hal ini tidak dapat melihat sumber daya Amazon Redshift yang dibuat oleh peserta. Cluster atau workgroup harus dibuat dapat diakses dengan mengaktifkan ketersediaan lintas-VPC dengan cara yang sama seperti yang dijelaskan pada langkah sebelumnya.

Catatan penggunaan untuk menggunakan resource Amazon Redshift di VPC bersama

Perhatikan perilaku berikut terkait penggunaan Amazon Redshift di subnet bersama:

- Seperti yang dijelaskan di bagian sebelumnya, pemilik VPC tidak dapat berbagi cluster Amazon Redshift atau workgroup Amazon Redshift Tanpa Server dengan peserta melalui berbagi VPC. Tetapi peserta dapat membuat cluster atau grup kerja Amazon Redshift Serverless di subnet pemilik. Dalam hal ini, Amazon Redshift tidak terlihat melalui berbagi VPC kepada pemiliknya.
- Pemilik VPC tidak dapat melihat, memperbarui, atau menghapus klaster yang disediakan Amazon Redshift atau grup kerja Tanpa Server Amazon Redshift yang dibuat peserta di subnet bersama.
- Tidak ada izin yang tersedia untuk membuatnya sehingga AWS akun lain dapat mengakses sumber daya Amazon Redshift yang Anda buat di VPC bersama.

Grup subnet klaster Amazon Redshift

Gambaran Umum

Anda membuat grup subnet klaster jika Anda menyediakan klaster Anda di virtual private cloud (VPC) Anda. Untuk informasi selengkapnya tentang VPC, lihat halaman detail [produk Amazon VPC](#).

VPC Anda dapat memiliki satu atau beberapa subnet, subset alamat IP dalam VPC Anda, yang memungkinkan Anda mengelompokkan sumber daya berdasarkan kebutuhan keamanan dan operasi

Anda. Grup subnet cluster memungkinkan Anda menentukan satu set subnet di VPC Anda. Saat menyediakan klaster, Anda menyediakan grup subnet dan Amazon Redshift membuat cluster di salah satu subnet dalam grup.

Untuk informasi selengkapnya tentang membuat VPC, buka Dokumentasi Panduan [Pengguna Amazon VPC](#).

Setelah membuat grup subnet, Anda dapat menghapus subnet yang sebelumnya Anda tambahkan atau menambahkan lebih banyak subnet. Amazon Redshift menyediakan operasi API bagi Anda untuk membuat, memodifikasi, atau menghapus grup subnet klaster. Anda juga dapat melakukan operasi ini di konsol.

Mengelola grup subnet cluster menggunakan konsol

Anda dapat mengelola grup subnet cluster menggunakan konsol Amazon Redshift. Anda dapat membuat grup subnet cluster, mengelola yang sudah ada, atau menghapusnya. Semua tugas ini dimulai dari daftar grup subnet cluster. Anda harus memilih grup subnet cluster untuk mengelolanya.

Anda dapat menyediakan cluster di salah satu subnet yang Anda berikan grup subnet. Grup subnet cluster memungkinkan Anda menentukan satu set subnet di virtual private cloud (VPC) Anda.

Membuat grup subnet cluster

Anda harus memiliki setidaknya satu grup subnet cluster yang ditentukan untuk menyediakan klaster di VPC.

Untuk membuat grup subnet cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Konfigurasi, lalu pilih Grup subnet. Daftar grup subnet ditampilkan.
3. Pilih Buat grup subnet cluster untuk menampilkan halaman buat.
4. Masukkan informasi untuk grup subnet, termasuk subnet mana yang akan ditambahkan.
5. Pilih Buat grup subnet cluster untuk membuat grup dengan subnet yang Anda pilih.

Memodifikasi grup subnet cluster

Untuk memodifikasi grup subnet cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Konfigurasi, lalu pilih Grup subnet. Daftar grup subnet ditampilkan.
3. Pilih grup subnet untuk dimodifikasi.
4. Untuk Tindakan, pilih Ubah untuk menampilkan detail grup subnet.
5. Perbarui informasi untuk grup subnet.
6. Pilih Simpan untuk memodifikasi grup.

Untuk mengubah atau menghapus subnet dalam beberapa kasus memerlukan langkah tambahan. Misalnya, artikel Pusat AWS Pengetahuan ini, [Bagaimana cara memindahkan cluster Amazon Redshift saya yang disediakan ke subnet yang berbeda?](#), menjelaskan kasus penggunaan yang mencakup pemindahan cluster.

Menghapus grup subnet cluster

Anda tidak dapat menghapus grup subnet cluster yang digunakan oleh cluster.

Untuk menghapus grup subnet cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Konfigurasi, lalu pilih Grup subnet. Daftar grup subnet ditampilkan.
3. Pilih grup subnet yang akan dihapus, lalu pilih Hapus.

Mengelola grup subnet cluster menggunakan API Amazon AWS CLI Redshift dan Amazon

Anda dapat menggunakan operasi Amazon Redshift CLI berikut untuk mengelola grup subnet cluster.

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

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

Anda dapat menggunakan operasi Amazon Redshift API berikut untuk mengelola grup subnet klaster.

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

Riwayat versi cluster

Amazon Redshift secara berkala merilis versi klaster baru yang digunakan untuk memperbarui klaster Anda.

Important

Untuk informasi tentang versi klaster Amazon Redshift yang tersedia, serta fitur, peningkatan, dan perbaikannya, lihat. [Versi cluster untuk Amazon Redshift](#)

Bekerja dengan integrasi nol-ETL

Topik ini mencakup dokumentasi prarilis untuk Aurora PostgreSQL dan RDS untuk integrasi MySQL Zero-ETL dengan Amazon Redshift, yang dalam rilis pratinjau. Dokumentasi dan fitur keduanya dapat berubah. Kami menyarankan Anda menggunakan RDS untuk MySQL dan Aurora PostgreSQL integrasi Zero-ETL hanya di lingkungan pengujian dan bukan di lingkungan produksi. Untuk syarat dan ketentuan pratinjau, lihat Beta dan Pratinjau dalam [Persyaratan Layanan AWS](#).

Integrasi nol-ETL adalah solusi yang dikelola sepenuhnya yang membuat data transaksional atau operasional tersedia di Amazon Redshift dalam waktu dekat. Dengan solusi ini, Anda dapat mengonfigurasi integrasi dari sumber Anda ke gudang data Amazon Redshift. Anda tidak perlu memelihara pipeline ekstrak, transformasi, dan beban (ETL). Kami menangani ETL untuk Anda dengan mengotomatiskan pembuatan dan pengelolaan replikasi data dari sumber data ke cluster Amazon Redshift atau namespace Redshift Tanpa Server. Anda dapat terus memperbarui dan menanyakan data sumber Anda sekaligus menggunakan Amazon Redshift untuk beban kerja analitik, seperti pelaporan dan dasbor.

Dengan integrasi Zero-ETL, Anda memiliki data yang lebih segar untuk analitik, AI/ML, dan pelaporan. Anda mendapatkan wawasan yang lebih akurat dan tepat waktu untuk kasus penggunaan seperti dasbor waktu nyata, pengalaman bermain game yang dioptimalkan, pemantauan kualitas data, dan analisis perilaku pelanggan. Anda dapat membuat prediksi berbasis data dengan lebih percaya diri, meningkatkan pengalaman pelanggan, dan mempromosikan wawasan berbasis data di seluruh bisnis.

Sumber-sumber berikut saat ini didukung untuk integrasi nol-ETL:

- Aurora Edisi yang Kompatibel dengan MySQL
- Edisi Kompatibel dengan Aurora PostgreSQL (pratinjau)
- RDS untuk MySQL (pratinjau)

Untuk membuat integrasi nol-ETL, Anda menentukan sumber integrasi dan gudang data Amazon Redshift sebagai target. Integrasi mereplikasi data dari sumber ke gudang data target. Data menjadi tersedia di Amazon Redshift dalam hitungan detik. Integrasi memantau kondisi pipeline data dan memulihkan dari masalah jika memungkinkan. Anda dapat membuat integrasi dari sumber dengan

jenis yang sama ke dalam satu gudang data Amazon Redshift untuk memperoleh wawasan holistik di beberapa aplikasi.

Dengan data di Amazon Redshift, Anda dapat menggunakan analitik yang disediakan Amazon Redshift. Misalnya, pembelajaran mesin bawaan (ML), tampilan terwujud, berbagi data, dan akses langsung ke beberapa penyimpanan data dan data lake. Integrasi nol-ETL membuat sumber daya komputasi Anda terisolasi dari sumber daya data Anda, sehingga Anda menggunakan alat yang paling efisien untuk memproses data. Untuk insinyur data, integrasi nol-ETL menyediakan akses ke data sensitif waktu yang jika tidak dapat ditunda oleh kesalahan intermiten dalam jaringan data yang kompleks. Anda dapat menjalankan kueri analitik dan model ML pada data transaksional untuk mendapatkan wawasan mendekati waktu nyata untuk peristiwa dan keputusan bisnis yang sensitif terhadap waktu.

Anda dapat membuat langganan notifikasi peristiwa Amazon Redshift sehingga Anda dapat diberi tahu saat peristiwa terjadi untuk integrasi nol-ETL tertentu. Untuk melihat daftar notifikasi peristiwa terkait integrasi, lihat [Pemberitahuan acara integrasi nol-ETL dengan Amazon EventBridge](#). Cara termudah untuk membuat langganan adalah dengan konsol Amazon SNS. Untuk informasi tentang cara membuat topik Amazon SNS dan berlangganan topik tersebut, lihat [Memulai Amazon SNS](#) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Saat mulai menggunakan integrasi nol-ETL, pertimbangkan konsep berikut ini:

- Database sumber adalah database tempat data direplikasi ke Amazon Redshift.
- Gudang data target adalah klaster yang disediakan Amazon Redshift atau grup kerja Redshift Serverless tempat data direplikasi.
- Database tujuan adalah database yang Anda buat dari integrasi nol-ETL di gudang data target.

Anda dapat memantau integrasi nol-ETL Anda dengan menanyakan tampilan sistem berikut di Amazon Redshift.

- [SVV_INTEGRATION](#) memberikan informasi tentang detail konfigurasi integrasi nol-ETL.
- [SYS_INTEGRATION_ACTIVITY](#) memberikan informasi tentang integrasi nol-ETL yang lengkap.
- [SVV_INTEGRATION_TABLE_STATE](#) memberikan informasi tentang status integrasi.
- [SYS_INTEGRATION_TABLE_STATE_CHANGE](#) memberikan informasi tentang log perubahan [status](#) tabel untuk integrasi.

Untuk informasi harga untuk integrasi nol-ETL, lihat halaman harga yang sesuai:

- [Harga Amazon Redshift](#)
- [Harga Amazon Aurora](#)
- [Harga Amazon RDS](#)

Untuk informasi selengkapnya tentang sumber integrasi nol-ETL, lihat topik berikut:

- Untuk integrasi Aurora Zero-ETL, lihat [Manfaat](#), [Konsep Utama](#), [Batasan](#), [Kuota](#), dan Wilayah yang [Didukung dari integrasi Nol-ETL](#) di Panduan Pengguna Amazon Aurora.
- Untuk integrasi RDS Nol-ETL, lihat [Manfaat](#), [Konsep Utama](#), [Batasan](#), [Kuota](#), dan Wilayah yang [Didukung dari integrasi Nol-ETL](#) di Panduan Pengguna Amazon RDS.

Topik

- [Pertimbangan saat menggunakan integrasi nol-ETL dengan Amazon Redshift](#)
- [Mulai menggunakan integrasi nol-ETL](#)
- [Membuat database tujuan di Amazon Redshift](#)
- [Menanyakan dan membuat tampilan terwujud dengan data yang direplikasi](#)
- [Mengelola integrasi nol-ETL](#)
- [Metrik untuk integrasi nol-ETL](#)
- [Memecahkan masalah integrasi nol-ETL](#)

Pertimbangan saat menggunakan integrasi nol-ETL dengan Amazon Redshift

Pertimbangan berikut berlaku untuk integrasi nol-ETL dengan Amazon Redshift.

- Gudang data Amazon Redshift target Anda harus memenuhi prasyarat berikut:
 - Menjalankan Amazon Redshift Serverless atau tipe node RA3 (ra3.16xlarge, ra3.4xlarge, dan ra3.xlplus).
 - Terenkripsi (jika menggunakan klaster yang disediakan).
 - Memiliki sensitivitas kasus diaktifkan.
- Anda tidak dapat mengaktifkan dukungan VPC yang disempurnakan di gudang data dengan integrasi yang dikonfigurasi.

- Jika Anda menghapus sumber yang merupakan sumber integrasi resmi untuk gudang data Amazon Redshift, semua integrasi terkait akan masuk ke status. FAILED
- Database tujuan adalah read-only. Anda tidak dapat membuat tabel, tampilan, atau tampilan terwujud dalam database tujuan. Namun, Anda dapat menggunakan tampilan terwujud pada tabel lain di gudang data target.
- Tampilan terwujud didukung saat digunakan dalam kueri lintas basis data. Menyegarkan tampilan terwujud dengan data yang direplikasi dari integrasi nol-ETL mengarah ke penyegaran penuh tampilan. Penyegaran tambahan, penulisan ulang kueri otomatis, autorefresh, dan tampilan terwujud otomatis tidak didukung. Untuk informasi tentang membuat tampilan terwujud dengan data yang direplikasi melalui integrasi nol-ETL, lihat [Membuat tampilan terwujud dengan data yang direplikasi](#)
- Anda dapat menanyakan tabel hanya di gudang data target yang berada di Synced negara bagian. Untuk informasi selengkapnya, lihat [Metrik untuk integrasi nol-ETL](#).
- Amazon Redshift hanya menerima karakter UTF-8, jadi mungkin tidak menghormati pemeriksaan yang ditentukan dalam sumber Anda. Aturan penyortiran dan perbandingan mungkin berbeda, yang pada akhirnya dapat mengubah hasil kueri.
- Panjang maksimum tipe data Amazon Redshift VARCHAR adalah 65.535 byte. Ketika konten dari sumber tidak sesuai dengan batas ini, replikasi tidak dilanjutkan dan tabel dimasukkan ke dalam keadaan gagal. Untuk informasi selengkapnya tentang perbedaan tipe data antara sumber integrasi nol-ETL dan database Amazon Redshift, lihat Perbedaan [tipe data antara Aurora dan Amazon Redshift di Panduan Pengguna Amazon Aurora](#).
- Tabel dalam sumber integrasi harus memiliki kunci utama. Jika tidak, tabel Anda tidak dapat direplikasi ke gudang data target di Amazon Redshift.
- Untuk integrasi Aurora PostgreSQL dan RDS untuk MySQL Zero-ETL MySQL dengan Amazon Redshift, buat gudang data target Anda di Pratinjau. Untuk informasi selengkapnya, lihat [Membuat dan mengonfigurasi gudang data Amazon Redshift target](#).
- Integrasi nol-ETL tidak mendukung transformasi saat mereplikasi data dari penyimpanan data transaksional ke Amazon Redshift. Data direplikasi apa adanya dari basis data sumber. Namun, Anda dapat menerapkan transformasi pada data yang direplikasi di Amazon Redshift.
- Mungkin ada dampak pada beban kerja lain yang berjalan di Amazon Redshift. Untuk menghilangkan dampak integrasi nol-ETL pada beban kerja lain, pertimbangkan untuk menggunakan endpoint terpisah untuk integrasi nol-ETL dan bagikan data dengan titik akhir lain yang memerlukan akses ke data ini menggunakan datasharing.

- Integrasi nol-ETL berjalan di Amazon Redshift menggunakan koneksi paralel. Ini berjalan menggunakan kredensial pengguna yang membuat database dari integrasi. Saat kueri berjalan, penskalaan konkurensi tidak berlaku untuk koneksi ini selama sinkronisasi (tuliskan). Pembacaan penskalaan konkurensi (dari klien Amazon Redshift) berfungsi untuk objek yang disinkronkan.

Untuk pertimbangan yang juga berlaku untuk sumber integrasi, lihat salah satu topik berikut:

- Untuk sumber Aurora, lihat [Batasan di Panduan Pengguna Amazon Aurora](#).
- Untuk sumber Amazon RDS, lihat [Batasan](#) dalam Panduan Pengguna Amazon RDS.

Mulai menggunakan integrasi nol-ETL

Sebelum mengonfigurasi integrasi Nol-ETL Anda di Amazon Redshift, konfigurasi sumber integrasi Anda dan atur dengan parameter dan izin yang diperlukan. Kemudian, lanjutkan ke sisa pengaturan awal dari konsol Amazon Redshift dan AWS CLI

Untuk membuat integrasi Aurora Zero-ETL dengan Amazon Redshift

Untuk membuat integrasi Aurora Zero-ETL dengan Amazon Redshift, lakukan hal berikut:

1. Dari konsol Amazon RDS, [buat grup parameter cluster DB kustom](#) seperti yang dijelaskan dalam Panduan Pengguna Amazon Aurora.
2. Dari konsol Amazon RDS, [buat cluster DB Amazon Aurora sumber](#) seperti yang dijelaskan dalam Panduan Pengguna Amazon Aurora.
3. Dari konsol Amazon Redshift: [Membuat dan mengonfigurasi gudang data Amazon Redshift target](#)
 - Dari AWS CLI atau konsol Amazon Redshift: [Aktifkan sensitivitas huruf besar untuk gudang data Anda](#)
 - Dari konsol Amazon Redshift: [Konfigurasi otorisasi untuk gudang data Amazon Redshift Anda](#)
4. Dari konsol Amazon RDS, [buat integrasi Nol-ETL](#) seperti yang dijelaskan dalam Panduan Pengguna Amazon Aurora.
5. Dari konsol Amazon Redshift atau editor kueri v2, [buat database Amazon Redshift](#) dari integrasi Anda.

Kemudian, [kueri dan buat tampilan terwujud dengan data yang direplikasi](#).

Untuk membuat integrasi RDS nol-ETL dengan Amazon Redshift

Untuk membuat integrasi RDS Zero-ETL dengan Amazon Redshift, lakukan hal berikut:

1. Dari konsol Amazon RDS, [buat grup parameter DB khusus](#) seperti yang dijelaskan dalam Panduan Pengguna Amazon RDS.
2. Dari konsol Amazon RDS, [buat instance Amazon RDS sumber](#) seperti yang dijelaskan dalam Panduan Pengguna Amazon RDS.
3. Dari konsol Amazon Redshift: [Membuat dan mengonfigurasi gudang data Amazon Redshift target](#)
 - Dari AWS CLI atau konsol Amazon Redshift: [Aktifkan sensitivitas huruf besar untuk gudang data Anda](#)
 - Dari konsol Amazon Redshift: [Konfigurasi otorisasi untuk gudang data Amazon Redshift Anda](#)
4. Dari konsol Amazon RDS, [buat integrasi nol-ETL](#) seperti yang dijelaskan dalam Panduan Pengguna Amazon RDS.
5. Dari konsol Amazon Redshift atau editor kueri v2, [buat database Amazon Redshift](#) dari integrasi Anda.

Kemudian, [kueri dan buat tampilan terwujud dengan data yang direplikasi](#).

Konsol Amazon RDS menawarkan alur pembuatan step-by-step integrasi, di mana Anda menentukan database sumber dan gudang data Amazon Redshift target. Jika masalah terjadi, maka Anda dapat memilih untuk meminta Amazon RDS memperbaiki masalah untuk Anda alih-alih memperbaikinya secara manual di konsol Amazon RDS atau Amazon Redshift.

Membuat dan mengonfigurasi gudang data Amazon Redshift target

Sebelum langkah ini, buat sumber integrasi Anda dan konfigurasi parameter yang diperlukan oleh tipe sumber untuk integrasi nol-ETL.

Pada langkah ini, Anda membuat dan mengonfigurasi gudang data Amazon Redshift target, seperti workgroup Redshift Tanpa Server atau kluster yang disediakan.

Gudang data target Anda harus memiliki karakteristik sebagai berikut:

- Menjalankan Amazon Redshift Serverless atau kluster tipe instans yang disediakan ra3.16xlarge, ra3.4xlarge, atau ra3.xlplus.

- Memiliki sensitivitas kasus (`enable_case_sensitive_identifier`) dihidupkan. Untuk informasi selengkapnya, lihat [Aktifkan sensitivitas huruf besar untuk gudang data Anda](#).
- Terenkripsi, jika gudang data target Anda adalah klaster yang disediakan Amazon Redshift. Untuk informasi selengkapnya, lihat [Enkripsi basis data Amazon Redshift](#).
- Dibuat di AWS Wilayah yang sama dengan sumber integrasi.

Note

Untuk integrasi Aurora PostgreSQL dan RDS untuk MySQL Zero-ETL dengan Amazon Redshift, pertimbangkan juga hal berikut untuk gudang data target Anda:

- Anda harus membuat gudang data Anda di Pratinjau di `preview_2023` trek. Anda tidak dapat menggunakan fitur pratinjau dalam produksi atau memindahkan gudang data pratinjau ke penerapan produksi.
- Jika Anda memilih untuk membuat klaster yang disediakan Amazon Redshift, klaster tersebut harus memiliki setidaknya dua node.
- Untuk sumber Aurora PostgreSQL, Anda harus membuat gudang data target Anda di Wilayah AS Timur (Ohio). AWS [Perhatikan bahwa Anda harus membuat database sumber untuk integrasi Aurora PostgreSQL Zero-ETL menggunakan Amazon RDS Database Preview Environment](#).

Untuk RDS untuk sumber MySQL, Anda harus membuat gudang data target di Wilayah yang didukung. AWS Untuk daftar AWS Wilayah di mana integrasi RDS untuk MySQL Zero-ETL tersedia, lihat Wilayah yang Didukung [untuk integrasi Nol-ETL dengan Amazon Redshift di Panduan Pengguna Amazon RDS](#).

Untuk membuat gudang data target Anda di Pratinjau untuk Aurora PostgreSQL dan RDS untuk integrasi MySQL Zero-ETL, lihat salah satu topik berikut tergantung pada jenis penerapan Anda:

- Untuk membuat pratinjau klaster yang disediakan Amazon Redshift, lihat. [Membuat klaster pratinjau](#) Pastikan Anda memilih `preview_2023` trek untuk menggunakan integrasi nol-ETL.
- Untuk membuat pratinjau grup kerja Amazon Redshift Tanpa Server, lihat. [Membuat workgroup pratinjau](#)

Untuk membuat gudang data target untuk integrasi Aurora MySQL Zero-ETL Anda, lihat salah satu topik berikut tergantung pada jenis penerapan Anda:

- Untuk membuat klaster yang disediakan Amazon Redshift, lihat. [Membuat klaster](#)
- Untuk membuat workgroup Amazon Redshift Tanpa Server dengan namespace, lihat. [Membuat workgroup dengan namespace](#)

Saat Anda membuat klaster yang disediakan, Amazon Redshift juga membuat grup parameter default. Anda tidak dapat mengedit grup parameter default. Namun, Anda dapat membuat grup parameter khusus sebelum membuat cluster baru dan kemudian mengaitkannya dengan cluster. Atau, Anda dapat mengedit grup parameter yang akan dikaitkan dengan cluster yang dibuat. Anda juga harus mengaktifkan sensitivitas huruf besar untuk grup parameter baik saat membuat grup parameter kustom atau saat mengedit grup parameter saat ini untuk menggunakan integrasi nol-ETL.

Anda dapat membuat grup parameter khusus menggunakan konsol Amazon Redshift atau AWS CLI sebagai berikut:

- Menggunakan konsol Amazon Redshift — [Mengelola grup parameter menggunakan konsol](#)
- Menggunakan AWS CLI - [Mengelola grup parameter menggunakan API Amazon Redshift AWS CLI dan Amazon](#)

Aktifkan sensitivitas huruf besar untuk gudang data Anda

Anda dapat melampirkan grup parameter dan mengaktifkan sensitivitas kasus untuk klaster yang disediakan selama pembuatan. Namun, Anda dapat memperbarui workgroup tanpa server melalui AWS Command Line Interface (AWS CLI) hanya setelah dibuat. Ini diperlukan untuk mendukung sensitivitas kasus MySQL dan PostgreSQL. `enable_case_sensitive_identifier` adalah nilai konfigurasi yang menentukan apakah pengidentifikasi nama database, tabel, dan kolom peka huruf besar/kecil. Parameter ini harus dihidupkan untuk membuat integrasi nol-ETL di gudang data. Untuk informasi selengkapnya, lihat [enable_case_sensitive_identifier](#).

Untuk Amazon Redshift Tanpa Server — [Aktifkan sensitivitas huruf besar/case untuk Amazon Redshift Serverless menggunakan AWS CLI](#) Perhatikan bahwa Anda dapat mengaktifkan sensitivitas huruf besar untuk Amazon Redshift Serverless hanya dari file. AWS CLI

Untuk klaster yang disediakan Amazon Redshift, aktifkan sensitivitas huruf besar untuk klaster target Anda menggunakan salah satu topik berikut:

- [Aktifkan sensitivitas huruf besar untuk cluster yang disediakan Amazon Redshift menggunakan konsol Amazon Redshift](#)
- [Aktifkan sensitivitas huruf besar/kecil untuk cluster yang disediakan Amazon Redshift menggunakan AWS CLI](#)

Aktifkan sensitivitas huruf besar/case untuk Amazon Redshift Serverless menggunakan AWS CLI

Jalankan AWS CLI perintah berikut untuk mengaktifkan sensitivitas huruf besar untuk workgroup Anda.

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

Tunggu status workgroup Active sebelum melanjutkan ke langkah berikutnya.

Aktifkan sensitivitas huruf besar untuk cluster yang disediakan Amazon Redshift menggunakan konsol Amazon Redshift

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Di panel navigasi kiri, pilih Dasbor cluster yang disediakan.
3. Pilih klaster yang disediakan tempat Anda ingin mereplikasi data.
4. Di panel navigasi kiri, pilih Konfigurasi > Manajemen beban kerja.
5. Pada halaman manajemen beban kerja, pilih grup parameter.
6. Pilih tab Parameter.
7. Pilih Edit parameter, lalu ubah `enable_case_sensitive_identifier` menjadi `true`.
8. Lalu, pilih Simpan.

Aktifkan sensitivitas huruf besar/kecil untuk cluster yang disediakan Amazon Redshift menggunakan AWS CLI

1. Karena Anda tidak dapat mengedit grup parameter default, dari program terminal Anda, jalankan AWS CLI perintah berikut untuk membuat grup parameter kustom. Nanti, Anda akan mengaitkannya dengan cluster yang disediakan.

```
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. Jalankan AWS CLI perintah berikut untuk mengaktifkan sensitivitas kasus untuk grup parameter.

```
aws redshift modify-cluster-parameter-group \  
  --parameter-group-name zero-etl-params \  
  --parameters ParameterName=enable_case_sensitive_identifier,ParameterValue=true
```

3. Jalankan perintah berikut untuk mengaitkan grup parameter dengan cluster.

```
aws redshift modify-cluster \  
  --cluster-identifier target-cluster \  
  --cluster-parameter-group-name zero-etl-params
```

4. Tunggu klaster yang disediakan tersedia. Anda dapat memeriksa status cluster dengan menggunakan `describe-cluster` perintah. Kemudian, jalankan perintah berikut untuk me-reboot cluster.

```
aws redshift reboot-cluster \  
  --cluster-identifier target-cluster
```

Konfigurasi otorisasi untuk gudang data Amazon Redshift Anda

Untuk mereplikasi data dari sumber integrasi ke gudang data Amazon Redshift, Anda harus menambahkan dua entitas berikut:

- Prinsipal resmi — mengidentifikasi pengguna atau peran yang dapat membuat integrasi nol-ETL ke dalam gudang data.

- Sumber integrasi resmi - mengidentifikasi basis data sumber yang dapat memperbarui gudang data.

Anda dapat mengonfigurasi prinsip resmi dan sumber integrasi resmi dari tab Kebijakan Sumber Daya di konsol Amazon Redshift atau menggunakan operasi Amazon Redshift API.

PutResourcePolicy

Tambahkan prinsipal resmi

Untuk membuat integrasi nol-ETL ke dalam workgroup Redshift Serverless atau kluster yang disediakan, otorisasi akses ke namespace terkait atau kluster yang disediakan.

Anda dapat melewati langkah ini jika kedua kondisi berikut benar:

- Akun AWS Yang memiliki grup kerja Redshift Serverless atau cluster yang disediakan juga memiliki database sumber.
- Prinsip tersebut dikaitkan dengan kebijakan IAM berbasis identitas dengan izin untuk membuat integrasi nol-ETL ke dalam namespace Redshift Tanpa Server atau cluster yang disediakan ini.

Tambahkan prinsipal resmi ke namespace Amazon Redshift Tanpa Server

1. Di konsol Amazon Redshift, di panel navigasi kiri, pilih Redshift Serverless.
2. Pilih konfigurasi Namespace, lalu pilih namespace Anda, dan buka tab Kebijakan Sumber Daya.
3. Pilih Tambahkan prinsipal resmi.
4. Untuk setiap prinsipal resmi yang ingin Anda tambahkan, masukkan ke dalam namespace baik ARN AWS pengguna atau peran, atau ID yang ingin Anda berikan akses untuk membuat Akun AWS integrasi nol-ETL. ID akun disimpan sebagai ARN.
5. Pilih Simpan perubahan.

Tambahkan prinsipal resmi ke kluster yang disediakan Amazon Redshift

1. Di konsol Amazon Redshift, di panel navigasi kiri, pilih Dasbor cluster yang disediakan.
2. Pilih Cluster, lalu pilih kluster, dan buka tab Kebijakan Sumber Daya.
3. Pilih Tambahkan prinsipal resmi.

4. Untuk setiap prinsipal resmi yang ingin Anda tambahkan, masukkan ke dalam kluster baik ARN AWS pengguna atau peran, atau ID Akun AWS yang ingin Anda berikan akses untuk membuat integrasi nol-ETL. ID akun disimpan sebagai ARN.
5. Pilih Simpan perubahan.

Tambahkan sumber integrasi resmi

Untuk mengizinkan sumber Anda memperbarui gudang data Amazon Redshift, Anda harus menemukannya sebagai sumber integrasi resmi ke namespace.

Menambahkan sumber integrasi resmi ke namespace Amazon Redshift Tanpa Server

1. Di konsol Amazon Redshift, buka dasbor Tanpa Server.
2. Pilih nama namespace.
3. Buka tab Kebijakan Sumber Daya.
4. Pilih Tambahkan sumber integrasi resmi.
5. Tentukan ARN sumber untuk integrasi nol-ETL.

Note

Menghapus sumber integrasi resmi menghentikan data mereplikasi ke namespace. Tindakan ini menonaktifkan semua integrasi nol-ETL dari sumber itu ke namespace ini.

Menambahkan sumber integrasi resmi ke kluster yang disediakan Amazon Redshift

1. Di konsol Amazon Redshift, buka dasbor cluster yang disediakan.
2. Pilih nama cluster yang disediakan.
3. Buka tab Kebijakan Sumber Daya.
4. Pilih Tambahkan sumber integrasi resmi.
5. Tentukan ARN dari sumber yang merupakan sumber data untuk integrasi nol-ETL.

Note

Menghapus sumber integrasi resmi menghentikan data mereplikasi ke dalam kluster yang disediakan. Tindakan ini menonaktifkan semua integrasi nol-ETL dari sumber itu ke dalam cluster yang disediakan Amazon Redshift ini.

Konfigurasi otorisasi menggunakan Amazon Redshift API

Anda dapat menggunakan operasi Amazon Redshift API untuk mengonfigurasi kebijakan sumber daya yang berfungsi dengan integrasi nol-ETL.

Untuk mengontrol sumber yang dapat membuat integrasi masuk ke dalam namespace, buat kebijakan sumber daya dan lampirkan ke namespace. Dengan kebijakan sumber daya, Anda dapat menentukan sumber yang memiliki akses ke integrasi. Kebijakan sumber daya dilampirkan ke namespace gudang data target Anda untuk memungkinkan sumber membuat integrasi masuk untuk mereplikasi data langsung dari sumber ke Amazon Redshift.

Berikut ini adalah contoh kebijakan sumber daya.

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

```
]
}
```

Berikut ini merangkum operasi Amazon Redshift API yang berlaku untuk mengonfigurasi kebijakan sumber daya untuk integrasi:

- Gunakan operasi API [PutResourceKebijakan](#) untuk mempertahankan kebijakan sumber daya. Saat Anda memberikan kebijakan sumber daya lain, kebijakan sumber daya sebelumnya pada sumber daya diganti. Gunakan contoh kebijakan sumber daya sebelumnya, yang memberikan izin untuk tindakan berikut:
 - `CreateInboundIntegration`— Memungkinkan prinsipal sumber untuk membuat integrasi inbound untuk data yang akan direplikasi dari sumber ke gudang data target.
 - `AuthorizeInboundIntegration`— Memungkinkan Amazon Redshift untuk terus memvalidasi bahwa gudang data target dapat menerima data yang direplikasi dari sumber ARN.
- Gunakan operasi [GetResourcePolicy](#) API untuk melihat kebijakan sumber daya yang ada.
- Gunakan operasi API [DeleteResourceKebijakan](#) untuk menghapus kebijakan sumber daya dari sumber daya.

Untuk memperbarui kebijakan sumber daya, Anda juga dapat menggunakan perintah [AWS CLI put-resource-policy](#).

Langkah selanjutnya

Sekarang setelah Anda mengonfigurasi otorisasi untuk gudang data Amazon Redshift target Anda, Anda dapat membuat integrasi nol-ETL dan mulai mereplikasi data.

Tergantung pada sumber Anda, lakukan salah satu hal berikut:

- Untuk membuat integrasi Aurora Zero-ETL, lihat [Membuat integrasi Nol-ETL Amazon Aurora dengan Amazon Redshift di Panduan Pengguna](#) Amazon Aurora.
- Untuk membuat integrasi RDS nol-ETL, lihat [Membuat integrasi Nol-ETL Amazon RDS dengan Amazon Redshift di Panduan Pengguna](#) Amazon RDS.

Membuat database tujuan di Amazon Redshift

Untuk mereplikasi data dari sumber Anda ke Amazon Redshift, Anda harus membuat database dari integrasi Anda di Amazon Redshift.

Connect ke workgroup Redshift Serverless target Anda atau klaster yang disediakan dan buat database dengan referensi ke pengenalan integrasi Anda. Pengidentifikasi ini adalah nilai yang dikembalikan `integration_id` saat Anda menanyakan tampilan [SVV_INTEGRATION](#).

Important

Sebelum membuat database dari integrasi Anda, integrasi nol-ETL Anda harus dibuat dan dalam status di Amazon RDS Active atau konsol Amazon Redshift.

Membuat database tujuan di Amazon Redshift

Sebelum Anda dapat mulai mereplikasi data dari sumber Anda ke Amazon Redshift, buat database dari integrasi di Amazon Redshift. Anda dapat membuat database menggunakan konsol Amazon Redshift atau editor kueri v2.

Membuat database tujuan menggunakan konsol Amazon Redshift

1. Di panel navigasi kiri, pilih Integrasi nol-ETL.
2. Dari daftar integrasi, pilih integrasi.
3. Jika Anda menggunakan klaster yang disediakan, Anda harus terlebih dahulu terhubung ke database. Pilih Hubungkan ke basis data. Anda dapat terhubung menggunakan koneksi terbaru, atau dengan membuat koneksi baru.
4. Untuk membuat database dari integrasi, pilih Buat database dari integrasi.
5. Masukkan nama Database. ID Integrasi dan nama gudang data sudah terisi sebelumnya.

Untuk sumber Aurora PostgreSQL, masukkan juga database bernama yang Anda tentukan saat membuat integrasi Zero-ETL Anda.

6. Pilih Buat basis data.

Membuat database tujuan menggunakan editor kueri v2

1. Arahkan ke konsol Amazon Redshift dan pilih Editor kueri v2.
2. Di panel kiri, pilih workgroup Amazon Redshift Serverless atau klaster yang disediakan Amazon Redshift, lalu sambungkan ke sana.
3. Untuk mendapatkan ID integrasi, navigasikan ke daftar integrasi di konsol Amazon Redshift.

Atau, jalankan perintah berikut untuk mendapatkan `integration_id` nilai:

```
SELECT integration_id FROM SVV_INTEGRATION;
```

4. Kemudian, jalankan perintah berikut untuk membuat database. Dengan menentukan ID integrasi, Anda membuat koneksi antara database dan sumber Anda.

Gantikan `integration_id` dengan nilai yang dikembalikan oleh perintah sebelumnya.

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

Untuk sumber PostgreSQL Aurora, Anda juga harus menyertakan referensi ke database bernama dalam cluster yang Anda tentukan saat Anda membuat integrasi. Sebagai contoh:

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

Note

Hanya sumber integrasi Anda yang dapat memperbarui data dalam database yang Anda buat dari integrasi Anda. Untuk mengubah skema tabel, jalankan perintah DDL atau DHTML terhadap tabel di sumbernya. Anda dapat menjalankan perintah DDL dan DHTML terhadap tabel di sumbernya, tetapi Anda hanya dapat menjalankan perintah DDL dan kueri hanya-baca pada database tujuan.

Untuk informasi tentang melihat status database tujuan, lihat [Mengelola integrasi nol-ETL](#).

Tambahkan data ke sumber Anda

Setelah membuat database tujuan, Anda dapat menambahkan data ke sumber Anda. Untuk menambahkan data ke sumber Anda, lihat salah satu topik berikut:

- Untuk sumber Aurora, lihat [Menambahkan data ke cluster DB sumber di Panduan Pengguna Amazon Aurora](#).
- Untuk sumber Amazon RDS, lihat [Menambahkan data ke instans DB sumber](#) di Panduan Pengguna Amazon RDS.

Menanyakan dan membuat tampilan terwujud dengan data yang direplikasi

Menanyakan data yang direplikasi di Amazon Redshift

Setelah Anda menambahkan data ke sumber Anda, itu direplikasi dalam waktu dekat ke gudang data Amazon Redshift, dan siap untuk kueri. Untuk informasi tentang metrik integrasi dan statistik tabel, lihat [Metrik untuk integrasi nol-ETL](#).

Note

Karena database sama dengan skema di MySQL, tingkat database MySQL memetakan ke tingkat skema Amazon Redshift. Perhatikan perbedaan pemetaan ini saat Anda menanyakan data yang direplikasi dari Aurora MySQL atau RDS untuk MySQL.

Untuk mengueri data yang direplikasi

1. Arahkan ke konsol Amazon Redshift dan pilih Editor kueri v2.
2. Connect ke workgroup Amazon Redshift Serverless atau klaster yang disediakan Amazon Redshift dan pilih database Anda dari daftar tarik-turun.
3. Gunakan pernyataan SELECT untuk memilih semua data yang direplikasi dari skema dan tabel yang Anda buat di sumber. Untuk sensitivitas kasus, gunakan tanda kutip ganda (") untuk nama skema, tabel, dan kolom. Sebagai contoh:

```
SELECT * FROM "schema_name"."table_name";
```

Anda juga dapat menanyakan data menggunakan Amazon Redshift CLI.

Membuat tampilan terwujud dengan data yang direplikasi

Anda dapat membuat tampilan terwujud di database Amazon Redshift lokal Anda untuk mengubah data yang direplikasi melalui integrasi nol-ETL. Connect ke database lokal Anda dan gunakan kueri lintas database untuk mengakses database tujuan. Anda dapat menggunakan nama objek yang sepenuhnya memenuhi syarat dengan notasi tiga bagian (destination-database-name.schema-name.table-name) atau membuat skema eksternal yang mereferensikan pasangan skema database

tujuan dan menggunakan notasi dua bagian (`external-schema-name.table-name`). Untuk informasi selengkapnya tentang kueri lintas basis data, lihat [Mengkueri data](#) di seluruh database.

Gunakan contoh berikut untuk membuat dan menyisipkan data sampel ke dalam tabel `sales_zetl` dan `event_zetl` dari sumber `ticket_zetl`. Tabel direplikasi ke dalam database Amazon Redshift `zetl_int_db`.

```
CREATE TABLE sales_zetl (
    salesid integer NOT NULL primary key,
    eventid integer NOT NULL,
    pricepaid decimal(8, 2)
);

CREATE TABLE event_zetl (
    eventid integer NOT NULL PRIMARY KEY,
    eventname varchar(200)
);

INSERT INTO sales_zetl VALUES(1, 1, 3.33);
INSERT INTO sales_zetl VALUES(2, 2, 4.44);
INSERT INTO sales_zetl VALUES(3, 2, 5.55);

INSERT INTO event_zetl VALUES(1, "Event 1");
INSERT INTO event_zetl VALUES(2, "Event 2");
```

Anda dapat membuat tampilan terwujud untuk mendapatkan total penjualan per acara menggunakan notasi tiga bagian:

```
--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.ticket_zetl.sales_zetl S, zetl_int_db.ticket_zetl.event_zetl E
WHERE S.eventid = E.eventid
GROUP BY 1);
```

Anda dapat membuat tampilan terwujud untuk mendapatkan total penjualan per acara menggunakan notasi dua bagian:

```
--two part notation external-schema-name.table-name notation
CREATE EXTERNAL schema ext_ticket_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
);

```

Untuk melihat tampilan terwujud yang Anda buat, gunakan contoh berikut.

```
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        |
+-----+-----+

```

Mengelola integrasi nol-ETL

Anda dapat melihat detail integrasi Nol-ETL untuk melihat informasi konfigurasi dan statusnya di konsol Amazon Redshift.

Untuk melihat detail integrasi nol-ETL

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Dari panel navigasi kiri, pilih dasbor tanpa server atau klaster yang disediakan. Kemudian, pilih integrasi nol-ETL.
3. Pilih integrasi nol-ETL yang ingin Anda lihat. Untuk setiap integrasi, informasi berikut disediakan:
 - **Integration ID** adalah identifier yang dikembalikan ketika integrasi dibuat.
 - **Status** dapat menjadi salah satu dari berikut ini:
 - **Active**—Integrasi Zero-ETL mengirimkan data transaksional ke gudang data Amazon Redshift target.
 - **Syncing**— Integrasi nol-ETL telah mengalami kesalahan yang dapat dipulihkan dan sedang melakukan reseeding data. Tabel yang terpengaruh tidak tersedia untuk kueri di Amazon Redshift hingga selesai disinkronkan ulang.
 - **Failed**— Integrasi nol-ETL mengalami peristiwa atau kesalahan yang tidak dapat dipulihkan yang tidak dapat diperbaiki. Anda harus menghapus dan membuat ulang integrasi nol-ETL.
 - **Creating**—Integrasi Zero-ETL sedang dibuat.
 - **Deleting**— Integrasi nol-ETL sedang dihapus.
 - **Needs attention**—Integrasi nol-ETL mengalami peristiwa atau kesalahan yang memerlukan intervensi manual untuk menyelesaikannya. Untuk memperbaiki masalah, ikuti langkah-langkah dalam pesan kesalahan.
 - **Sumber ARN** adalah ARN dari sumber data.
 - **Tujuan** adalah ARN dari namespace gudang data target.
 - **Database** dapat menjadi salah satu dari berikut ini:
 - **No database**—Tidak ada database tujuan untuk integrasi.
 - **Creating**— Amazon Redshift membuat database tujuan untuk integrasi.
 - **Active**— Data sedang direplikasi dari sumber integrasi ke Amazon Redshift.
 - **Error**— Ada kesalahan dengan integrasi.
 - **Recovering**— Integrasi pulih setelah gudang data dimulai ulang.
 - **Resyncing**— Amazon Redshift menyinkronkan ulang tabel dalam integrasi.
 - **Jenis tujuan** adalah jenis gudang data Amazon Redshift.
 - **Tanggal pembuatan** adalah tanggal dan waktu (UTC) saat integrasi dibuat.

Note

Untuk melihat detail integrasi untuk gudang data, pilih halaman detail untuk klaster yang disediakan atau namespace tanpa server, lalu pilih tab integrasi nol-ETL.

Dari daftar integrasi Nol-ETL, Anda dapat memilih Data kueri untuk beralih ke editor kueri Amazon Redshift v2. Basis data target Amazon Redshift mengaktifkan parameter [enable_case_sensitive_identifier](#). Saat Anda menulis SQL, Anda mungkin perlu mengelilingi skema, tabel, dan nama kolom dengan tanda kutip ganda (""). Untuk informasi selengkapnya tentang kueri data di gudang data Amazon Redshift, lihat [Mengkueri database menggunakan editor kueri Amazon Redshift v2](#)

Dari daftar integrasi nol-ETL, Anda dapat memilih Bagian data untuk membuat datashare. Untuk membuat datashare untuk database Amazon Redshift, ikuti petunjuk pada halaman Create datashare. Sebelum Anda dapat berbagi data dalam database Amazon Redshift Anda, Anda harus terlebih dahulu membuat database tujuan. Untuk informasi selengkapnya tentang berbagi data, lihat [Konsep berbagi data untuk Amazon Redshift](#).

Untuk menyegarkan integrasi Anda, Anda dapat menggunakan perintah [ALTER DATABASE](#). Melakukan hal itu mereplikasi semua data dari sumber integrasi Anda ke database tujuan Anda. Contoh berikut menyegarkan semua tabel yang disinkronkan dan gagal dalam integrasi nol-ETL Anda.

```
ALTER DATABASE sample_integration_db INTEGRATION REFRESH ALL tables;
```

Berbagi data Anda di Amazon Redshift

Setelah Anda menambahkan data ke sumber, itu segera direplikasi ke Amazon Redshift dan siap untuk dibagikan dengan membuat datashares.

Untuk berbagi data, Anda harus membuat database tujuan terlebih dahulu.

Important

Untuk membagikan data dari gudang data pratinjau Amazon Redshift ke gudang data konsumen Amazon Redshift, gudang data konsumen Anda harus berada di jalur. `preview_2023` Untuk informasi selengkapnya tentang datashares, lihat [Apa itu datashare?](#) di Panduan Pengembang Database Amazon Redshift.

Untuk membuat gudang data target dalam pratinjau, lihat salah satu topik berikut tergantung pada jenis penerapan Anda:

- Cluster yang disediakan Amazon Redshift — [Membuat kluster pratinjau](#)
- Kelompok kerja Redshift Tanpa Server - [Membuat workgroup pratinjau](#)

Berbagi data di Amazon Redshift Tanpa Server menggunakan konsol Amazon Redshift

1. Di konsol Amazon Redshift, di panel navigasi kiri, pilih dasbor Amazon Redshift Tanpa Server > Tanpa Server.
2. Di panel navigasi sebelah kiri, pilih Integrasi nol-ETL.
3. Pilih Bagikan data.
4. Pada halaman create datashare, ikuti langkah-langkah dalam [Membuat](#) datashares.

Berbagi data di kluster yang disediakan Amazon Redshift menggunakan konsol Amazon Redshift

1. Di konsol Amazon Redshift, di panel navigasi kiri, pilih Dasbor cluster yang disediakan.
2. Di panel navigasi sebelah kiri, pilih Integrasi nol-ETL.
3. Dari daftar integrasi, pilih integrasi.
4. Pada halaman detail integrasi, pilih Connect to database.
5. Pada halaman Koneksi ke database, Anda dapat membuat koneksi baru atau menggunakan koneksi terbaru. Pastikan koneksi dibuat ke database tujuan.
6. Jika Anda membuat koneksi baru, maka masukkan nama Database untuk database. Kemudian, klik Connect.
7. Pada halaman detail integrasi, pilih Bagikan data.
8. Pada halaman create datashare, ikuti langkah-langkah dalam [Membuat](#) datashares.

Metrik untuk integrasi nol-ETL

Anda dapat menggunakan metrik di konsol Amazon Redshift dan CloudWatch Amazon untuk mempelajari kesehatan dan kinerja integrasi nol-ETL Anda. Anda dapat menyesuaikan metrik untuk

menampilkan data untuk durasi yang lebih pendek atau lebih lama, atau memilih untuk melihat metrik. CloudWatch Untuk melihat metrik integrasi Anda di konsol Amazon Redshift, pilih integrasi Nol-ETL di panel navigasi kiri dan pilih ID integrasi Anda.

Untuk integrasi Aurora dan Amazon RDS Zero-ETL, Amazon Redshift menyediakan dua jenis metrik pada halaman detail integrasi untuk integrasi. Jenis metriknya adalah sebagai berikut:

- Dari tab Metrik Integrasi, ini adalah bagan yang tersedia:

Metrik	Deskripsi
Lag	<p>Kelambatan dari data waktu berkomitmen ke sumber Anda hingga saat data tersedia untuk kueri di Amazon Redshift.</p> <p>Unit: Kedua</p> <p>Dimensi: IntegrationLag</p>
Tables replicated	<p>Jumlah tabel yang telah direplikasi dari database sumber Anda ke Amazon Redshift.</p> <p>Unit: Hitungan</p> <p>Dimensi: IntegrationNumTablesReplicated</p>
Tables failed	<p>Jumlah tabel yang gagal replikasi.</p> <p>Unit: Hitungan</p> <p>Dimensi: IntegrationNumTablesFailedReplicatio n</p>

- Dari tab Statistik tabel, Anda dapat melihat daftar tabel yang saat ini aktif atau mengalami kesalahan. Statistik pada tab ini adalah sebagai berikut:
 - Nama skema — Nama skema tempat tabel berada.
 - Nama tabel — Nama tabel dalam database sumber.
 - Status — Status tabel. Nilai yang mungkin termasuk adalah Synced, Failed, Deleted, Resync Required, dan Resync Initiated.
 - Database — Database Amazon Redshift tempat tabelnya berada.

- Terakhir diperbarui - Tanggal dan waktu (UTC) saat pembaruan terakhir dilakukan ke tabel.

Memecahkan masalah integrasi nol-ETL

Memecahkan masalah integrasi nol-ETL dengan Aurora MySQL

Gunakan informasi berikut untuk memecahkan masalah umum dengan integrasi Nol-ETL dengan Aurora MySQL.

Topik

- [Pembuatan integrasi gagal](#)
- [Tabel tidak memiliki kunci utama](#)
- [Tipe data yang tidak didukung dalam tabel](#)
- [Perintah bahasa manipulasi data gagal](#)
- [Perubahan yang dilacak antar sumber data tidak cocok](#)
- [Otorisasi gagal](#)
- [Jumlah tabel lebih dari 100K atau jumlah skema lebih dari 4950](#)
- [Amazon Redshift tidak dapat memuat data](#)
- [Pengaturan parameter Workgroup salah](#)
- [Database tidak dibuat untuk mengaktifkan integrasi nol-ETL](#)
- [Tabel berada dalam status Resinkronisasi Diperlukan atau Resinkronisasi Inisiasi](#)

Pembuatan integrasi gagal

Jika pembuatan integrasi nol-ETL gagal, status integrasinya adalah. Inactive Pastikan bahwa berikut ini benar untuk cluster Aurora DB sumber Anda:

- Anda membuat cluster Anda di konsol Amazon RDS.
- Cluster Aurora DB sumber Anda menjalankan MySQL versi 3.05 atau lebih tinggi. Untuk memvalidasi ini, buka tab Konfigurasi untuk cluster dan periksa versi Engine.
- Anda mengonfigurasi pengaturan parameter binlog dengan benar untuk cluster Anda. Jika parameter binlog Aurora MySQL Anda disetel secara tidak benar atau tidak terkait dengan cluster Aurora DB sumber, pembuatan gagal. Lihat [Mengkonfigurasi parameter cluster DB](#).

Selain itu, pastikan yang berikut ini benar untuk gudang data Amazon Redshift Anda:

- Sensitivitas kasus dihidupkan. Lihat [Aktifkan sensitivitas huruf besar untuk gudang data Anda](#).
- Anda menambahkan sumber utama dan integrasi resmi yang benar untuk namespace Anda. Lihat [Konfigurasi otorisasi untuk gudang data Amazon Redshift Anda](#).

Tabel tidak memiliki kunci utama

Dalam database tujuan, satu atau beberapa tabel tidak memiliki kunci utama dan tidak dapat disinkronkan.

Untuk mengatasi masalah ini, buka tab Statistik tabel di halaman detail integrasi atau gunakan `SVV_INTEGRATION_TABLE_STATE` untuk melihat tabel yang gagal. Anda dapat menambahkan kunci utama ke tabel dan Amazon Redshift akan menyinkronkan ulang tabel. Atau, meskipun tidak disarankan, Anda dapat menjatuhkan tabel ini di Aurora dan membuat tabel dengan kunci utama. Untuk informasi selengkapnya, lihat [Praktik terbaik Amazon Redshift untuk mendesain tabel](#).

Tipe data yang tidak didukung dalam tabel

Dalam database yang Anda buat dari integrasi di Amazon Redshift dan di mana data direplikasi dari cluster Aurora DB, satu atau beberapa tabel memiliki tipe data yang tidak didukung dan tidak dapat disinkronkan.

Untuk mengatasi masalah ini, buka tab Statistik tabel di halaman detail integrasi atau gunakan `SVV_INTEGRATION_TABLE_STATE` untuk melihat tabel yang gagal. Kemudian, hapus tabel ini dan buat ulang tabel baru di Amazon RDS. Untuk informasi selengkapnya tentang tipe data yang tidak didukung, lihat [Perbedaan tipe data antara database Aurora dan Amazon Redshift di Panduan Pengguna Amazon Aurora](#).

Perintah bahasa manipulasi data gagal

Amazon Redshift tidak dapat menjalankan perintah DHTML pada tabel Redshift. Untuk mengatasi masalah ini, gunakan `SVV_INTEGRATION_TABLE_STATE` untuk melihat tabel yang gagal. Amazon Redshift secara otomatis menyinkronkan ulang tabel untuk mengatasi kesalahan ini.

Perubahan yang dilacak antar sumber data tidak cocok

Kesalahan ini terjadi ketika perubahan antara Amazon Aurora dan Amazon Redshift tidak cocok, yang menyebabkan integrasi memasuki status. `Failed`

Untuk mengatasi ini, hapus integrasi nol-ETL dan buat lagi di Amazon RDS. [Untuk informasi selengkapnya, lihat Membuat integrasi Nol-ETL dan Menghapus integrasi Nol-ETL.](#)

Otorisasi gagal

Otorisasi gagal karena sumber cluster Aurora DB telah dihapus sebagai sumber integrasi resmi untuk gudang data Amazon Redshift.

Untuk mengatasi masalah ini, hapus integrasi nol-ETL dan buat lagi di Amazon RDS. [Untuk informasi selengkapnya, lihat Membuat integrasi Nol-ETL dan Menghapus integrasi Nol-ETL.](#)

Jumlah tabel lebih dari 100K atau jumlah skema lebih dari 4950

Untuk gudang data tujuan, jumlah tabel lebih dari 100K atau jumlah skema lebih dari 4950. Amazon Aurora tidak dapat mengirim data ke Amazon Redshift. Jumlah tabel dan skema melebihi batas yang ditetapkan. Untuk mengatasi masalah ini, hapus skema atau tabel yang tidak perlu dari database sumber.

Amazon Redshift tidak dapat memuat data

Amazon Redshift tidak dapat memuat data ke integrasi Nol-ETL.

Untuk mengatasi masalah ini, hapus integrasi nol-ETL di Amazon RDS dan buat lagi. [Untuk informasi selengkapnya, lihat Membuat integrasi Nol-ETL dan Menghapus integrasi Nol-ETL.](#)

Pengaturan parameter Workgroup salah

Workgroup Anda tidak mengaktifkan sensitivitas huruf besar/case sensitivity.

Untuk mengatasi masalah ini, buka tab Properties pada halaman detail integrasi, pilih grup parameter, dan aktifkan pengenalan peka huruf besar/kecil dari tab Properties. Jika Anda tidak memiliki grup parameter yang ada, buat satu dengan pengidentifikasi peka huruf besar/kecil diaktifkan. Kemudian, buat integrasi nol-ETL baru di Amazon RDS. Untuk informasi selengkapnya, lihat [Membuat integrasi nol-ETL.](#)

Database tidak dibuat untuk mengaktifkan integrasi nol-ETL

Tidak ada database yang dibuat untuk integrasi nol-ETL untuk mengaktifkannya.

Untuk mengatasi masalah ini, buat database untuk integrasi. Untuk informasi selengkapnya, lihat [Membuat database tujuan di Amazon Redshift.](#)

Tabel berada dalam status Resinkronisasi Diperlukan atau Resinkronisasi Inisiasi

Tabel Anda berada dalam status Resinkronisasi Diperlukan atau Resinkronisasi Inisiasi.

Untuk mengumpulkan informasi kesalahan yang lebih rinci tentang mengapa tabel Anda berada dalam status itu, gunakan tampilan [sistem SYS_LOAD_ERROR_DETAIL](#).

Memecahkan masalah integrasi nol-ETL dengan Aurora PostgreSQL

Gunakan informasi berikut untuk memecahkan masalah umum dengan integrasi nol-ETL dengan Aurora PostgreSQL.

Topik

- [Pembuatan integrasi gagal](#)
- [Tabel tidak memiliki kunci utama](#)
- [Tipe data yang tidak didukung dalam tabel](#)
- [Perintah bahasa manipulasi data gagal](#)
- [Perubahan yang dilacak antar sumber data tidak cocok](#)
- [Otorisasi gagal](#)
- [Jumlah tabel lebih dari 100K atau jumlah skema lebih dari 4950](#)
- [Amazon Redshift tidak dapat memuat data](#)
- [Pengaturan parameter Workgroup salah](#)
- [Database tidak dibuat untuk mengaktifkan integrasi nol-ETL](#)
- [Tabel berada dalam status Resinkronisasi Diperlukan atau Resinkronisasi Inisiasi](#)

Pembuatan integrasi gagal

Jika pembuatan integrasi nol-ETL gagal, status integrasinya adalah `Inactive`. Pastikan bahwa berikut ini benar untuk cluster Aurora DB sumber Anda:

- Anda membuat cluster Anda di konsol Amazon RDS.
- Cluster Aurora DB sumber Anda menjalankan Aurora PostgreSQL versi 15.4.99 atau lebih tinggi. Untuk memvalidasi ini, buka tab Konfigurasi untuk cluster dan periksa versi Engine.
- Anda mengonfigurasi pengaturan parameter binlog dengan benar untuk cluster Anda. Jika parameter binlog Aurora PostgreSQL Anda disetel secara tidak benar atau tidak terkait dengan cluster Aurora DB sumber, pembuatan gagal. Lihat [Mengkonfigurasi parameter cluster DB](#).

Selain itu, pastikan yang berikut ini benar untuk gudang data Amazon Redshift Anda:

- Sensitivitas kasus dihidupkan. Lihat [Aktifkan sensitivitas huruf besar untuk gudang data Anda](#).
- Anda menambahkan sumber utama dan integrasi resmi yang benar untuk `endterm="zero-etl-using.redshift-iam.title" />`.

Tabel tidak memiliki kunci utama

Dalam database tujuan, satu atau beberapa tabel tidak memiliki kunci utama dan tidak dapat disinkronkan.

Untuk mengatasi masalah ini, buka tab Statistik tabel di halaman detail integrasi atau gunakan `SVV_INTEGRATION_TABLE_STATE` untuk melihat tabel yang gagal. Anda dapat menambahkan kunci utama ke tabel dan Amazon Redshift akan menyinkronkan ulang tabel. Atau, meskipun tidak disarankan, Anda dapat menjatuhkan tabel ini di Aurora dan membuat tabel dengan kunci utama. Untuk informasi selengkapnya, lihat [Praktik terbaik Amazon Redshift untuk mendesain tabel](#).

Tipe data yang tidak didukung dalam tabel

Dalam database yang Anda buat dari integrasi di Amazon Redshift dan di mana data direplikasi dari cluster Aurora DB, satu atau beberapa tabel memiliki tipe data yang tidak didukung dan tidak dapat disinkronkan.

Untuk mengatasi masalah ini, buka tab Statistik tabel di halaman detail integrasi atau gunakan `SVV_INTEGRATION_TABLE_STATE` untuk melihat tabel yang gagal. Kemudian, hapus tabel ini dan buat ulang tabel baru di Amazon RDS. Untuk informasi selengkapnya tentang tipe data yang tidak didukung, lihat [Perbedaan tipe data antara database Aurora dan Amazon Redshift di Panduan Pengguna Amazon Aurora](#).

Perintah bahasa manipulasi data gagal

Amazon Redshift tidak dapat menjalankan perintah DHTML pada tabel Redshift. Untuk mengatasi masalah ini, gunakan `SVV_INTEGRATION_TABLE_STATE` untuk melihat tabel yang gagal. Amazon Redshift secara otomatis menyinkronkan ulang tabel untuk mengatasi kesalahan ini.

Perubahan yang dilacak antar sumber data tidak cocok

Kesalahan ini terjadi ketika perubahan antara Amazon Aurora dan Amazon Redshift tidak cocok, yang menyebabkan integrasi memasuki status. `Failed`

Untuk mengatasi ini, hapus integrasi nol-ETL dan buat lagi di Amazon RDS. [Untuk informasi selengkapnya, lihat Membuat integrasi Nol-ETL dan Menghapus integrasi Nol-ETL.](#)

Otorisasi gagal

Otorisasi gagal karena sumber cluster Aurora DB telah dihapus sebagai sumber integrasi resmi untuk gudang data Amazon Redshift.

Untuk mengatasi masalah ini, hapus integrasi nol-ETL dan buat lagi di Amazon RDS. [Untuk informasi selengkapnya, lihat Membuat integrasi Nol-ETL dan Menghapus integrasi Nol-ETL.](#)

Jumlah tabel lebih dari 100K atau jumlah skema lebih dari 4950

Untuk gudang data tujuan, jumlah tabel lebih dari 100K atau jumlah skema lebih dari 4950. Amazon Aurora tidak dapat mengirim data ke Amazon Redshift. Jumlah tabel dan skema melebihi batas yang ditetapkan. Untuk mengatasi masalah ini, hapus skema atau tabel yang tidak perlu dari database sumber.

Amazon Redshift tidak dapat memuat data

Amazon Redshift tidak dapat memuat data ke integrasi Nol-ETL.

Untuk mengatasi masalah ini, hapus integrasi nol-ETL di Amazon RDS dan buat lagi. [Untuk informasi selengkapnya, lihat Membuat integrasi Nol-ETL dan Menghapus integrasi Nol-ETL.](#)

Pengaturan parameter Workgroup salah

Workgroup Anda tidak mengaktifkan sensitivitas huruf besar/case sensitivity.

Untuk mengatasi masalah ini, buka tab Properties pada halaman detail integrasi, pilih grup parameter, dan aktifkan pengenalan peka huruf besar/kecil dari tab Properties. Jika Anda tidak memiliki grup parameter yang ada, buat satu dengan pengidentifikasi peka huruf besar/kecil diaktifkan. Kemudian, buat integrasi nol-ETL baru di Amazon RDS. Untuk informasi selengkapnya, lihat [Membuat integrasi nol-ETL.](#)

Database tidak dibuat untuk mengaktifkan integrasi nol-ETL

Tidak ada database yang dibuat untuk integrasi nol-ETL untuk mengaktifkannya.

Untuk mengatasi masalah ini, buat database untuk integrasi. Untuk informasi selengkapnya, lihat [Membuat database tujuan di Amazon Redshift.](#)

Tabel berada dalam status Resinkronisasi Diperlukan atau Resinkronisasi Inisiasi

Tabel Anda berada dalam status Resinkronisasi Diperlukan atau Resinkronisasi Inisiasi.

Untuk mengumpulkan informasi kesalahan yang lebih rinci tentang mengapa tabel Anda berada dalam status itu, gunakan tampilan [sistem SYS_LOAD_ERROR_DETAIL](#).

Memecahkan masalah integrasi nol-ETL dengan RDS untuk MySQL

Gunakan informasi berikut untuk memecahkan masalah umum dengan integrasi nol-ETL dengan RDS untuk MySQL.

Topik

- [Pembuatan integrasi gagal](#)
- [Tabel tidak memiliki kunci utama](#)
- [Tipe data yang tidak didukung dalam tabel](#)
- [Perintah bahasa manipulasi data gagal](#)
- [Perubahan yang dilacak antar sumber data tidak cocok](#)
- [Otorisasi gagal](#)
- [Jumlah tabel lebih dari 100K atau jumlah skema lebih dari 4950](#)
- [Amazon Redshift tidak dapat memuat data](#)
- [Pengaturan parameter Workgroup salah](#)
- [Database tidak dibuat untuk mengaktifkan integrasi nol-ETL](#)
- [Tabel berada dalam status Resinkronisasi Diperlukan atau Resinkronisasi Inisiasi](#)

Pembuatan integrasi gagal

Jika pembuatan integrasi nol-ETL gagal, status integrasinya adalah. Inactive Pastikan bahwa berikut ini benar untuk instans RDS DB sumber Anda:

- Anda membuat instans Anda di konsol Amazon RDS.
- Instance RDS DB sumber Anda menjalankan RDS untuk MySQL versi 8.0.32 atau lebih tinggi. Untuk memvalidasi ini, buka tab Konfigurasi untuk instance dan periksa versi Engine.
- Anda mengonfigurasi pengaturan parameter binlog dengan benar untuk instance Anda. Jika parameter binlog RDS untuk MySQL Anda disetel secara tidak benar atau tidak terkait dengan instans RDS DB sumber, pembuatan gagal. Lihat [Mengkonfigurasi parameter instans DB](#).

Selain itu, pastikan yang berikut ini benar untuk gudang data Amazon Redshift Anda:

- Sensitivitas kasus dihidupkan. Lihat [Aktifkan sensitivitas huruf besar untuk gudang data Anda](#).
- Anda menambahkan sumber utama dan integrasi resmi yang benar untuk namespace Anda. Lihat [Konfigurasi otorisasi untuk gudang data Amazon Redshift Anda](#).

Tabel tidak memiliki kunci utama

Dalam database tujuan, satu atau beberapa tabel tidak memiliki kunci utama dan tidak dapat disinkronkan.

Untuk mengatasi masalah ini, buka tab Statistik tabel di halaman detail integrasi atau gunakan `SVV_INTEGRATION_TABLE_STATE` untuk melihat tabel yang gagal. Anda dapat menambahkan kunci utama ke tabel dan Amazon Redshift akan menyinkronkan ulang tabel. Atau, meskipun tidak disarankan, Anda dapat menjatuhkan tabel ini pada RDS dan membuat tabel dengan kunci utama. Untuk informasi selengkapnya, lihat [Praktik terbaik Amazon Redshift untuk mendesain tabel](#).

Tipe data yang tidak didukung dalam tabel

Dalam database yang Anda buat dari integrasi di Amazon Redshift dan di mana data direplikasi dari instans RDS DB, satu atau beberapa tabel memiliki tipe data yang tidak didukung dan tidak dapat disinkronkan.

Untuk mengatasi masalah ini, buka tab Statistik tabel di halaman detail integrasi atau gunakan `SVV_INTEGRATION_TABLE_STATE` untuk melihat tabel yang gagal. Kemudian, hapus tabel ini dan buat ulang tabel baru di Amazon RDS. Untuk informasi selengkapnya tentang tipe data yang tidak didukung, lihat [Perbedaan tipe data antara database RDS dan Amazon Redshift](#) di Panduan Pengguna Amazon RDS.

Perintah bahasa manipulasi data gagal

Amazon Redshift tidak dapat menjalankan perintah DHTML pada tabel Redshift. Untuk mengatasi masalah ini, gunakan `SVV_INTEGRATION_TABLE_STATE` untuk melihat tabel yang gagal. Amazon Redshift secara otomatis menyinkronkan ulang tabel untuk mengatasi kesalahan ini.

Perubahan yang dilacak antar sumber data tidak cocok

Kesalahan ini terjadi ketika perubahan antara Amazon Aurora dan Amazon Redshift tidak cocok, yang menyebabkan integrasi memasuki status. `Failed`

Untuk mengatasi ini, hapus integrasi nol-ETL dan buat lagi di Amazon RDS. [Untuk informasi selengkapnya, lihat Membuat integrasi Nol-ETL dan Menghapus integrasi Nol-ETL.](#)

Otorisasi gagal

Otorisasi gagal karena instans RDS DB sumber telah dihapus sebagai sumber integrasi resmi untuk gudang data Amazon Redshift.

Untuk mengatasi masalah ini, hapus integrasi nol-ETL dan buat lagi di Amazon RDS. [Untuk informasi selengkapnya, lihat Membuat integrasi Nol-ETL dan Menghapus integrasi Nol-ETL.](#)

Jumlah tabel lebih dari 100K atau jumlah skema lebih dari 4950

Untuk gudang data tujuan, jumlah tabel lebih dari 100K atau jumlah skema lebih dari 4950. Amazon Aurora tidak dapat mengirim data ke Amazon Redshift. Jumlah tabel dan skema melebihi batas yang ditetapkan. Untuk mengatasi masalah ini, hapus skema atau tabel yang tidak perlu dari database sumber.

Amazon Redshift tidak dapat memuat data

Amazon Redshift tidak dapat memuat data ke integrasi Nol-ETL.

Untuk mengatasi masalah ini, hapus integrasi nol-ETL di Amazon RDS dan buat lagi. [Untuk informasi selengkapnya, lihat Membuat integrasi Nol-ETL dan Menghapus integrasi Nol-ETL.](#)

Pengaturan parameter Workgroup salah

Workgroup Anda tidak mengaktifkan sensitivitas huruf besar/case sensitivity.

Untuk mengatasi masalah ini, buka tab Properties pada halaman detail integrasi, pilih grup parameter, dan aktifkan pengenalan peka huruf besar/kecil dari tab Properties. Jika Anda tidak memiliki grup parameter yang ada, buat satu dengan pengidentifikasi peka huruf besar/kecil diaktifkan. Kemudian, buat integrasi nol-ETL baru di Amazon RDS. Untuk informasi selengkapnya, lihat [Membuat integrasi nol-ETL.](#)

Database tidak dibuat untuk mengaktifkan integrasi nol-ETL

Tidak ada database yang dibuat untuk integrasi nol-ETL untuk mengaktifkannya.

Untuk mengatasi masalah ini, buat database untuk integrasi. Untuk informasi selengkapnya, lihat [Membuat database tujuan di Amazon Redshift.](#)

Tabel berada dalam status Resinkronisasi Diperlukan atau Resinkronisasi Inisiasi

Tabel Anda berada dalam status Resinkronisasi Diperlukan atau Resinkronisasi Inisiasi.

Untuk mengumpulkan informasi kesalahan yang lebih rinci tentang mengapa tabel Anda berada dalam status itu, gunakan tampilan [sistem SYS_LOAD_ERROR_DETAIL](#).

Meminta database

Untuk menanyakan database yang dihosting oleh cluster Amazon Redshift Anda, Anda memiliki dua opsi:

- Hubungkan ke klaster Anda dan jalankan kueri AWS Management Console dengan editor kueri.
Jika Anda menggunakan editor kueri di konsol Amazon Redshift, Anda tidak perlu mengunduh dan menyiapkan aplikasi klien SQL.
- Connect ke cluster Anda melalui alat klien SQL, seperti SQL Workbench/J.

Amazon Redshift mendukung alat klien SQL yang terhubung melalui Java Database Connectivity (JDBC) dan Open Database Connectivity (ODBC). Amazon Redshift tidak menyediakan atau menginstal alat atau pustaka klien SQL apa pun, jadi Anda harus menginstalnya di komputer klien atau instans Amazon EC2 untuk menggunakannya. Anda dapat menggunakan sebagian besar alat klien SQL yang mendukung driver JDBC atau ODBC.

Note

Saat Anda menulis prosedur tersimpan, kami merekomendasikan praktik terbaik untuk mengamankan nilai sensitif:

Jangan membuat kode keras informasi sensitif apa pun dalam logika prosedur yang disimpan. Misalnya, jangan tetapkan kata sandi pengguna dalam pernyataan CREATE USER di badan prosedur yang disimpan. Ini menimbulkan risiko keamanan, karena nilai hard-code dapat dicatat sebagai metadata skema dalam tabel katalog. Sebagai gantinya, berikan nilai sensitif, seperti kata sandi, sebagai argumen ke prosedur yang disimpan, melalui parameter. Untuk informasi selengkapnya tentang prosedur tersimpan, lihat [MEMBUAT PROSEDUR](#) dan [Membuat prosedur tersimpan di Amazon Redshift](#). Untuk informasi selengkapnya tentang tabel katalog, lihat [Tabel katalog sistem](#).

Topik

- [Menghubungkan ke Amazon Redshift](#)
- [Mengkueri database menggunakan editor kueri Amazon Redshift v2](#)
- [Menanyakan database menggunakan editor kueri](#)
- [Menyambung ke gudang data Amazon Redshift menggunakan alat klien SQL](#)

- [Menggunakan API Data Amazon Redshift](#)

Menghubungkan ke Amazon Redshift

Anda dapat terhubung ke database Anda menggunakan sintaks berikut.

```
cluster-name.account-number.aws-region.redshift.amazonaws.com/database-name
```

Elemen sintaks didefinisikan sebagai berikut.

- `cluster-name`

Nama kluster Anda.

- `account-number`

Pengenal unik yang terkait dengan nomor AWS akun Anda di tertentu Wilayah AWS. Semua cluster yang dibuat oleh akun tertentu di tertentu Wilayah AWS memiliki hal yang sama `account-number`.

- `aws-region`

Kode untuk tempat Wilayah AWS cluster berada.

- `database-name`

Nama database Anda.

Misalnya, string koneksi berikut menentukan `my-db` database dalam `my-cluster` cluster di Wilayah AWS `us-east-1`.

```
my-cluster.123456789012.us-east-1.redshift.amazonaws.com/my-db
```

Mengkueri database menggunakan editor kueri Amazon Redshift v2

Editor kueri v2 adalah aplikasi klien SQL berbasis web terpisah yang Anda gunakan untuk membuat dan menjalankan kueri di gudang data Amazon Redshift Anda. Anda dapat memvisualisasikan hasil

Anda dalam bagan dan berkolaborasi dengan membagikan pertanyaan Anda dengan orang lain di tim Anda. Editor kueri v2 adalah pengganti editor kueri sebelumnya.

Note

Editor kueri v2 tersedia dalam komersial Wilayah AWS. Untuk daftar Wilayah AWS di mana editor kueri v2 tersedia, lihat titik akhir yang terdaftar untuk [Redshift query editor](#) v2 di Referensi Umum Amazon Web Services

Untuk demo query editor v2, tonton video berikut. [Editor kueri Amazon Redshift v2](#).

Untuk demo analisis data, tonton video berikut. [Analisis data menggunakan editor kueri Amazon Redshift v2](#).

Untuk demo menggunakan editor kueri v2 yang menjalankan beberapa kueri dengan koneksi terisolasi atau bersama, tonton video berikut. [Eksekusi Query Concurrent menggunakan Query Editor v2](#).

Editor kueri v2 memiliki serangkaian fitur yang kaya untuk mengelola dan menjalankan pernyataan SQL Anda. Topik di bagian berikut membantu Anda memulai dengan banyak fitur ini. Jelajahi editor kueri v2 Anda sendiri untuk membiasakan diri dengan kemampuannya.

Topik

- [Mengkonfigurasi Akun AWS](#)
- [Bekerja dengan editor kueri v2](#)
- [Berinteraksi dengan editor kueri v2 generatif SQL \(pratinjau\)](#)
- [Memuat data ke dalam database](#)
- [Menulis dan menjalankan kueri](#)
- [Menulis dan menjalankan notebook](#)
- [Menanyakan AWS Glue Data Catalog](#)
- [Menanyakan data lake](#)
- [Bekerja dengan datashares](#)
- [Menjadwalkan kueri dengan editor kueri v2](#)
- [Memvisualisasikan hasil kueri](#)
- [Berkolaborasi dan berbagi sebagai sebuah tim](#)

Mengkonfigurasi Akun AWS

Saat Anda memilih editor kueri v2 dari konsol Amazon Redshift, tab baru di browser Anda terbuka dengan antarmuka editor kueri v2. Dengan izin yang tepat, Anda dapat mengakses data di klaster Amazon Redshift atau grup kerja milik Akun AWS Anda yang ada di saat ini. Wilayah AWS

Pertama kali administrator mengonfigurasi editor kueri v2 untuk Anda Akun AWS, mereka memilih AWS KMS key yang digunakan untuk mengenkripsi sumber daya editor kueri v2. Secara default, kunci yang AWS dimiliki digunakan untuk mengenkripsi sumber daya. Atau administrator dapat menggunakan kunci yang dikelola pelanggan dengan memilih Nama Sumber Daya Amazon (ARN) untuk kunci di halaman konfigurasi. Setelah mengonfigurasi akun, pengaturan AWS KMS enkripsi tidak dapat diubah. Untuk informasi selengkapnya tentang membuat dan menggunakan kunci yang dikelola pelanggan dengan editor kueri v2, lihat [Membuat kunci yang dikelola AWS KMS pelanggan untuk digunakan dengan editor kueri v2](#). Administrator juga dapat secara opsional memilih bucket dan jalur S3 yang digunakan untuk beberapa fitur, seperti memuat data dari file. Untuk informasi selengkapnya, lihat [Memuat data dari pengaturan file lokal dan alur kerja](#).

Editor kueri Amazon Redshift v2 mendukung autentikasi, enkripsi, isolasi, dan kepatuhan untuk menjaga data Anda tetap diam dan data dalam transit tetap aman. Untuk informasi selengkapnya tentang keamanan data dan editor kueri v2, lihat berikut ini:

- [Enkripsi diam](#)
- [Enkripsi dalam bergerak](#)
- [Analisis konfigurasi dan kelemahan di Amazon Redshift](#)

AWS CloudTrail menangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama Anda Akun AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk mempelajari selengkapnya tentang bagaimana editor kueri v2 berjalan AWS CloudTrail, lihat [Logging dengan CloudTrail](#). Untuk informasi selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

Editor kueri v2 memiliki kuota yang dapat disesuaikan untuk beberapa sumber dayanya. Untuk informasi selengkapnya, lihat [Kuota untuk objek Amazon Redshift](#).

Sumber daya dibuat dengan editor kueri v2

Dalam editor kueri v2, Anda dapat membuat sumber daya seperti kueri dan bagan yang disimpan. Semua sumber daya di editor kueri v2 dikaitkan dengan peran IAM atau dengan pengguna. Sebaiknya Anda melampirkan kebijakan ke peran IAM dan menetapkan peran tersebut kepada pengguna.

Di editor kueri v2, Anda dapat menambahkan dan menghapus tag untuk kueri dan bagan yang disimpan. Anda dapat menggunakan tag ini saat menyiapkan kebijakan IAM khusus atau untuk mencari sumber daya. Anda juga dapat mengelola tag dengan menggunakan Editor AWS Resource Groups Tag.

Anda dapat mengatur peran IAM dengan kebijakan IAM untuk berbagi kueri dengan orang lain di bagian yang sama Akun AWS . Wilayah AWS

Membuat kunci yang dikelola AWS KMS pelanggan untuk digunakan dengan editor kueri v2

Untuk membuat kunci terkelola enkripsi simetris yang dikelola pelanggan:

Anda dapat membuat kunci terkelola pelanggan enkripsi simetris untuk mengenkripsi sumber daya editor kueri v2 menggunakan operasi AWS KMS konsol atau AWS KMS API. Untuk petunjuk tentang membuat kunci, lihat [Membuat AWS KMS kunci enkripsi simetris](#) di Panduan AWS Key Management Service Pengembang.

Kebijakan utama

Kebijakan utama mengontrol akses ke kunci yang dikelola pelanggan Anda. Setiap kunci yang dikelola pelanggan harus memiliki persis satu kebijakan utama, yang berisi pernyataan yang menentukan siapa yang dapat menggunakan kunci dan bagaimana mereka dapat menggunakannya. Saat membuat kunci terkelola pelanggan, Anda dapat menentukan kebijakan kunci. Untuk informasi selengkapnya, lihat [Mengelola akses ke AWS KMS kunci](#) di Panduan AWS Key Management Service Pengembang.

Untuk menggunakan kunci terkelola pelanggan Anda dengan editor kueri Amazon Redshift v2, operasi API berikut harus diizinkan dalam kebijakan kunci:

- `kms:GenerateDataKey`— Menghasilkan kunci data simetris yang unik untuk mengenkripsi data Anda.

- `kms:Decrypt`— Mendekripsi data yang dienkripsi dengan kunci yang dikelola pelanggan.
- `kms:DescribeKey`— Memberikan detail kunci yang dikelola pelanggan untuk memungkinkan layanan memvalidasi kunci.

Berikut ini adalah contoh AWS KMS kebijakan untuk Akun AWS 111122223333. Di bagian pertama, `kms:ViaService` batas penggunaan kunci untuk layanan editor kueri v2 (yang dinamai `sqlworkbench.region.amazonaws.com` dalam kebijakan). Akun AWS Menggunakan kunci harus111122223333. Di bagian kedua, pengguna root dan administrator kunci Akun AWS 111122223333 dapat mengakses ke kunci.

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy",
  "Statement": [
    {
      "Sid": "Allow access to principals authorized to use Amazon Redshift Query Editor V2",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "sqlworkbench.region.amazonaws.com",
          "kms:CallerAccount": "111122223333"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "Allow access for key administrators",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
      "kms:*"
    ],
    "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
  }
]
}

```

Sumber daya berikut memberikan informasi lebih lanjut tentang AWS KMS kunci:

- Untuk informasi selengkapnya tentang AWS KMS kebijakan, lihat [Menentukan izin dalam kebijakan di Panduan AWS Key Management Service](#) Pengembang.
- Untuk informasi tentang AWS KMS kebijakan pemecahan masalah, lihat [Memecahkan masalah akses kunci](#) di Panduan Pengembang.AWS Key Management Service
- Untuk informasi selengkapnya tentang kunci, lihat [kunci AWS KMS](#) di Panduan AWS Key Management Service Pengembang.

Mengakses editor kueri v2

Untuk mengakses editor kueri v2, Anda memerlukan izin. Administrator dapat melampirkan salah satu kebijakan AWS terkelola berikut ke peran untuk memberikan izin. (Kami merekomendasikan untuk melampirkan kebijakan ke peran IAM dan menetapkan peran tersebut kepada pengguna.) Kebijakan AWS terkelola ini ditulis dengan opsi berbeda yang mengontrol bagaimana sumber daya penandaan memungkinkan berbagi kueri. Anda dapat menggunakan konsol IAM (<https://console.aws.amazon.com/iam/>) untuk melampirkan kebijakan IAM.

- AmazonRedshiftQueryEditorV2 FullAccess - Memberikan akses penuh ke operasi dan sumber daya editor kueri Amazon Redshift v2. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan.

- AmazonRedshiftQueryEditorV2 NoSharing - Memberikan kemampuan untuk bekerja dengan editor kueri Amazon Redshift v2 tanpa berbagi sumber daya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan.
- AmazonRedshiftQueryEditorV2 ReadSharing - Memberikan kemampuan untuk bekerja dengan editor kueri Amazon Redshift v2 dengan berbagi sumber daya yang terbatas. Prinsipal yang diberikan dapat membaca sumber daya yang dibagikan dengan timnya tetapi tidak dapat memperbaruinya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan.
- AmazonRedshiftQueryEditorReadWriteBerbagi V2 - Memberikan kemampuan untuk bekerja dengan editor kueri Amazon Redshift v2 dengan berbagi sumber daya. Kepala sekolah yang diberikan dapat membaca dan memperbarui sumber daya yang dibagikan dengan timnya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan.

Anda juga dapat membuat kebijakan sendiri berdasarkan izin yang diizinkan dan ditolak dalam kebijakan terkelola yang disediakan. Jika Anda menggunakan editor kebijakan konsol IAM untuk membuat kebijakan Anda sendiri, pilih SQL Workbench sebagai layanan yang Anda buat kebijakan di editor visual. Query editor v2 menggunakan nama layanan AWS SQL Workbench di editor visual dan IAM Policy Simulator.

Untuk prinsipal (pengguna dengan peran IAM yang ditetapkan) untuk terhubung ke kluster Amazon Redshift, mereka memerlukan izin di salah satu kebijakan terkelola editor kueri v2. Mereka juga membutuhkan `redshift:GetClusterCredentials` izin ke cluster. Untuk mendapatkan izin ini, seseorang dengan izin administratif dapat melampirkan kebijakan ke peran IAM yang digunakan untuk terhubung ke kluster dengan menggunakan kredensial sementara. Anda dapat membuat cakupan kebijakan ke kluster tertentu atau lebih umum. Untuk informasi selengkapnya tentang izin untuk menggunakan kredensial sementara, lihat [Membuat peran IAM atau pengguna dengan izin](#) untuk menelepon. `GetClusterCredentials`

Untuk prinsipal (biasanya pengguna dengan peran IAM yang ditetapkan) untuk mengaktifkan kemampuan di halaman Pengaturan akun untuk orang lain di akun ke set hasil Ekspor, mereka memerlukan `sqlworkbench:UpdateAccountExportSettings` izin yang dilampirkan peran tersebut. Izin ini termasuk dalam kebijakan `AmazonRedshiftQueryEditorV2FullAccess` AWS terkelola.

Karena fitur baru ditambahkan ke editor kueri v2, kebijakan AWS terkelola diperbarui sesuai kebutuhan. Jika Anda membuat kebijakan sendiri berdasarkan izin yang diizinkan dan ditolak dalam kebijakan terkelola yang disediakan, edit kebijakan Anda agar tetap up to date dengan perubahan

pada kebijakan terkelola. Untuk informasi selengkapnya tentang kebijakan terkelola di Amazon Redshift, lihat. [AWS kebijakan terkelola untuk Amazon Redshift](#)

Untuk memberikan akses, menambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

Buat rangkaian izin. Ikuti instruksi di [Buat rangkaian izin](#) di Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

Buat peran untuk federasi identitas. Ikuti instruksi dalam [Membuat peran untuk penyedia identitas pihak ketiga \(federasi\)](#) di Panduan Pengguna IAM.

- Pengguna IAM:

- Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam [Membuat peran untuk pengguna IAM](#) dalam Panduan Pengguna IAM.
- (Tidak disarankan) Pasang kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti instruksi dalam [Menambahkan izin ke pengguna \(konsol\)](#) dalam Panduan Pengguna IAM.

Note

Jika AWS IAM Identity Center administrator menghapus semua asosiasi set izin untuk set izin tertentu di seluruh akun, akses ke sumber daya editor kueri yang awalnya terkait dengan kumpulan izin yang dihapus tidak lagi dapat diakses. Jika nanti izin yang sama dibuat ulang, pengenalan internal baru dibuat. Karena pengenalan internal telah berubah, akses ke sumber daya editor kueri yang sebelumnya dimiliki oleh pengguna tidak dapat diakses. Sebaiknya sebelum administrator menghapus set izin, pengguna izin tersebut menetapkan sumber daya editor kueri ekspor seperti buku catatan dan kueri sebagai cadangan.

Menyiapkan tag utama untuk menghubungkan cluster atau workgroup dari editor kueri v2

Untuk terhubung ke kluster atau grup kerja menggunakan opsi pengguna federasi, siapkan peran IAM Anda atau pengguna dengan tag utama. Atau, atur penyedia identitas Anda (iDP) untuk masuk `RedshiftDbUser` dan (opsional). `RedshiftDbGroups` Untuk informasi selengkapnya

tentang menggunakan IAM untuk mengelola tag, lihat [Melewati tag sesi AWS Security Token Service di Panduan Pengguna IAM](#). Untuk mengatur akses menggunakan AWS Identity and Access Management, administrator dapat menambahkan tag menggunakan konsol IAM (<https://console.aws.amazon.com/iam/>).

Untuk menambahkan tag utama ke peran IAM

1. Masuk ke AWS Management Console dan buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Pilih Peran di panel navigasi.
3. Pilih peran yang memerlukan akses ke editor kueri v2 menggunakan pengguna federasi.
4. Pilih tab Tanda.
5. Pilih tag Kelola.
6. Pilih Tambah tag dan masukkan Kunci sebagai `RedshiftDbUser` dan masukkan Nilai nama pengguna federasi.
7. Secara opsional pilih Tambahkan tag dan masukkan Kunci sebagai `RedshiftDbGroups` dan masukkan Nilai nama grup untuk dikaitkan dengan pengguna.
8. Pilih Simpan perubahan untuk melihat daftar tag yang terkait dengan peran IAM yang Anda pilih. Menyebarkan perubahan mungkin memakan waktu beberapa detik.
9. Untuk menggunakan pengguna federasi, segarkan halaman v2 editor kueri Anda setelah perubahan disebar.

Siapkan penyedia identitas Anda (iDP) untuk meneruskan tag utama

Prosedur untuk mengatur tag menggunakan penyedia identitas (iDP) bervariasi menurut IDP. Lihat dokumentasi IDP Anda untuk petunjuk tentang cara meneruskan informasi pengguna dan grup ke atribut SAMP. Ketika dikonfigurasi dengan benar, atribut berikut muncul dalam respons SAMP Anda yang digunakan oleh AWS Security Token Service untuk mengisi tag utama untuk `RedshiftDbUser` dan `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>
```

Db_groups opsional harus berupa daftar yang dipisahkan titik dua seperti.

```
group1:group2:group3
```

Selain itu, Anda dapat mengatur `TransitiveTagKeys` atribut untuk mempertahankan tag selama rantai peran.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
  <AttributeValue>RedshiftDbUser</AttributeValue>
  <AttributeValue>RedshiftDbGroups</AttributeValue>
</Attribute>
```

Untuk informasi selengkapnya tentang menyiapkan editor kueri v2, lihat [izin yang diperlukan untuk menggunakan editor kueri v2](#).

Note

Saat Anda terhubung ke klaster atau grup kerja menggunakan opsi koneksi pengguna Federasi dari editor kueri v2, Penyedia Identitas (IDP) dapat menyediakan tag utama khusus untuk dan. `RedshiftDbUser` `RedshiftDbGroups` Saat ini, AWS IAM Identity Center doesn't support tag utama khusus yang diteruskan langsung ke editor kueri v2.

Bekerja dengan editor kueri v2

Editor kueri v2 terutama digunakan untuk mengedit dan menjalankan kueri, memvisualisasikan hasil, dan berbagi pekerjaan Anda dengan tim Anda. Dengan query editor v2, Anda dapat membuat database, skema, tabel, dan fungsi yang ditentukan pengguna (UDF). Dalam panel tampilan pohon, untuk setiap database Anda, Anda dapat melihat skema. Untuk setiap skema, Anda dapat melihat tabel, tampilan, UDF, dan prosedur tersimpan.

Topik

- [Membuka editor kueri v2](#)
- [Menghubungkan ke database Amazon Redshift](#)
- [Menjelajahi database Amazon Redshift](#)
- [Membuat objek database](#)
- [Melihat kueri dan riwayat tab](#)
- [Pertimbangan saat bekerja dengan editor kueri v2](#)

- [Mengubah pengaturan akun](#)

Membuka editor kueri v2

Untuk membuka editor kueri v2

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dari menu navigator, pilih Editor, lalu Query editor V2. Editor kueri v2 terbuka di tab browser baru.

Halaman editor kueri memiliki menu navigator tempat Anda memilih tampilan sebagai berikut:

Penyunting



Anda mengelola dan menanyakan data Anda diatur sebagai tabel dan terkandung dalam database. Basis data dapat berisi data yang disimpan atau berisi referensi ke data yang disimpan di tempat lain, seperti Amazon S3. Anda terhubung ke database yang terdapat dalam kluster atau grup kerja tanpa server.

Saat bekerja di tampilan Editor, Anda memiliki kontrol berikut:

- Bidang Cluster atau Workgroup menampilkan nama yang saat ini Anda sambungkan. Bidang Database menampilkan database dalam cluster atau workgroup. Tindakan yang Anda lakukan dalam tampilan Database default untuk bertindak pada database yang telah Anda pilih.
- Tampilan hierarkis tampilan pohon dari cluster atau kelompok kerja, database, dan skema Anda. Di bawah skema, Anda dapat bekerja dengan tabel, tampilan, fungsi, dan prosedur tersimpan. Setiap objek dalam tampilan pohon mendukung menu konteks untuk melakukan tindakan terkait, seperti Refresh atau Drop, untuk objek.
- Tindakan



Buat untuk membuat database, skema, tabel, dan fungsi.

- Tindakan



Muat data untuk memuat data dari Amazon S3 atau dari file lokal ke database Anda.

- Ikon



Simpan untuk menyimpan kueri Anda.

- Ikon



Pintasan untuk menampilkan pintasan keyboard untuk editor.

- Ikon



Lainnya untuk menampilkan lebih banyak tindakan di editor. Seperti:

- Bagikan dengan tim saya untuk membagikan kueri atau buku catatan dengan tim Anda. Untuk informasi selengkapnya, lihat [Berkolaborasi dan berbagi sebagai sebuah tim](#).
- Pintasan untuk menampilkan pintasan keyboard untuk editor.
- Riwayat tab untuk menampilkan riwayat tab tab di editor.
- Segarkan pelengkapan otomatis untuk menyegarkan saran yang ditampilkan saat membuat SQL.

- Area



Editor tempat Anda dapat memasukkan dan menjalankan kueri Anda.

Setelah Anda menjalankan kueri, tab Hasil muncul dengan hasil. Di sinilah Anda dapat mengaktifkan Bagan untuk memvisualisasikan hasil Anda. Anda juga dapat mengekspor hasil Anda.

- Area



Notebook tempat Anda dapat menambahkan bagian untuk masuk dan menjalankan SQL atau menambahkan Markdown.

Setelah Anda menjalankan kueri, tab Hasil muncul dengan hasil. Di sinilah Anda dapat Mengekspor hasil Anda.

Pertanyaan



Kueri berisi perintah SQL untuk mengelola dan menanyakan data Anda dalam database. Saat Anda menggunakan editor kueri v2 untuk memuat data sampel, itu juga membuat dan menyimpan kueri sampel untuk Anda.

Ketika Anda memilih kueri yang disimpan, Anda dapat membuka, mengganti nama, dan menghapusnya menggunakan menu konteks (klik kanan). Anda dapat melihat atribut seperti ARN Kueri dari kueri yang disimpan dengan memilih Detail kueri. Anda juga dapat melihat riwayat versinya, mengedit tag yang dilampirkan ke kueri, dan membagikannya dengan tim Anda.

Notebook



Notebook SQL berisi sel SQL dan Markdown. Gunakan buku catatan untuk mengatur, membubuhi keterangan, dan berbagi beberapa perintah SQL dalam satu dokumen.

Ketika Anda memilih buku catatan yang disimpan, Anda dapat membuka, mengganti nama, menggandakan, dan menghapusnya menggunakan menu konteks (klik kanan). Anda dapat melihat atribut seperti ARN Notebook buku catatan yang disimpan dengan memilih detail Notebook. Anda juga dapat melihat riwayat versinya, mengedit tag yang dilampirkan ke buku catatan, mengeksportnya, dan membagikannya dengan tim Anda. Untuk informasi selengkapnya, lihat [Menulis dan menjalankan notebook](#).

Grafik



Bagan adalah representasi visual dari data Anda. Editor kueri v2 menyediakan alat untuk membuat banyak jenis bagan dan menyimpannya.

Saat Anda memilih bagan yang disimpan, Anda dapat membuka, mengganti nama, dan menghapusnya menggunakan menu konteks (klik kanan). Anda dapat melihat atribut seperti Bagan ARN dari bagan yang disimpan dengan memilih Detail bagan. Anda juga dapat mengedit tag yang dilampirkan pada bagan dan mengeksportnya. Untuk informasi selengkapnya, lihat [Memvisualisasikan hasil kueri](#).

Sejarah



Riwayat kueri adalah daftar kueri yang Anda jalankan menggunakan editor kueri Amazon Redshift v2. Kueri ini berjalan sebagai kueri individual atau sebagai bagian dari notebook SQL. Untuk informasi selengkapnya, lihat [Melihat kueri dan riwayat tab](#).

Pertanyaan terjadwal



Kueri terjadwal adalah kueri yang diatur untuk memulai pada waktu tertentu.

Semua tampilan editor kueri v2 memiliki ikon berikut:

- Ikon mode



Visual untuk beralih antara mode terang dan mode gelap.

- Ikon



Pengaturan untuk menampilkan menu layar pengaturan yang berbeda.

- Ikon preferensi



Editor untuk mengedit preferensi Anda saat Anda menggunakan editor kueri v2. Di sini Anda dapat Mengedit pengaturan ruang kerja untuk mengubah ukuran font, ukuran tab, dan pengaturan tampilan lainnya. Anda juga dapat mengaktifkan (atau menonaktifkan) Pelengkapan Otomatis untuk menampilkan saran saat Anda memasukkan SQL Anda.

- Ikon



Connections untuk melihat koneksi yang digunakan oleh tab editor Anda.

Koneksi digunakan untuk mengambil data dari database. Koneksi dibuat untuk database tertentu. Dengan koneksi terisolasi, hasil perintah SQL yang mengubah database, seperti membuat tabel sementara, dalam satu tab editor, tidak terlihat di tab editor lain. Saat Anda

membuka tab editor di editor kueri v2, defaultnya adalah koneksi terisolasi. Saat Anda membuat koneksi bersama, yaitu mematikan sakelar sesi terisolasi, maka hasil koneksi bersama lainnya ke database yang sama akan terlihat satu sama lain. Namun, tab editor yang menggunakan koneksi bersama ke database tidak berjalan secara paralel. Pertanyaan yang menggunakan koneksi yang sama harus menunggu hingga koneksi tersedia. Koneksi ke satu database tidak dapat dibagikan dengan database lain, dan dengan demikian hasil SQL tidak terlihat di seluruh koneksi database yang berbeda.

Jumlah koneksi yang dapat diaktifkan oleh pengguna di akun dikendalikan oleh administrator editor kueri v2.

- Ikon Pengaturan



akun yang digunakan oleh administrator untuk mengubah pengaturan tertentu dari semua pengguna di akun. Untuk informasi selengkapnya, lihat [Mengubah pengaturan akun](#).

Menghubungkan ke database Amazon Redshift

Untuk menyambung ke database, pilih nama cluster atau workgroup di panel tampilan pohon. Jika diminta, masukkan parameter koneksi.

Ketika Anda terhubung ke cluster atau workgroup dan database-nya, Anda biasanya memberikan nama Database. Anda juga menyediakan parameter yang diperlukan untuk salah satu metode otentikasi berikut:

Pusat Identitas IAM

Dengan metode ini, sambungkan ke gudang data Amazon Redshift Anda dengan kredensi masuk tunggal Anda dari penyedia identitas (iDP) Anda. Cluster atau workgroup Anda harus diaktifkan untuk IAM Identity Center di konsol Amazon Redshift. Untuk bantuan menyiapkan koneksi ke Pusat Identitas IAM, lihat [Hubungkan Redshift dengan IAM Identity Center untuk memberi pengguna pengalaman masuk tunggal](#).

Pengguna federasi

Dengan metode ini, tag utama peran IAM atau pengguna Anda harus memberikan detail koneksi. Anda mengonfigurasi tag ini di AWS Identity and Access Management atau penyedia identitas Anda (iDP). Editor kueri v2 bergantung pada tag berikut.

- `RedshiftDbUserTag` ini mendefinisikan pengguna database yang digunakan oleh query editor v2. Tag ini diperlukan.

- `RedshiftDbGroups`— Tag ini mendefinisikan grup database yang bergabung saat menghubungkan ke editor kueri v2. Tag ini opsional dan nilainya harus berupa daftar yang dipisahkan titik dua seperti. `group1:group2:group3` Nilai kosong diabaikan, yaitu, `group1:::group2` ditafsirkan sebagai `group1:group2`.

Tag ini diteruskan ke `redshift:GetClusterCredentials` API untuk mendapatkan kredensial untuk klaster Anda. Untuk informasi selengkapnya, lihat [Menyiapkan tag utama untuk menghubungkan cluster atau workgroup dari editor kueri v2](#).

Kredensi sementara menggunakan nama pengguna database

Opsi ini hanya tersedia saat menghubungkan ke cluster. Dengan metode ini, query editor v2, memberikan nama pengguna untuk database. Editor kueri v2 menghasilkan kata sandi sementara untuk terhubung ke database sebagai nama pengguna database Anda. Seorang pengguna yang menggunakan metode ini untuk terhubung harus diizinkan izin IAM untuk `redshift:GetClusterCredentials`. Untuk mencegah pengguna menggunakan metode ini, ubah pengguna atau peran IAM mereka untuk menolak izin ini.

Kredensi sementara menggunakan identitas IAM Anda

Opsi ini hanya tersedia saat menghubungkan ke cluster. Dengan metode ini, editor kueri v2 memetakan nama pengguna ke identitas IAM Anda dan menghasilkan kata sandi sementara untuk terhubung ke database sebagai identitas IAM Anda. Seorang pengguna yang menggunakan metode ini untuk terhubung harus diizinkan izin IAM untuk `redshift:GetClusterCredentialsWithIAM`. Untuk mencegah pengguna menggunakan metode ini, ubah pengguna atau peran IAM mereka untuk menolak izin ini.

Nama pengguna dan kata sandi basis data

Dengan metode ini, berikan juga nama Pengguna dan Kata Sandi untuk database yang Anda sambungkan. Editor kueri v2 membuat rahasia atas nama Anda yang disimpan di AWS Secrets Manager. Rahasia ini berisi kredensial untuk terhubung ke database Anda.

AWS Secrets Manager

Dengan metode ini, alih-alih nama database, Anda memberikan Rahasia yang disimpan di Secrets Manager yang berisi database dan kredensi login Anda. Untuk informasi tentang membuat rahasia, lihat [Membuat rahasia untuk kredensi koneksi database](#).

Ketika Anda memilih klaster atau workgroup dengan editor kueri v2, tergantung pada konteksnya, Anda dapat membuat, mengedit, dan menghapus koneksi menggunakan menu konteks (klik kanan).

Anda dapat melihat atribut seperti ARN Koneksi koneksi dengan memilih Detail koneksi. Anda juga dapat mengedit tag yang dilampirkan ke koneksi.
































Menjelajahi database Amazon Redshift

Dalam database, Anda dapat mengelola skema, tabel, tampilan, fungsi, dan prosedur tersimpan di panel tampilan pohon. Setiap objek dalam tampilan memiliki tindakan yang terkait dengannya dalam menu konteks (klik kanan).

Panel tampilan pohon hierarkis menampilkan objek database. Untuk me-refresh panel tampilan pohon untuk menampilkan objek database yang mungkin telah dibuat setelah tampilan pohon terakhir ditampilkan, pilih ikon.



Buka menu konteks (klik kanan) untuk objek untuk melihat tindakan apa yang dapat Anda lakukan.

- ▼  **redshift-cluster-tickit**
- ▼  dev
- ▼  public
- ▼  Tables 11
-  accommodations
-  category
-  customer_activity
-  date
-  event
-  listing
-  sales
-  sales2
-  users
-  venue
-  zipcode
- ▼  Views 1
-  myevent
- ▼  Functions 2
- fx* f_py_greater(float8,float8)
- fx* f_sql_greater(float8,float8)
- ▼  Stored procedures 1
- fx* test_sp1(int4,varchar)
- >  testschema
- >  testschema2
- ▼  sample_data_dev
- ▼  tickit 
- >  Tables 7
- >  Views 0
- >  Functions 0
- >  Stored procedures 0
- >  tpcds 
- >  testdb

Setelah Anda memilih tabel, Anda dapat melakukan hal berikut:

- Untuk memulai kueri di editor dengan pernyataan SELECT yang menanyakan semua kolom dalam tabel, gunakan Pilih tabel.
- Untuk melihat atribut atau tabel, gunakan Tampilkan definisi tabel. Gunakan ini untuk melihat nama kolom, jenis kolom, pengkodean, kunci distribusi, kunci pengurutan, dan apakah kolom dapat berisi nilai nol. Untuk informasi selengkapnya tentang atribut tabel, lihat [MEMBUAT TABEL](#) di Panduan Pengembang Database Amazon Redshift.
- Untuk menghapus tabel, gunakan Hapus. Anda dapat menggunakan tabel Truncate untuk menghapus semua baris dari tabel atau Drop table untuk menghapus tabel dari database. Untuk informasi selengkapnya, lihat [TRUNCATE](#) dan [DROP TABLE di Panduan](#) Pengembang Database Amazon Redshift.

Pilih skema untuk Refresh atau Drop schema.

Pilih tampilan untuk Tampilkan definisi tampilan atau Tampilan Jatuhkan.

Pilih fungsi untuk Tampilkan definisi fungsi atau fungsi Drop.

Pilih prosedur tersimpan untuk Tampilkan definisi prosedur atau prosedur Drop.

Membuat objek database

Anda dapat membuat objek database, termasuk database, skema, tabel, dan fungsi yang ditentukan pengguna (UDF). Anda harus terhubung ke cluster atau workgroup dan database untuk membuat objek database.

Membuat database

Anda dapat menggunakan query editor v2 untuk membuat database di cluster atau workgroup Anda.

Untuk membuat basis data

Untuk informasi tentang database, lihat [MEMBUAT DATABASE di Panduan Pengembang Database](#) Amazon Redshift.

1. Pilih



Buat, lalu pilih Database.

2. Masukkan nama Database.
3. (Opsional) Pilih Pengguna dan grup, dan pilih pengguna Database.
4. (Opsional) Anda dapat membuat database dari datashare atau file. AWS Glue Data Catalog Untuk informasi lebih lanjut tentang AWS Glue, lihat [Apa itu AWS Glue?](#) di Panduan AWS Glue Pengembang.
 - (Opsional) Pilih Buat menggunakan datashare, dan pilih Pilih datashare. Daftar ini mencakup datashares produsen yang dapat digunakan untuk membuat datashare konsumen di cluster atau workgroup saat ini.
 - (Opsional) Pilih Buat menggunakan AWS Glue Data Catalog, dan pilih database Choose an AWS Glue. Dalam skema katalog Data, masukkan nama yang akan digunakan untuk skema saat mereferensikan data dalam nama tiga bagian (database.schema.table).
5. Pilih Buat basis data.

Database baru ditampilkan di panel tampilan pohon.

Bila Anda memilih langkah opsional untuk menanyakan database yang dibuat dari datashare, sambungkan ke database Amazon Redshift di cluster atau workgroup (misalnya, database default`dev`), dan gunakan notasi tiga bagian (database.schema.table) yang mereferensikan nama database yang Anda buat saat memilih Buat menggunakan datashare. Database datasharing tercantum di tab editor editor kueri v2, tetapi tidak diaktifkan untuk koneksi langsung.

Bila Anda memilih langkah opsional untuk menanyakan database yang dibuat dari AWS Glue Data Catalog, sambungkan ke database Amazon Redshift Anda di cluster atau grup kerja (misalnya, database default`dev`), dan gunakan notasi tiga bagian (database.schema.table) yang mereferensikan nama database yang Anda buat saat Anda memilih Buat menggunakan AWS Glue Data Catalog, skema yang Anda beri nama dalam skema katalog Data, dan tabel di. AWS Glue Data Catalog Mirip dengan:

```
SELECT * FROM glue-database.glue-schema.glue-table
```

Note

Konfirmasikan bahwa Anda terhubung ke database default menggunakan metode koneksi Kredensial sementara menggunakan identitas IAM Anda, dan bahwa kredensial IAM Anda telah diberikan hak penggunaan ke database. AWS Glue

```
GRANT USAGE ON DATABASE glue-database to "IAM:MyIAMUser"
```

AWS Glue Basis data tercantum di tab editor kueri v2 editor, tetapi tidak diaktifkan untuk koneksi langsung.

Untuk informasi selengkapnya tentang kueri AWS Glue Data Catalog, lihat [Bekerja dengan rangkaian data yang dikelola Lake Formation sebagai konsumen dan Bekerja dengan rangkaian data yang dikelola Lake Formation sebagai produsen di Panduan Pengembang Basis Data Amazon Redshift](#).

Contoh membuat database sebagai konsumen datashare

Contoh berikut menjelaskan skenario tertentu yang digunakan untuk membuat database dari datashare menggunakan query editor v2. Tinjau skenario ini untuk mempelajari cara membuat database dari datashare di lingkungan Anda. Skenario ini menggunakan dua cluster, `cluster-base` (cluster produsen) dan `cluster-view` (cluster konsumen).

1. Gunakan konsol Amazon Redshift untuk membuat datashare untuk tabel di cluster. `category2` `cluster-base` Datashare produser diberi nama. `datashare_base`

Untuk informasi tentang membuat rangkaian data, lihat [Berbagi data di seluruh klaster di Amazon Redshift di Panduan Pengembang Database](#) Amazon Redshift.

2. Gunakan konsol Amazon Redshift untuk menerima datashare `datashare_base` sebagai konsumen untuk tabel di cluster. `category2` `cluster-view`
3. Lihat panel tampilan pohon di editor kueri v2 yang menunjukkan hierarki sebagai: `cluster-base`
 - Kluster: `cluster-base`
 - Database: `dev`
 - Skema: `public`
 - Tabel: `category2`

4. Pilih



Buat, lalu pilih Database.

5. Masukkan `see_datashare_base` nama Database.

6. Pilih Buat menggunakan datashare, dan pilih Pilih datashare. Pilih `datashare_base` untuk digunakan sebagai sumber database yang Anda buat.

Panel tampilan pohon di editor kueri v2 menunjukkan hierarki sebagai: `cluster-view`

- Kluster: `cluster-view`
 - Database: `see_datashare_base`
 - Skema: `public`
 - Tabel: `category2`
- 7. Saat Anda menanyakan data, sambungkan ke database default cluster `cluster-view` (biasanya bernama `dev`), tetapi referensi database datashare `see_datashare_base` di SQL Anda.

Note

Dalam tampilan editor editor kueri v2, cluster yang dipilih adalah `cluster-view`. Database yang dipilih adalah `dev`. Database `see_datashare_base` terdaftar tetapi tidak diaktifkan untuk koneksi langsung. Anda memilih `dev` database dan referensi `see_datashare_base` di SQL yang Anda jalankan.

```
SELECT * FROM "see_datashare_base"."public"."category2";
```

Query mengambil data dari datashare `datashare_base` di cluster. `cluster_base`

Contoh membuat database dari AWS Glue Data Catalog

Contoh berikut menjelaskan skenario tertentu yang digunakan untuk membuat database dari AWS Glue Data Catalog menggunakan editor query v2. Tinjau skenario ini untuk mempelajari cara membuat database dari AWS Glue Data Catalog lingkungan Anda. Skenario ini menggunakan satu cluster, `cluster-view` untuk memuat database yang Anda buat.

1. Pilih



Buat, lalu pilih Database.

2. Masukkan `data_catalog_database` nama Database.
3. Pilih Buat menggunakan AWS Glue Data Catalog, dan pilih Pilih AWS Glue database. Pilih `glue_db` untuk digunakan sebagai sumber database yang Anda buat.

Pilih Skema katalog data dan masukkan `myschema` sebagai nama skema yang akan digunakan dalam notasi tiga bagian.

Panel tampilan pohon di editor kueri v2 menunjukkan hierarki sebagai: `cluster-view`

- Kluster: `cluster-view`
 - Database: `data_catalog_database`
 - Skema: `myschema`
 - Tabel: `category3`
- 4. Saat Anda menanyakan data, sambungkan ke database default cluster `cluster-view` (biasanya bernama `dev`), tetapi referensi database `data_catalog_database` di SQL Anda.

Note

Dalam tampilan editor editor kueri v2, cluster yang dipilih adalah `cluster-view`. Database yang dipilih adalah `dev`. Database `data_catalog_database` terdaftar tetapi tidak diaktifkan untuk koneksi langsung. Anda memilih `dev` database dan referensi `data_catalog_database` di SQL yang Anda jalankan.

```
SELECT * FROM "data_catalog_database"."myschema"."category3";
```

Kueri mengambil data yang dikatalogkan oleh. AWS Glue Data Catalog

Membuat skema

Anda dapat menggunakan editor kueri v2 untuk membuat skema di cluster atau grup kerja Anda.

Untuk membuat skema

Untuk informasi tentang skema, lihat [Skema](#) di Panduan Pengembang Database Amazon Redshift.

1. Pilih



Buat, lalu pilih Skema.

2. Masukkan nama Skema.

3. Pilih Lokal atau Eksternal sebagai tipe Skema.

Untuk informasi selengkapnya tentang skema lokal, lihat [MEMBUAT SKEMA di Panduan Pengembang](#) Database Amazon Redshift. Untuk informasi selengkapnya tentang skema eksternal, lihat [MEMBUAT SKEMA EKSTERNAL di Panduan](#) Pengembang Database Amazon Redshift.

4. Jika Anda memilih Eksternal, maka Anda memiliki pilihan skema eksternal berikut.

- Glue Data Catalog — untuk membuat skema eksternal di Amazon Redshift yang mereferensikan tabel. AWS Glue Selain memilih AWS Glue database, pilih peran IAM yang terkait dengan cluster dan peran IAM yang terkait dengan Katalog Data.
- PostgreSQL — untuk membuat skema eksternal di Amazon Redshift yang mereferensikan database Amazon RDS for PostgreSQL atau Amazon Aurora PostgreSQL Edition yang kompatibel. Juga berikan informasi koneksi ke database. Untuk informasi selengkapnya tentang kueri federasi, lihat [Mengkueri data dengan kueri gabungan di Panduan Pengembang](#) Database Amazon Redshift.
- MySQL — untuk membuat skema eksternal di Amazon Redshift yang mereferensikan Amazon RDS untuk MySQL atau database Amazon Aurora MySQL Edisi yang kompatibel. Juga berikan informasi koneksi ke database. Untuk informasi selengkapnya tentang kueri federasi, lihat [Mengkueri data dengan kueri gabungan di Panduan Pengembang](#) Database Amazon Redshift.

5. Pilih Buat skema.

Skema baru muncul di panel tampilan pohon.

Membuat tabel

Anda dapat menggunakan editor kueri v2 untuk membuat tabel di cluster atau workgroup Anda.

Untuk membuat tabel

Anda dapat membuat tabel berdasarkan file nilai dipisahkan koma (CSV) yang Anda tentukan atau tentukan setiap kolom tabel. Untuk informasi tentang tabel, lihat [Merancang tabel](#) dan [MEMBUAT TABEL](#) di Panduan Pengembang Database Amazon Redshift.

Pilih Buka kueri di editor untuk melihat dan mengedit pernyataan CREATE TABLE sebelum Anda menjalankan kueri untuk membuat tabel.

1. Pilih



Buat, dan pilih Tabel.

2. Pilih skema.

3. Masukkan nama tabel.

4. Pilih



Tambahkan bidang untuk menambahkan kolom.

5. Gunakan file CSV sebagai templat untuk definisi tabel:

- a. Pilih Load dari CSV.

- b. Jelajahi lokasi file.

Jika Anda menggunakan file CSV, pastikan baris pertama file berisi judul kolom.

- c. Pilih file dan pilih Buka. Konfirmasikan bahwa nama kolom dan tipe data adalah apa yang Anda inginkan.

6. Untuk setiap kolom, pilih kolom dan pilih opsi yang Anda inginkan:

- Pilih nilai untuk Encoding.
- Pilih nilai Default.
- Aktifkan Kenaikan secara otomatis jika Anda ingin nilai kolom bertambah. Kemudian tentukan nilai untuk benih kenaikan Otomatis dan langkah kenaikan Otomatis.
- Aktifkan Not NULL jika kolom harus selalu berisi nilai.
- Masukkan nilai Ukuran untuk kolom.
- Aktifkan kunci utama jika Anda ingin kolom menjadi kunci utama.
- Aktifkan tombol Unik jika Anda ingin kolom menjadi kunci unik.

7. (Opsional) Pilih detail Tabel dan pilih salah satu opsi berikut:
 - Kolom dan gaya kunci distribusi.
 - Urutkan kolom kunci dan jenis sortir.
 - Aktifkan Backup untuk menyertakan tabel dalam snapshot.
 - Nyalakan Tabel sementara untuk membuat tabel sebagai tabel sementara.
8. Pilih Buka kueri di editor untuk melanjutkan menentukan opsi untuk menentukan tabel atau pilih Buat tabel untuk membuat tabel.

Membuat fungsi

Anda dapat menggunakan query editor v2 untuk membuat fungsi di cluster atau workgroup Anda.

Untuk membuat fungsi

1. Pilih



Create, dan pilih Function.

2. Untuk Type, pilih SQL atau Python.
3. Pilih nilai untuk Skema.
4. Masukkan nilai untuk Nama untuk fungsi tersebut.
5. Masukkan nilai Volatilitas untuk fungsi tersebut.
6. Pilih Parameter berdasarkan tipe datanya sesuai urutan parameter input.
7. Untuk Pengembalian, pilih tipe data.
8. Masukkan program SQL atau kode program Python untuk fungsi tersebut.
9. Pilih Buat.

Untuk informasi selengkapnya tentang fungsi yang ditentukan pengguna (UDF), lihat [Membuat fungsi yang ditentukan pengguna di Panduan Pengembang Database Amazon Redshift](#).

Melihat kueri dan riwayat tab

Anda dapat melihat riwayat kueri Anda dengan editor kueri v2. Hanya kueri yang Anda jalankan menggunakan editor kueri v2 yang muncul di riwayat kueri. Kedua kueri yang dijalankan dari menggunakan tab Editor atau tab Notebook ditampilkan. Anda dapat memfilter daftar yang

ditampilkan berdasarkan periode waktu, seperti `This week`, di mana seminggu didefinisikan sebagai Senin-Minggu. Daftar kueri mengambil 25 baris kueri yang cocok dengan filter Anda sekaligus. Pilih Muat lebih banyak untuk melihat set berikutnya. Pilih kueri dan dari menu Tindakan. Tindakan yang tersedia tergantung pada apakah kueri yang dipilih telah disimpan. Anda dapat memilih operasi berikut:

- Lihat detail kueri - Menampilkan halaman detail kueri dengan informasi lebih lanjut tentang kueri yang dijalankan.
- Buka kueri di tab baru — Membuka tab editor baru dan memasangnya dengan kueri yang dipilih. Jika masih terhubung, cluster atau workgroup dan database dipilih secara otomatis. Untuk menjalankan kueri, pertama-tama konfirmasi bahwa cluster atau workgroup dan database yang benar dipilih.
- Tab sumber terbuka — Jika masih terbuka, navigasikan ke tab editor atau buku catatan yang berisi kueri saat dijalankan. Isi editor atau buku catatan mungkin telah berubah setelah kueri dijalankan.
- Buka kueri tersimpan — Menavigasi ke tab editor atau buku catatan dan membuka kueri.

Anda juga dapat melihat riwayat kueri yang dijalankan di tab Editor atau riwayat kueri yang dijalankan di tab Notebook. Untuk melihat riwayat kueri di tab, pilih Riwayat tab. Dalam riwayat tab, Anda dapat melakukan operasi berikut:

- Salin kueri - Menyalin konten SQL versi kueri ke clipboard.
- Buka kueri di tab baru — Membuka tab editor baru dan memasangnya dengan kueri yang dipilih. Untuk menjalankan query, Anda harus memilih cluster atau workgroup dan database.
- Lihat detail kueri - Menampilkan halaman detail kueri dengan informasi lebih lanjut tentang kueri yang dijalankan.

Pertimbangan saat bekerja dengan editor kueri v2

Pertimbangkan hal berikut saat bekerja dengan editor kueri v2.

- Ukuran hasil kueri maksimum adalah yang lebih kecil dari 5 MB atau 100.000 baris.
- Anda dapat menjalankan kueri hingga 300.000 karakter.
- Anda dapat menyimpan kueri hingga 30.000 karakter.
- Secara default, editor kueri v2 secara otomatis melakukan setiap perintah SQL individual yang berjalan. Ketika pernyataan `BEGIN` disediakan, pernyataan dalam blok `BEGIN-COMMIT` atau

BEGIN-ROLLBACK dijalankan sebagai satu transaksi. Untuk informasi selengkapnya tentang transaksi, lihat [MULAI](#) di Panduan Pengembang Database Amazon Redshift.

- Jumlah maksimum peringatan yang ditampilkan oleh editor kueri v2 saat menjalankan pernyataan SQL adalah 10. Misalnya, ketika prosedur tersimpan dijalankan, tidak lebih dari 10 pernyataan RAISE ditampilkan.
- Editor kueri v2 tidak mendukung IAM RoleSessionName yang berisi koma (.). Anda mungkin melihat kesalahan yang mirip dengan berikut ini: Pesan Kesalahan: “aroa123456789Example:MyText, yourtext' bukan nilai yang valid untuk TagValue - ini berisi karakter ilegal” Masalah ini muncul saat Anda mendefinisikan IAM yang menyertakan koma dan kemudian menggunakan editor kueri v2 dengan peran IAM RoleSessionName tersebut.

Untuk informasi selengkapnya tentang IAMRoleSessionName, lihat [atribut RoleSessionName SAMP](#) di Panduan Pengguna IAM.

Mengubah pengaturan akun

Pengguna dengan izin IAM yang tepat dapat melihat dan mengubah pengaturan Akun untuk pengguna lain dalam hal yang sama. Akun AWS Administrator ini dapat melihat atau mengatur hal-hal berikut:

- Koneksi database bersamaan maksimum per pengguna di akun. Ini termasuk koneksi untuk sesi Terisolasi. Saat Anda mengubah nilai ini, perlu waktu 10 menit agar perubahan diterapkan.
- Izinkan pengguna di akun untuk mengekspor seluruh hasil yang ditetapkan dari perintah SQL ke file.
- Muat dan tampilkan database sampel dengan beberapa kueri tersimpan terkait.
- Tentukan jalur Amazon S3 yang digunakan oleh pengguna akun untuk memuat data dari file lokal.
- Lihat ARN kunci KMS yang digunakan untuk mengenkripsi sumber daya editor kueri v2.

Berinteraksi dengan editor kueri v2 generatif SQL (pratinjau)

Ini adalah dokumentasi prarilis untuk query editor v2 generatif SQL, yang dalam rilis pratinjau. Dokumentasi dan fitur dapat berubah. Sebaiknya gunakan fitur ini hanya dalam lingkungan pengujian, bukan dalam lingkungan produksi. Untuk syarat dan ketentuan pratinjau, lihat Partisipasi Layanan Beta dalam [Ketentuan AWS Layanan](#).

Note

Saat ini, dukungan SQL generatif hanya tersedia dalam hal berikut: Wilayah AWS

- Wilayah AS Timur (Virginia N.) (us-east-1)
- Wilayah AS Barat (Oregon) (us-west-2)
- Wilayah Eropa (Frankfurt) (eu-central-1)

Anda dapat berinteraksi dengan kemampuan SQL generatif Amazon Q di editor kueri Amazon Redshift v2. Ini adalah asisten pengkodean yang menghasilkan pernyataan SQL berdasarkan prompt dan skema database Anda. Asisten pengkodean ini tersedia saat Anda membuat buku catatan di editor kueri v2.

Saat berinteraksi dengan SQL generatif, ajukan pertanyaan spesifik, ulangi ketika Anda memiliki permintaan yang kompleks, dan verifikasi jawaban untuk akurasi.

Saat memberikan permintaan analisis dalam bahasa alami, sespesifik mungkin untuk membantu asisten pengkodean memahami dengan tepat apa yang Anda butuhkan. Alih-alih bertanya “temukan tempat teratas yang menjual tiket terbanyak,” berikan detail lebih lanjut seperti “temukan nama/id dari tiga tempat teratas yang menjual tiket terbanyak pada tahun 2008.” Gunakan nama objek yang konsisten dalam database Anda, seperti skema, tabel, dan nama kolom seperti yang didefinisikan dalam database Anda alih-alih merujuk ke objek yang sama dengan cara yang berbeda, yang dapat membingungkan asisten.

Memecah permintaan kompleks menjadi beberapa pernyataan sederhana yang lebih mudah bagi asisten untuk menafsirkan. Ajukan pertanyaan tindak lanjut secara berulang untuk mendapatkan analisis yang lebih rinci dari asisten. Misalnya, tanyakan dulu “negara bagian mana yang memiliki tempat paling banyak?” Kemudian berdasarkan tanggapan, tanyakan “tempat mana yang paling populer dari negara bagian ini?”.

Tinjau SQL yang dihasilkan sebelum menjalankannya untuk memastikan akurasi. Jika kueri SQL yang dihasilkan memiliki kesalahan atau tidak cocok dengan maksud Anda, berikan instruksi kepada asisten tentang cara memperbaikinya alih-alih mengulangi seluruh permintaan. Misalnya, jika kueri tidak memiliki klausa predikat pada tahun, tanyakan “Sediakan tempat dari tahun 2008.”

Pertimbangan saat berinteraksi dengan SQL generatif

Pertimbangkan hal berikut saat bekerja di panel obrolan.

- Administrator editor kueri v2 untuk akun Anda harus mengaktifkan kemampuan obrolan di halaman pengaturan SQL Generatif.
- Untuk menggunakan SQL generatif editor kueri v2, Anda memerlukan izin `sqlworkbench:GetQSQLRecommendations` dalam kebijakan IAM Anda, selain izin lain yang ditentukan dalam kebijakan AWS terkelola untuk editor kueri v2. Untuk informasi selengkapnya tentang kebijakan AWS terkelola, lihat [Mengakses editor kueri v2](#).
- Pertanyaan Anda harus ditulis dalam bahasa Inggris.
- Pertanyaan Anda harus mengacu pada database yang terhubung di cluster atau workgroup Anda. Untuk menghindari kesalahan status kosong, harus ada setidaknya satu tabel dan beberapa data dalam database.
- Pertanyaan Anda harus mengacu pada data yang disimpan dalam database yang terhubung. Itu tidak dapat merujuk skema eksternal. Untuk informasi selengkapnya tentang skema yang didukung, lihat [Membuat skema](#) di Panduan Pengembang Database Amazon Redshift.
- Setiap pertanyaan yang menghasilkan SQL yang mengubah database yang terhubung dapat menghasilkan peringatan.
- Teknologi AI generatif adalah hal baru dan mungkin ada kesalahan, kadang-kadang disebut halusinasi, dalam tanggapannya. Uji dan tinjau semua kode untuk kesalahan dan kerentanan sebelum menggunakannya di lingkungan atau beban kerja Anda.
- Anda dapat meningkatkan rekomendasi dengan membagikan kueri SQL yang dijalankan oleh pengguna lain di akun Anda. Administrator akun Anda dapat menjalankan perintah SQL berikut untuk memungkinkan akses ke riwayat kueri akun.

```
GRANT ROLE SYS:MONITOR to "IAMR:role-name";  
GRANT ROLE SYS:MONITOR to "IAM:user-name";  
GRANT ROLE SYS:MONITOR to "database-username";
```

Untuk informasi selengkapnya `SYS:MONITOR`, lihat [peran yang ditentukan sistem Amazon Redshift di Panduan](#) Pengembang Database Amazon Redshift.

- Data Anda aman dan pribadi. Data Anda tidak dibagikan di seluruh akun. Kueri, data, dan skema basis data Anda tidak digunakan untuk melatih model fondasi AI generatif (FM). Masukan Anda digunakan sebagai petunjuk kontekstual ke FM untuk menjawab hanya pertanyaan Anda.

Menggunakan SQL generatif

Setelah izin yang benar dikonfigurasi, saat bekerja dengan buku catatan di editor kueri v2, Anda dapat memilih ikon untuk memulai percakapan.

Untuk berinteraksi dengan editor kueri v2 obrolan SQL generatif untuk menghasilkan SQL

1. Di tab Editor dari editor kueri v2, buka buku catatan.
2. Pilih ikon



Generative SQL, lalu ikuti petunjuk untuk mengajukan pertanyaan Anda tentang SQL generatif Amazon Redshift editor v2 generatif di panel obrolan.

Anda memberikan pertanyaan di bidang prompt dan editor kueri v2 merespons dengan SQL yang disarankan. Setiap kesalahan yang ditemui dikembalikan kepada Anda di panel obrolan.

3. Pilih Tambahkan ke buku catatan untuk menambahkan sel Markdown dengan prompt Anda dan sel SQL dengan SQL yang disarankan ke buku catatan Anda.
4. (Opsional) Pilih Regenerate SQL untuk menghasilkan respons lain untuk prompt yang sama. Anda dapat memilih untuk Regenerasi SQL satu kali untuk prompt saat ini.
5. (Opsional) Di panel obrolan SQL generatif, pilih ikon



Lainnya, lalu pilih Refresh database untuk menyegarkan metadata yang menjelaskan database Anda yang terhubung. Metadata ini mencakup definisi skema, tabel, dan kolom dalam database Anda.

Memperbarui pengaturan SQL generatif sebagai administrator

Seorang pengguna dengan izin IAM yang tepat dapat melihat dan mengubah pengaturan SQL Generatif untuk pengguna lain dalam hal yang sama. Akun AWS Administrator ini harus memiliki izin `sqlworkbench:UpdateAccountQSQLSettings` dalam kebijakan IAM mereka, selain izin lain yang ditentukan dalam kebijakan AWS terkelola untuk editor kueri v2. Untuk informasi selengkapnya tentang kebijakan terkelola, lihat [Izin yang diperlukan untuk menggunakan editor kueri v2](#).

Agar administrator mengaktifkan obrolan SQL generatif untuk semua pengguna di akun

1. Pilih ikon



Pengaturan untuk menampilkan menu layar pengaturan yang berbeda.

2. Kemudian pilih ikon



Generative SQL settings untuk menampilkan halaman Generative SQL settings.

3. Pilih Generative SQL untuk mengaktifkan kemampuan SQL generatif bagi pengguna di akun.

Contoh menggunakan kemampuan SQL generatif Amazon Q dengan data TICKIT

Untuk membuat prompt yang efisien untuk menghasilkan SQL, Anda harus belajar tentang skema database dan data Anda. Data TICKIT terdiri dari tujuh tabel: dua tabel fakta dan lima dimensi. Data sampel berisi catatan tentang penjualan kepada petugas acara hiburan yang terjadi pada tahun 2008. Untuk informasi selengkapnya tentang skema data TICKIT, lihat [Contoh database](#) di Panduan Pengembang Database Amazon Redshift. Anda dapat memuat data TICKIT ke dalam database dengan berbagai metode di konsol Amazon Redshift dan editor kueri v2. Query editor v2 menyediakan metode untuk memuat data TICKIT ke dalam `databasesample_data_dev`. Untuk informasi, lihat [Memuat data sampel](#). Editor kueri v2 juga menyediakan contoh prompt untuk data TICKIT. Skenario berikut menjelaskan percakapan dengan SQL generatif untuk menghasilkan SQL tentang data sampel TICKIT. Dalam skenario ini, data sampel TICKIT sudah dibuat dalam dev database di cluster Amazon Redshift.

Note

Contoh ini adalah untuk menggambarkan percakapan. Respons dari SQL generatif mungkin tidak cocok dengan hasil Anda menggunakan prompt yang sama.

Contoh percakapan dengan editor kueri v2 generatif SQL

1. Di Editor, sambungkan ke cluster atau workgroup yang berisi data sampel TICKIT.

2. Buat buku catatan kosong dan pilih ikon



Generative SQL untuk membuka panel obrolan.

3. Masukkan prompt berikut untuk menghasilkan SQL untuk memverifikasi jumlah catatan dalam VENUE tabel:

```
How many venues are there?
```

```
SELECT
  COUNT(*) AS num_venues
FROM
  tickit.venue
```

Pilih Tambahkan ke buku catatan untuk menambahkan dua sel ke buku catatan yang terbuka. Satu sel Markdown “Ada berapa tempat?” dan satu berisi SQL yang dihasilkan.

Di sel SQL, pilih Jalankan untuk menerima hasilnya:

```
count
-----
202
```

4. Untuk meminta versi SQL lain, pilih Regenerate SQL dan terima jawaban berikut:

```
SELECT
  venuestate,
  COUNT(*) AS num_venues
FROM
  tickit.venue
GROUP BY
  venuestate
```

Pilih Tambahkan ke buku catatan untuk menambahkan dua sel lagi ke buku catatan yang terbuka. Satu sel Markdown “Ada berapa tempat?” dan satu berisi SQL yang dihasilkan.

Di sel SQL, pilih Jalankan untuk menerima status tempat daftar hasil berdasarkan nomor:

```

venuestate num_venues
-----
MA          4
OH          8
MI          5
...

```

5. Asisten SQL generatif dapat membuat asumsi tentang apa yang Anda tanyakan. Meskipun tidak ada widget dalam database, Anda masih bisa bertanya. Dalam hal ini, ini memberi Anda pesan bahwa itu tidak dapat menghasilkan SQL.

How many widgets are there?

I was not able to generate any SQL

6. Saat Anda mempelajari lebih lanjut tentang database Anda, Anda dapat mengajukan pertanyaan yang lebih spesifik untuk menghasilkan SQL. Misalnya, Anda menyadari bahwa database berisi data penjualan selama beberapa bulan di tahun 2008. Masukkan prompt berikut untuk menghasilkan SQL untuk menemukan jumlah penjualan pada bulan November 2008:

How many sales were there in November 2008?

```

SELECT
  COUNT(*) AS num_sales
FROM
  tickit.sales s
  JOIN tickit.date d ON s.dateid = d.dateid
WHERE
  d.month = 'November'
  AND d.year = 2008

```

Pilih Tambahkan ke buku catatan untuk menambahkan dua sel ke buku catatan yang terbuka. Satu sel penurunan harga “Berapa banyak penjualan yang ada pada November 2008?” dan satu berisi SQL yang dihasilkan.

Di sel SQL, pilih Jalankan untuk menerima hasilnya:

num_sales

```
-----
0
```

Anda menyadari ini bukan hasil yang Anda harapkan.

- Anda melihat bahwa predikat `date.month = 'November'` mengharapakan bulan dalam tabel `DATE` diwakili oleh singkatan dari nama bulan. Anda mengubah predikat ke `d.month = 'NOV'` dan menjalankan kembali SQL.

```
SELECT
  COUNT(*)
FROM
  sales
  JOIN date ON sales.dateid = date.dateid
WHERE
  date.month = 'NOV'
  AND date.year = 2008
```

Di sel SQL, pilih Jalankan untuk mendapatkan hasil baru.

```
count
-----
14261
```

- Jika Anda mengajukan pertanyaan yang mencoba mengubah database yang terhubung, pesan peringatan dikembalikan bersama dengan SQL yang direkomendasikan. Masukkan prompt berikut untuk menghasilkan SQL untuk memasukkan data ke dalam tabel:

```
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.

Jika Anda memilih Tambahkan ke notebook untuk menambahkan dua sel ke notebook yang terbuka dan menjalankan SQL, maka SQL gagal.

```
ERROR: syntax error at or near "," Position: 132 [ErrorId:
1-6546764a-011df2691778846219ce6ec2]
```

Skenario ini hanya menggambarkan beberapa cara dasar untuk berinteraksi dengan query editor v2 generatif SQL. Anda dapat bereksperimen lebih banyak lagi dengan teknologi AI generatif ini untuk membantu Anda mulai membuat SQL untuk menanyakan database Anda.

Memuat data ke dalam database

Anda dapat menggunakan editor kueri v2 untuk memuat data ke dalam database di kluster atau grup kerja Amazon Redshift.

Memuat data sampel

Editor kueri v2 dilengkapi dengan data sampel dan buku catatan yang tersedia untuk dimuat ke dalam database sampel dan skema yang sesuai.

Untuk memuat data sampel, pilih



ikon yang terkait dengan data sampel yang ingin Anda muat. Editor kueri v2 kemudian memuat data ke dalam skema dalam database **sample_data_dev** dan membuat folder buku catatan yang disimpan di folder Notebook Anda.

Kumpulan data sampel berikut tersedia.

ticket

Sebagian besar contoh dalam dokumentasi Amazon Redshift menggunakan data sampel yang disebut. **ticket** Data ini terdiri dari tujuh tabel: dua tabel fakta dan lima dimensi. Saat Anda memuat data ini, skema **ticket** diperbarui dengan data sampel. Untuk informasi selengkapnya

tentang ticket data, lihat [Contoh database](#) di Panduan Pengembang Database Amazon Redshift.

tpch

Data ini digunakan untuk tolok ukur dukungan keputusan. Saat Anda memuat data ini, skema tpch diperbarui dengan data sampel. Untuk informasi lebih lanjut tentang tpch data, lihat [TPC-H](#).

tpcds

Data ini digunakan untuk tolok ukur dukungan keputusan. Saat Anda memuat data ini, skema tpcds diperbarui dengan data sampel. Untuk informasi lebih lanjut tentang tpcds data, lihat [TPC-DS](#).

Memuat data dari Amazon S3

Anda dapat memuat data Amazon S3 ke tabel yang sudah ada atau yang baru.

Untuk memuat data ke dalam tabel yang ada

Perintah COPY digunakan oleh editor kueri v2 untuk memuat data dari Amazon S3. Perintah COPY yang dihasilkan dan digunakan dalam wizard memuat data editor kueri v2 mendukung banyak parameter yang tersedia untuk sintaks perintah COPY untuk disalin dari Amazon S3. Untuk informasi tentang perintah COPY dan opsinya yang digunakan untuk memuat data dari Amazon S3, lihat [COPY dari Amazon Simple Storage Service](#) di Panduan Pengembang Database Amazon Redshift.

1. Konfirmasikan bahwa tabel sudah dibuat di database tempat Anda ingin memuat data.
2. Konfirmasikan bahwa Anda terhubung ke database target di panel tampilan pohon editor kueri v2 sebelum melanjutkan. Anda dapat membuat koneksi menggunakan menu konteks (klik kanan) ke cluster atau workgroup tempat data akan dimuat.

Pilih



Muat data.

3. Untuk sumber Data, pilih Muat dari bucket S3.
4. Di URI S3, pilih Browse S3 untuk mencari bucket Amazon S3 yang berisi data yang akan dimuat.
5. Jika bucket Amazon S3 yang ditentukan tidak Wilayah AWS sama dengan tabel target, pilih lokasi file S3 untuk lokasi data tersebut Wilayah AWS berada.

6. Pilih File ini adalah file manifes jika file Amazon S3 sebenarnya adalah manifes yang berisi beberapa URI bucket Amazon S3.
7. Pilih format File untuk file yang akan diunggah. Format data yang didukung adalah CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET, dan ORC. Tergantung pada format file yang ditentukan, Anda dapat memilih opsi File masing-masing. Anda juga dapat memilih Data dienkripsi jika data dienkripsi dan masukkan Nama Sumber Daya Amazon (ARN) dari kunci KMS yang digunakan untuk mengenkripsi data.

Jika Anda memilih CSV atau DELIMITER, Anda juga dapat memilih karakter Delimiter dan apakah akan Abaikan baris header jika jumlah baris yang ditentukan sebenarnya adalah nama kolom dan bukan data yang akan dimuat.

8. Pilih metode kompresi untuk mengompres file Anda. Defaultnya adalah tidak ada kompresi.
9. (Opsional) Pengaturan lanjutan mendukung berbagai parameter konversi Data dan operasi Beban. Masukkan informasi ini sesuai kebutuhan untuk file Anda.

Untuk informasi selengkapnya tentang konversi data dan parameter pemuatan data, lihat [Parameter konversi data](#) dan [Operasi pemuatan data](#) di Panduan Pengembang Database Amazon Redshift.

10. Pilih Selanjutnya.
11. Pilih Muat tabel yang ada.
12. Konfirmasikan atau pilih lokasi tabel Target termasuk Cluster atau kelompok kerja, Database, Skema, dan nama Tabel tempat data dimuat.
13. Pilih peran IAM yang memiliki izin yang diperlukan untuk memuat data dari Amazon S3.
14. (Opsional) Pilih nama kolom untuk memasukkannya Pemetaan kolom untuk memetakan kolom dalam urutan file data input.
15. Pilih Muat data untuk memulai pemuatan data.

Saat beban selesai, editor kueri ditampilkan dengan perintah COPY yang dihasilkan yang digunakan untuk memuat data Anda. Hasil COPY ditampilkan. Jika berhasil, Anda sekarang dapat menggunakan SQL untuk memilih data dari tabel yang dimuat. Ketika ada kesalahan, kueri tampilan sistem STL_LOAD_ERRORS untuk mendapatkan detail lebih lanjut. Untuk informasi tentang kesalahan perintah COPY, lihat [STL_LOAD_ERRORS di Panduan Pengembang Database](#) Amazon Redshift.

Saat Anda memuat data ke dalam tabel baru, editor kueri v2 pertama-tama membuat tabel di database, lalu memuat data sebagai tindakan terpisah dalam alur kerja yang sama.

Untuk memuat data ke dalam tabel baru

Perintah COPY digunakan oleh editor kueri v2 untuk memuat data dari Amazon S3. Perintah COPY yang dihasilkan dan digunakan dalam wizard memuat data editor kueri v2 mendukung banyak parameter yang tersedia untuk sintaks perintah COPY untuk disalin dari Amazon S3. Untuk informasi tentang perintah COPY dan opsinya yang digunakan untuk memuat data dari Amazon S3, lihat [COPY dari Amazon Simple Storage Service](#) di Panduan Pengembang Database Amazon Redshift.

1. Konfirmasikan bahwa Anda terhubung ke database target di panel tampilan pohon editor kueri v2 sebelum melanjutkan. Anda dapat membuat koneksi menggunakan menu konteks (klik kanan) ke cluster atau workgroup tempat data akan dimuat.

Pilih



Muat data.

2. Untuk sumber Data, pilih Muat dari bucket S3.
3. Di URI S3, pilih Browse S3 untuk mencari bucket Amazon S3 yang berisi data yang akan dimuat.
4. Jika bucket Amazon S3 yang ditentukan tidak Wilayah AWS sama dengan tabel target, pilih lokasi file S3 untuk lokasi data tersebut Wilayah AWS berada.
5. Pilih File ini adalah file manifes jika file Amazon S3 sebenarnya adalah manifes yang berisi beberapa URI bucket Amazon S3.
6. Pilih format File untuk file yang akan diunggah. Format data yang didukung adalah CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET, dan ORC. Tergantung pada format file yang ditentukan, Anda dapat memilih opsi File masing-masing. Anda juga dapat memilih Data dienkripsi jika data dienkripsi dan masukkan Nama Sumber Daya Amazon (ARN) dari kunci KMS yang digunakan untuk mengenkripsi data.

Jika Anda memilih CSV atau DELIMITER, Anda juga dapat memilih karakter Delimiter dan apakah akan Abaikan baris header jika jumlah baris yang ditentukan sebenarnya adalah nama kolom dan bukan data yang akan dimuat.

7. Pilih metode kompresi untuk mengompres file Anda. Defaultnya adalah tidak ada kompresi.
8. (Opsional) Pengaturan lanjutan mendukung berbagai parameter konversi Data dan operasi Beban. Masukkan informasi ini sesuai kebutuhan untuk file Anda.

Untuk informasi selengkapnya tentang konversi data dan parameter pemuatan data, lihat [Parameter konversi data](#) dan [Operasi pemuatan data](#) di Panduan Pengembang Database Amazon Redshift.

9. Pilih Selanjutnya.
10. Pilih Muat tabel baru.

Kolom tabel disimpulkan dari data input. Anda dapat memodifikasi definisi skema tabel dengan menambahkan kolom dan detail tabel. Untuk kembali ke skema tabel yang disimpulkan editor kueri v2, pilih Pulihkan ke default.

11. Konfirmasikan atau pilih lokasi tabel Target termasuk Cluster atau workgroup, Database, dan Skema tempat data dimuat. Masukkan nama Tabel yang akan dibuat.
12. Pilih peran IAM yang memiliki izin yang diperlukan untuk memuat data dari Amazon S3.
13. Pilih Buat tabel untuk membuat tabel menggunakan definisi yang ditampilkan.

Ringkasan tinjauan definisi tabel ditampilkan. Tabel dibuat dalam database. Untuk kemudian menghapus tabel, jalankan perintah DROP TABLE SQL. Untuk informasi selengkapnya, lihat [DROP TABLE](#) di Panduan Pengembang Database Amazon Redshift.

14. Pilih Muat data untuk memulai pemuatan data.

Saat beban selesai, editor kueri ditampilkan dengan perintah COPY yang dihasilkan yang digunakan untuk memuat data Anda. Hasil COPY ditampilkan. Jika berhasil, Anda sekarang dapat menggunakan SQL untuk memilih data dari tabel yang dimuat. Ketika ada kesalahan, kueri tampilan sistem STL_LOAD_ERRORS untuk mendapatkan detail lebih lanjut. Untuk informasi tentang kesalahan perintah COPY, lihat [STL_LOAD_ERRORS di Panduan Pengembang Database](#) Amazon Redshift.

Memuat data dari pengaturan file lokal dan alur kerja

Anda dapat memuat data dari file lokal ke tabel yang sudah ada atau yang baru.

Pengaturan administrator untuk memuat data dari file lokal

Administrator editor kueri v2 Anda harus menentukan bucket Amazon S3 umum di jendela Pengaturan akun. Pengguna akun harus dikonfigurasi dengan izin yang tepat.

- Izin IAM yang diperlukan — pengguna pemuatan dari file lokal harus memilikis3:ListBucket,,s3:GetBucketLocation, s3:putObjects3:getObject, dan

s3:deleteObject izin. *Awalan opsional dapat ditentukan untuk membatasi penggunaan bucket ini terkait editor kueri v2 ke objek dengan awalan ini.* Anda dapat menggunakan opsi ini saat menggunakan bucket Amazon S3 yang sama ini untuk penggunaan selain editor kueri v2. Untuk informasi selengkapnya tentang bucket dan awalan, lihat [Mengelola akses pengguna ke folder tertentu](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Untuk memastikan bahwa akses data lintas pengguna tidak diizinkan, sebaiknya administrator editor kueri v2 menggunakan kebijakan bucket Amazon S3 untuk membatasi akses objek berdasarkan. `aws:userid` Contoh berikut memungkinkan izin Amazon S3 ke a <staging-bucket-name> dengan akses baca/tulis hanya ke objek Amazon S3 dengan awalan sebagai. `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}/*"
      ]
    }
  ]
}
```

- Pemisahan data — kami menyarankan agar pengguna tidak memiliki akses ke data satu sama lain (bahkan sebentar). Memuat dari file lokal menggunakan bucket Amazon S3 pementasan yang

disiapkan oleh administrator editor kueri v2. Konfigurasi kebijakan bucket untuk bucket staging untuk menyediakan pemisahan data antar pengguna. <staging-bucket-name>Contoh berikut menunjukkan kebijakan bucket yang memisahkan data antara pengguna.

```
{
  "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}/*"
      ]
    }
  ]
}
```

Memuat data dari file lokal

Untuk memuat data file lokal ke dalam tabel yang ada

Administrator editor kueri v2 Anda harus menentukan bucket Amazon S3 umum di jendela Pengaturan akun. editor kueri v2 secara otomatis mengunggah file lokal ke bucket Amazon S3 umum yang digunakan oleh akun Anda, lalu menggunakan perintah COPY untuk memuat data. Perintah COPY yang dihasilkan dan dijalankan oleh editor kueri v2 memuat jendela file lokal mendukung banyak parameter yang tersedia untuk sintaks perintah COPY untuk disalin dari Amazon S3. Untuk informasi tentang perintah COPY dan opsinya yang digunakan untuk memuat data dari Amazon S3, lihat [COPY dari Amazon S3](#) di Panduan Pengembang Database Amazon Redshift.

1. Konfirmasikan bahwa tabel sudah dibuat di database tempat Anda ingin memuat data.
2. Konfirmasikan bahwa Anda terhubung ke database target di panel tampilan pohon editor kueri v2. Anda dapat membuat koneksi menggunakan menu konteks (klik kanan) ke cluster atau workgroup tempat data akan dimuat.

3. Pilih



Muat data.

4. Untuk Sumber data, pilih Muat dari file lokal.
5. Pilih Browse untuk menemukan file yang berisi data untuk Memuat file. Secara default, file dengan ekstensi `.csv`, `.avro.parquet`, dan `.orc` ditampilkan, tetapi Anda dapat memilih jenis file lainnya. Ukuran file maksimum adalah 100 MB.
6. Pilih format File untuk file yang akan diunggah. Format data yang didukung adalah CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET, dan ORC. Tergantung pada format file yang ditentukan, Anda dapat memilih opsi File masing-masing. Anda juga dapat memilih Data dienkripsi jika data dienkripsi dan masukkan Nama Sumber Daya Amazon (ARN) dari kunci KMS yang digunakan untuk mengenkripsi data.

Jika Anda memilih CSV atau DELIMITER, Anda juga dapat memilih karakter Delimiter dan apakah akan Abaikan baris header jika jumlah baris yang ditentukan sebenarnya adalah nama kolom dan bukan data yang akan dimuat.

7. (Opsional) Pengaturan lanjutan mendukung berbagai parameter konversi Data dan operasi Beban. Masukkan informasi ini sesuai kebutuhan untuk file Anda.

Untuk informasi selengkapnya tentang konversi data dan parameter pemuatan data, lihat [Parameter konversi data](#) dan [Operasi pemuatan data](#) di Panduan Pengembang Database Amazon Redshift.

8. Pilih Selanjutnya.
9. Pilih Muat tabel yang ada.
10. Konfirmasikan atau pilih lokasi tabel Target termasuk Cluster atau kelompok kerja, Database, Skema, dan nama Tabel tempat data dimuat.
11. (Opsional) Anda dapat memilih nama kolom untuk dimasukkan Pemetaan kolom untuk memetakan kolom dalam urutan file data input.
12. Pilih Muat data untuk memulai pemuatan data.

Ketika beban selesai, pesan ditampilkan apakah beban berhasil atau tidak. Jika berhasil, Anda sekarang dapat menggunakan SQL untuk memilih data dari tabel yang dimuat. Ketika ada kesalahan, kueri tampilan sistem `STL_LOAD_ERRORS` untuk mendapatkan detail lebih lanjut.


Untuk informasi tentang kesalahan perintah COPY, lihat [STL_LOAD_ERRORS di Panduan Pengembang Database](#) Amazon Redshift.

Template perintah COPY yang digunakan untuk memuat data muncul di riwayat Query Anda. Template perintah COPY ini menunjukkan beberapa parameter yang digunakan, tetapi tidak dapat dijalankan langsung di tab editor. Untuk informasi selengkapnya tentang riwayat kueri, lihat [Melihat kueri dan riwayat tab](#).

Saat Anda memuat data ke dalam tabel baru, editor kueri v2 pertama-tama membuat tabel di database, lalu memuat data sebagai tindakan terpisah dalam alur kerja yang sama.

Untuk memuat data file lokal ke dalam tabel baru

Administrator editor kueri v2 Anda harus menentukan bucket Amazon S3 umum di jendela Pengaturan akun. File lokal secara otomatis diunggah ke bucket Amazon S3 umum yang digunakan oleh akun Anda, dan kemudian perintah COPY digunakan oleh editor kueri v2 untuk memuat data. Perintah COPY yang dihasilkan dan dijalankan oleh editor kueri v2 memuat jendela file lokal mendukung banyak parameter yang tersedia untuk sintaks perintah COPY untuk disalin dari Amazon S3. Untuk informasi tentang perintah COPY dan opsinya yang digunakan untuk memuat data dari Amazon S3, lihat [COPY dari Amazon S3](#) di Panduan Pengembang Database Amazon Redshift.

1. Konfirmasikan bahwa Anda terhubung ke database target di panel tampilan pohon editor kueri v2. Anda dapat membuat koneksi menggunakan menu konteks (klik kanan) ke cluster atau workgroup tempat data akan dimuat.
2. Pilih  Muat data.
3. Untuk Sumber data, pilih Muat dari file lokal.
4. Pilih Browse untuk menemukan file yang berisi data untuk Memuat file. Secara default, file dengan ekstensi `.csv`, `.avro.parquet`, dan `.orc` ditampilkan, tetapi Anda dapat memilih jenis file lainnya. Ukuran file maksimum adalah 100 MB.
5. Pilih format File untuk file yang akan diunggah. Format data yang didukung adalah CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET, dan ORC. Tergantung pada format file yang ditentukan, Anda dapat memilih opsi File masing-masing. Anda juga dapat memilih Data dienkripsi jika data dienkripsi dan masukkan Nama Sumber Daya Amazon (ARN) dari kunci KMS yang digunakan untuk mengenkripsi data.

Jika Anda memilih CSV atau DELIMITER, Anda juga dapat memilih karakter Delimiter dan apakah akan Abaikan baris header jika jumlah baris yang ditentukan sebenarnya adalah nama kolom dan bukan data yang akan dimuat.

6. (Opsional) Pengaturan lanjutan mendukung berbagai parameter konversi Data dan operasi Beban. Masukkan informasi ini sesuai kebutuhan untuk file Anda.

Untuk informasi selengkapnya tentang konversi data dan parameter pemuatan data, lihat [Parameter konversi data](#) dan [Operasi pemuatan data](#) di Panduan Pengembang Database Amazon Redshift.

7. Pilih Selanjutnya.
8. Pilih Muat tabel baru.
9. Konfirmasikan atau pilih lokasi tabel Target termasuk Cluster atau workgroup, Database, dan Skema tempat data dimuat. Masukkan nama Tabel yang akan dibuat.
10. Pilih Buat tabel untuk membuat tabel menggunakan definisi yang ditampilkan.

Ringkasan tinjauan definisi tabel ditampilkan. Tabel dibuat dalam database. Untuk kemudian menghapus tabel, jalankan perintah DROP TABLE SQL. Untuk informasi selengkapnya, lihat [DROP TABLE](#) di Panduan Pengembang Database Amazon Redshift.

11. Pilih Muat data untuk memulai pemuatan data.

Ketika beban selesai, pesan ditampilkan yang menunjukkan apakah beban berhasil atau tidak. Jika berhasil, Anda sekarang dapat menggunakan SQL untuk memilih data dari tabel yang dimuat. Ketika ada kesalahan, kueri tampilan sistem STL_LOAD_ERRORS untuk mendapatkan detail lebih lanjut. Untuk informasi tentang kesalahan perintah COPY, lihat [STL_LOAD_ERRORS di Panduan Pengembang Database](#) Amazon Redshift.

Template perintah COPY yang digunakan untuk memuat data muncul di riwayat Query Anda. Template perintah COPY ini menunjukkan beberapa parameter yang digunakan, tetapi tidak dapat dijalankan langsung di tab editor. Untuk informasi selengkapnya tentang riwayat kueri, lihat [Melihat kueri dan riwayat tab](#).

Menulis dan menjalankan kueri

Anda dapat memasukkan kueri di editor atau memilih kueri yang disimpan dari daftar Kueri dan memilih Jalankan.

Secara default, Batas 100 diatur untuk membatasi hasil hingga 100 baris. Anda dapat mematikan opsi ini untuk mengembalikan set hasil yang lebih besar. Jika Anda mematikan opsi ini, Anda dapat menyertakan opsi `LIMIT` dalam pernyataan SQL Anda jika Anda ingin menghindari set hasil yang sangat besar. Untuk informasi selengkapnya, lihat [klausa ORDER BY](#) di Panduan Pengembang Database Amazon Redshift.

Untuk menampilkan rencana kueri di area hasil, aktifkan `Jelaskan`. Aktifkan grafik `Jelaskan` untuk hasil untuk juga menampilkan representasi grafis dari rencana penjelasan.

Untuk menyimpan kueri ke folder Kueri, pilih `Simpan`.

Untuk kueri yang berhasil, pesan sukses muncul. Jika kueri mengembalikan informasi, hasilnya akan ditampilkan di bagian Hasil. Jika jumlah hasil melebihi area tampilan, angka muncul di bagian atas area hasil. Anda dapat memilih angka untuk menampilkan halaman hasil yang berurutan.

Anda dapat memfilter dan mengurutkan Hasil untuk setiap kolom. Untuk memasukkan kriteria filter di header kolom hasil, arahkan kursor ke kolom untuk melihat menu



di mana Anda dapat memasukkan kriteria untuk memfilter kolom.

Jika kueri berisi kesalahan, editor kueri v2 menampilkan pesan kesalahan di area hasil. Pesan tersebut memberikan informasi tentang cara memperbaiki kueri.

Anda dapat mengekspor atau menyalin hasil kueri Anda dengan menggunakan menu konteks (klik kanan) di area hasil sebagai berikut:

- Pilih `Ekspor` set hasil dan `JSON` atau `CSV` untuk mengunduh seluruh rangkaian hasil baris ke file. Jumlah baris dalam kumpulan hasil mungkin dibatasi oleh opsi `Limit` atau `limit` klausa SQL dalam kueri. Ukuran maksimum set hasil yang diunduh adalah 5 MB.
- Jika tidak ada baris yang dipilih, pilih `Ekspor halaman saat ini` dan `JSON` atau `CSV` untuk mengunduh baris dari halaman saat ini ke file.
- Jika baris dipilih, lalu pilih `Ekspor baris yang dipilih` dan `JSON` atau `CSV` untuk mengunduh baris yang dipilih ke file.
- Jika baris dipilih, lalu pilih `Salin baris` untuk menyalin baris yang dipilih ke clipboard.
- Jika baris dipilih, lalu pilih `Salin baris dengan header` untuk menyalin baris yang dipilih dengan header kolom ke clipboard.

Anda juga dapat menggunakan pintasan Ctrl+C di Windows atau Cmd+C di macOS untuk menyalin data dari halaman hasil saat ini ke clipboard. Jika tidak ada baris yang dipilih, maka sel dengan fokus disalin ke clipboard. Jika baris dipilih, maka baris yang dipilih disalin ke clipboard.

Untuk menambahkan tab kueri baru, pilih



ikon, lalu Editor, yang muncul di baris dengan tab kueri. Tab kueri menggunakan `Isolated session` atau tidak. Dengan sesi terisolasi, hasil perintah SQL, seperti membuat tabel sementara di satu tab editor, tidak terlihat di tab editor lain. Saat Anda membuka tab editor di editor kueri v2, defaultnya adalah sesi terisolasi.

Untuk menjalankan kueri

1. Di area kueri, lakukan salah satu hal berikut:
 - Masukkan kueri.
 - Tempelkan kueri yang Anda salin.
 - Pilih folder Kueri, buka menu konteks (klik kanan) kueri yang disimpan, dan pilih Buka kueri.
2. Konfirmasikan bahwa Anda memilih Cluster atau Workgroup yang benar, dan nilai Database untuk SQL yang Anda rencanakan untuk dijalankan.

Awalnya, Anda dapat memilih Cluster atau Workgroup Anda di tampilan pohon. Pilih Database Anda di tampilan pohon juga.

Anda dapat mengubah Cluster atau Workgroup, dan Database dalam setiap tab editor dengan kontrol drop-down yang terletak di dekat header sesi Terisolasi dari setiap tab editor.

Untuk setiap tab editor, Anda memilih apakah akan menjalankan SQL dalam sesi Terisolasi. Sesi terisolasi memiliki koneksi sendiri ke database. Gunakan untuk menjalankan SQL yang terisolasi dari sesi editor kueri lainnya. Untuk informasi selengkapnya tentang koneksi, lihat [Membuka editor kueri v2](#).

3. Pilih Jalankan.

Area Hasil membuka dan menampilkan hasil kueri.

Untuk menampilkan rencana penjelasan untuk kueri

1. Pilih kueri.

2. Aktifkan Jelaskan.

Secara default, grafik Jelaskan juga aktif.

3. Pilih Jalankan.

Kueri berjalan dan rencana penjelasan ditampilkan di area Hasil kueri.

Editor kueri v2 mendukung fitur-fitur berikut:

- Anda dapat membuat kueri dengan beberapa pernyataan SQL dalam satu tab kueri. Kueri dijalankan secara serial dan beberapa tab hasil terbuka untuk setiap kueri.
- Anda dapat membuat kueri dengan variabel sesi dan tabel sementara.
- Anda dapat membuat kueri dengan parameter yang dapat diganti yang ditunjuk oleh `#{parameter}`. Anda dapat membuat kueri SQL Anda dengan beberapa parameter yang dapat diganti dan menggunakan parameter yang sama di beberapa tempat dalam pernyataan SQL Anda.

Saat kueri berjalan, sebuah jendela disajikan untuk memasukkan nilai parameter. Setiap kali Anda menjalankan kueri, jendela disajikan untuk memasukkan nilai parameter Anda.

Sebagai contoh, lihat [Contoh: Penjualan lebih besar dari parameter tertentu](#).

- Kueri diversi secara otomatis. Anda dapat memilih versi kueri yang lebih lama untuk dijalankan.
- Anda tidak perlu menunggu kueri selesai sebelum melanjutkan alur kerja Anda. Kueri Anda terus berjalan bahkan jika Anda menutup editor kueri.
- Saat membuat kueri, penyelesaian otomatis nama skema, tabel, dan kolom didukung.

Editor SQL mendukung fitur-fitur berikut:

- Tanda kurung awal dan akhir yang digunakan dalam SQL memiliki warna yang cocok. Garis vertikal ditampilkan di editor untuk membantu Anda mencocokkan tanda kurung.
- Anda dapat memciutkan dan memperluas bagian SQL Anda.
- Anda dapat mencari dan mengganti teks di SQL Anda.
- Anda dapat menggunakan tombol pintas untuk beberapa tugas pengeditan umum.
- Kesalahan SQL disorot di editor untuk lokasi area masalah yang nyaman.

Untuk demo fitur pengeditan, tonton video berikut: [Pengalaman Pengeditan Baru dan Ditingkatkan di editor kueri Amazon Redshift v2](#).

Contoh kueri

Berikut ini, Anda dapat menemukan deskripsi dari berbagai jenis kueri yang dapat Anda jalankan.

Data yang digunakan dalam banyak kueri ini berasal dari skema `ticket` sampel. Untuk informasi selengkapnya tentang memuat `ticket` data sampel, lihat [Memuat data sampel](#). Untuk informasi selengkapnya tentang data `ticket` sampel, lihat [Contoh database](#) di Panduan Pengembang Database Amazon Redshift.

Saat Anda menjalankan contoh kueri ini, konfirmasikan bahwa Anda memilih database yang benar di editor, seperti `sample_data_dev`.

Topik

- [Contoh: Mengatur variabel sesi](#)
- [Contoh: Acara teratas berdasarkan total penjualan](#)
- [Contoh: Penjualan lebih besar dari parameter tertentu](#)
- [Contoh: Buat tabel sementara](#)
- [Contoh: Memilih dari tabel sementara](#)

Contoh: Mengatur variabel sesi

Perintah berikut menetapkan parameter konfigurasi `search_path` server ke publik untuk sesi tersebut. Untuk informasi selengkapnya, lihat [SET](#) dan [search_path](#) di Panduan Pengembang Database Amazon Redshift.

```
set search_path to public;
```

Contoh: Acara teratas berdasarkan total penjualan

Kueri berikut menemukan acara dengan penjualan terbanyak.

```
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
```

```
group by eventname
order by 3;
```

Berikut ini adalah sebagian daftar hasil.

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
...		

Contoh: Penjualan lebih besar dari parameter tertentu

Kueri berikut menemukan penjualan di mana jumlah yang terjual lebih besar dari parameter yang ditentukan oleh `${numberoforders}`. Ketika nilai parameternya 7, hasilnya adalah 60 baris.

Saat Anda menjalankan kueri, editor kueri v2 menampilkan jendela formulir kueri Jalankan untuk mengumpulkan nilai parameter dalam pernyataan SQL.

```
select salesid, qtysold
from sales
where qtysold > ${numberoforders}
order by 2;
```

Berikut ini adalah sebagian daftar hasil.

salesid	qtysold
20005	8
21279	8
130232	8
42737	8
74681	8
67103	8
105533	8
91620	8
121552	8
...	

Contoh: Buat tabel sementara

Pernyataan berikut menciptakan tabel `eventsalestemp` sementara dengan memilih informasi dari tabel penjualan dan acara.

```
create temporary table eventsalestemp as
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname;
```

Contoh: Memilih dari tabel sementara

Pernyataan berikut memilih acara, total pesanan, dan total penjualan dari `eventsalestemp` tabel sementara, dipesan berdasarkan total pesanan.

```
select eventname, totalorders, totalsales
from eventsalestemp
order by 2;
```

Berikut ini adalah sebagian daftar hasil.

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
...		

Menulis dan menjalankan notebook

Anda dapat menggunakan buku catatan untuk mengatur, membuat anotasi, dan berbagi beberapa kueri SQL dalam satu dokumen. Anda dapat menambahkan beberapa kueri SQL dan sel Markdown ke buku catatan. Notebook menyediakan cara untuk mengelompokkan kueri dan penjelasan yang terkait dengan analisis data dalam satu dokumen dengan menggunakan beberapa kueri dan sel Markdown. Anda dapat menambahkan teks dan memformat tampilan menggunakan sintaks Markdown untuk memberikan konteks dan informasi tambahan untuk tugas analisis data Anda. Anda dapat membagikan buku catatan Anda dengan anggota tim.

Untuk menggunakan buku catatan, Anda harus menambahkan izin untuk buku catatan ke kepala IAM Anda (pengguna IAM atau peran IAM). Sebagai praktik terbaik, kami merekomendasikan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#). Anda dapat menambahkan izin ke salah satu kebijakan terkelola editor kueri v2. Untuk informasi selengkapnya, lihat [Mengakses editor kueri v2](#).

Anda bisa Jalankan semua sel notebook secara berurutan. Sel kueri SQL notebook memiliki sebagian besar kemampuan yang sama dengan tab editor kueri. Untuk informasi selengkapnya, lihat [Menulis dan menjalankan kueri](#). Berikut ini adalah perbedaan antara tab query editor dan sel SQL di notebook.

- Tidak ada kontrol untuk dijalankan Explain pada pernyataan SQL di notebook.
- Anda hanya dapat membuat satu bagan per sel SQL di buku catatan.

Anda dapat mengekspor dan mengimpor buku catatan ke file yang dibuat dengan editor kueri v2. Ekstensi file adalah .ipynb dan ukuran file bisa maksimal 5 MB. Sel SQL dan Markdown disimpan dalam file. Cluster atau workgroup dan database tidak disimpan di notebook yang diekspor. Saat Anda membuka buku catatan yang diimpor, Anda memilih cluster atau workgroup dan database tempat menjalankannya. Setelah menjalankan sel SQL, Anda kemudian dapat memilih di tab hasil apakah akan menampilkan halaman hasil saat ini sebagai bagan. Kumpulan hasil kueri tidak disimpan di buku catatan.

Saat Anda menjalankan buku catatan, baik dengan Run all atau Run, maka panel status Run akan tersedia. Pilih



ikon untuk membuka panel. Panel ini berisi ringkasan status Run all atau Run terbaru dari sel SQL di buku catatan Anda. Jika Anda menjalankan beberapa sel SQL, Anda dapat melihat sekilas status, waktu yang telah berlalu, dan beberapa detail tentang proses. Anda dapat memfilter sel yang ditampilkan berdasarkan status: All, Succeeded, Error, In progress, atau Canceled. Anda juga dapat menggunakan panel ini untuk menavigasi ke sel SQL di editor.

Untuk membuat buku catatan

1. Dari menu navigator, pilih



Editor.

2. Pilih 

lalu pilih Notebook.

Secara default, sel kueri SQL muncul di buku catatan.

3. Di sel kueri SQL, lakukan salah satu hal berikut:

- Masukkan kueri.
- Tempelkan kueri yang Anda salin.

4. (Opsional) Pilih



ikon, lalu pilih Markdown untuk menambahkan sel Markdown di mana Anda dapat memberikan teks deskriptif atau penjelasan menggunakan sintaks Markdown standar.

5. (Opsional) Pilih



ikon, lalu pilih SQL untuk menyisipkan sel SQL.

Anda dapat mengganti nama notebook menggunakan ikon



(pensil).

Dari menu







(lainnya), Anda juga dapat melakukan operasi berikut pada buku catatan:



dengan tim saya — Untuk berbagi buku catatan dengan tim Anda seperti yang ditentukan oleh tag.

Lihat informasi yang lebih lengkap di [Berbagi kueri](#)

Bagika

-  - Untuk mengekspor buku catatan ke file lokal dengan `.ipynb` ekstensi. Ekspor
-  versi — Untuk membuat versi notebook. Untuk melihat versi buku catatan, navigasikan ke buku catatan yang disimpan dan buka Riwayat versi. Simpan
-  — Untuk membuat salinan buku catatan dan membukanya di tab notebook baru. Duplika
-  - Untuk menampilkan pintasan yang tersedia saat membuat buku catatan. Pintasa

Untuk membuka buku catatan yang disimpan

1. Dari menu navigator, pilih



Notebook. Notebook dan folder notebook Anda yang disimpan akan ditampilkan.

2. Pilih buku catatan yang ingin Anda buka dan klik dua kali.

Anda dapat menampilkan buku catatan saya, buku catatan yang Dibagikan oleh saya, dan buku catatan yang Dibagikan ke tim saya dalam tab buku catatan.

Untuk mengimpor buku catatan dari file lokal ke buku catatan saya, pilih



Impor, lalu arahkan ke `.ipynb` file yang berisi buku catatan Anda. Notebook diimpor ke folder notebook yang sedang terbuka. Anda kemudian dapat membuka notebook di editor notebook.

Dari menu konteks (klik kanan) notebook Anda dapat melakukan operasi berikut:

- Buka buku catatan — Untuk membuka buku catatan di editor.
- Simpan versi — Untuk menyimpan versi notebook.
- Riwayat versi — Untuk menampilkan versi notebook. Dari jendela Riwayat versi Anda dapat menghapus dan mengembalikan versi. Anda juga dapat membuat buku catatan dari versi yang dipilih saat ini.
- Edit tag — Untuk membuat dan mengedit tag pada buku catatan.

- Bagikan dengan tim saya — Untuk berbagi buku catatan dengan tim Anda.

Untuk berbagi buku catatan dengan tim Anda, pastikan bahwa Anda memiliki tag utama yang `sqlworkbench-team` disetel ke nilai yang sama dengan anggota tim lainnya di akun Anda. Misalnya, administrator mungkin menetapkan nilai `accounting-team` untuk semua orang di departemen akuntansi. Lihat contohnya di [Izin yang diperlukan untuk menggunakan editor kueri v2](#)

- Ekspor - Untuk mengekspor buku catatan ke file lokal.
- Ganti nama - Untuk mengganti nama notebook.
- Duplikat — Untuk membuat salinan buku catatan.
- Hapus — Untuk menghapus buku catatan.

Untuk demo notebook, tonton video berikut: [Amazon Redshift SQL Notebooks](#) di editor kueri v2.

Menanyakan AWS Glue Data Catalog

Anda dapat menggunakan editor kueri v2 untuk menanyakan data yang dikatalogkan di AWS Glue Data Catalog. Secara default, terdaftar sebagai editor kueri v2 database bernama `awsdatacatalog`. AWS Glue Data Catalog Menanyakan tidak tersedia di semua Amazon Wilayah AWS Redshift. Gunakan perintah `SHOW` untuk menentukan apakah kemampuan ini tersedia. Untuk informasi lebih lanjut tentang AWS Glue, lihat [Apa itu AWS Glue?](#) di Panduan AWS Glue Pengembang.

Note

Kueri hanya AWS Glue Data Catalog didukung di cluster tipe node Amazon Redshift RA3 dan Amazon Redshift Tanpa Server.

Anda dapat mengonfigurasi gudang data dan melihat objek AWS Glue database yang dikatalogkan menggunakan perintah SQL berikut:

- `SHOW` - untuk menampilkan `awsdatacatalog` apakah dipasang untuk gudang data yang saat ini terhubung. Misalnya, untuk menampilkan nilai `data_catalog_auto_mount` parameter, jalankan:

```
SHOW data_catalog_auto_mount;
```

Untuk informasi selengkapnya, lihat [TAMPILKAN](#) di Panduan Pengembang Database Amazon Redshift.

- **ALTER SYSTEM** — untuk mengubah konfigurasi tingkat sistem. `data_catalog_auto_mount` Misalnya, untuk mengubah nilai `data_catalog_auto_mount` parameter menjadion, jalankan:

```
ALTER SYSTEM SET data_catalog_auto_mount = on;
```

Perubahan akan berlaku ketika klaster yang disediakan di-boot ulang atau grup kerja tanpa server secara otomatis dijeda dan dilanjutkan. Untuk informasi selengkapnya, lihat [MENGUBAH SISTEM di Panduan](#) Pengembang Database Amazon Redshift.

- **TAMPILKAN SKEMA** - menunjukkan daftar skema. Skema dalam database bernama `awsdatacatalog` mewakili database yang dikatalogkan AWS Glue dalam. AWS Glue Data Catalog Misalnya, untuk menampilkan skema ini, jalankan:

```
SHOW SCHEMAS FROM DATABASE awsdatacatalog;
```

Untuk informasi selengkapnya, lihat [TAMPILKAN SKEMA](#) di Panduan Pengembang Database Amazon Redshift.

- **TAMPILKAN TABEL** - menunjukkan daftar tabel dalam skema. Misalnya, untuk menampilkan tabel dalam AWS Glue Data Catalog database bernama `awsdatacatalog` yang sedang `myglue` dijalankan skema:

```
SHOW TABLES FROM SCHEMA awsdatacatalog.myschema;
```

Untuk informasi selengkapnya, lihat [TAMPILKAN TABEL](#) di Panduan Pengembang Database Amazon Redshift.

- **TAMPILKAN KOLOM** - menunjukkan daftar kolom dalam tabel. Misalnya, untuk menampilkan kolom dalam AWS Glue Data Catalog database bernama `awsdatacatalog` yang berada dalam skema `myglue` dan tabel `mytable` berjalan:

```
SHOW COLUMNS FROM TABLE awsdatacatalog.myglue.mytable;
```

Untuk informasi selengkapnya, lihat [TAMPILKAN KOLOM](#) di Panduan Pengembang Database Amazon Redshift.

Untuk memberikan izin kepada pengguna atau peran IAM Anda untuk melakukan kueri AWS Glue Data Catalog, ikuti langkah-langkah ini

1. Di panel tampilan pohon, sambungkan ke database awal di klaster yang disediakan atau grup kerja tanpa server menggunakan metode autentikasi nama pengguna dan kata sandi Database. Misalnya, sambungkan ke dev database menggunakan pengguna admin dan kata sandi yang Anda gunakan saat membuat klaster atau grup kerja.
2. Di tab editor, jalankan pernyataan SQL berikut untuk memberikan akses pengguna IAM ke file. AWS Glue Data Catalog

```
GRANT USAGE ON DATABASE awsdatalog to "IAM:myIAMUser"
```

Di mana *iam:myiamUser* adalah *pengguna* IAM yang ingin Anda berikan hak istimewa penggunaan ke. AWS Glue Data Catalog Atau, Anda dapat memberikan hak istimewa penggunaan ke *IAMR:myiamRole* untuk peran IAM.

3. Di panel tampilan pohon, edit atau hapus sambungan ke klaster atau grup kerja yang sebelumnya Anda buat. Connect ke cluster atau workgroup Anda dengan salah satu cara berikut:
 - Untuk mengakses awsdatalog database dari cluster, Anda harus menggunakan metode otentikasi Kredensial sementara menggunakan identitas IAM Anda. Untuk informasi selengkapnya tentang metode otentikasi ini, lihat [Menghubungkan ke database Amazon Redshift](#). Administrator editor kueri v2 Anda mungkin perlu mengonfigurasi pengaturan Akun untuk akun untuk menampilkan metode otentikasi ini di jendela koneksi.
 - Untuk mengakses awsdatalog database dari workgroup, Anda harus menggunakan metode otentikasi Pengguna Federasi. Untuk informasi selengkapnya tentang metode otentikasi ini, lihat [Menghubungkan ke database Amazon Redshift](#).
4. Dengan hak istimewa yang diberikan, Anda dapat menggunakan identitas IAM Anda untuk menjalankan SQL terhadap Anda. AWS Glue Data Catalog

Setelah menghubungkan, Anda dapat menggunakan editor kueri v2 untuk menanyakan data yang dikatalogkan. AWS Glue Data Catalog Pada panel tampilan pohon editor kueri v2, pilih cluster atau workgroup dan database. awsdatalog Di panel editor atau buku catatan, konfirmasi klaster atau grup kerja yang benar dipilih. Basis data yang dipilih harus menjadi basis data Amazon Redshift awal seperti. dev Untuk informasi tentang membuat kueri, lihat [Menulis dan menjalankan kueri](#) dan [Menulis dan menjalankan notebook](#) Nama database awsdatalog dicadangkan untuk referensi

database Katalog Data eksternal di akun Anda. Query terhadap `awsdatacatalog` database hanya bisa read-only. Gunakan notasi tiga bagian untuk mereferensikan tabel dalam pernyataan `SELECT` Anda. Di mana bagian pertama adalah nama database, bagian kedua adalah nama AWS Glue database, dan bagian ketiga adalah nama AWS Glue tabel.

```
SELECT * FROM awsdatacatalog.<aws-glue-db-name>.<aws-glue-table-name>;
```

Anda dapat melakukan berbagai skenario yang membaca AWS Glue Data Catalog data dan mengisi tabel Amazon Redshift.

Contoh SQL berikut bergabung dengan dua tabel yang didefinisikan dalam. 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;
```

Contoh SQL berikut membuat tabel Amazon Redshift dan mengisinya dengan data dari gabungan dua tabel. AWS Glue

```
CREATE TABLE dev.public.glue AS
SELECT pn.emp_id, alias, role, project_name
FROM "awsdatacatalog"."empl_db"."project_name_table" pn,
"awsdatacatalog"."empl_db"."project_alias_table" pa
WHERE pn.emp_id = pa.emp_id;
```

Menanyakan data lake

Anda dapat membuat kueri data di danau data Amazon S3. Pertama, Anda membuat skema eksternal untuk referensi database eksternal di [AWS Glue Data Catalog](#). Kemudian, Anda dapat melakukan kueri data di data lake Amazon S3.

Demo: Kueri data lake

Untuk demo tentang cara query data lake, menonton video berikut. [Kueri data lake Anda dari editor kueri Amazon Redshift v2](#).

Prasyarat

Sebelum Anda bekerja dengan data lake di editor kueri v2, konfirmasi hal berikut telah diatur di lingkungan Amazon Redshift Anda:

- Perayapi data Amazon S3 Anda menggunakan AWS Glue dan mengaktifkan Katalog Data Anda AWS Lake Formation.
- Buat peran IAM untuk Amazon Redshift menggunakan Katalog Data yang AWS Glue diaktifkan untuk AWS Lake Formation. Untuk detail tentang prosedur ini, lihat [Untuk membuat peran IAM untuk Amazon Redshift menggunakan AWS Glue Data Catalog diaktifkan untuk AWS Lake Formation](#). Untuk informasi selengkapnya tentang penggunaan Redshift Spectrum dan Lake Formation, lihat [Menggunakan Redshift Spectrum dengan AWS Lake Formation](#).
- Berikan izin SELECT pada tabel untuk query dalam database Lake Formation. Untuk rincian tentang prosedur ini, lihat [Untuk memberikan izin SELECT pada tabel untuk query dalam database Lake Formation](#).

Anda dapat memverifikasi di konsol Lake Formation (<https://console.aws.amazon.com/lakeformation/>), bagian Izin, halaman izin danau data, bahwa peran IAM, AWS Glue database, dan tabel memiliki izin yang tepat.

- Konfirmasikan pengguna Anda yang terhubung memiliki izin untuk membuat skema di database Amazon Redshift dan mengakses data di data lake Anda. Saat Anda terhubung ke database di editor kueri v2, Anda memilih metode otentikasi yang menyertakan kredensial, yang dapat berupa pengguna database atau pengguna IAM. Pengguna yang terhubung harus memiliki hak akses dan database yang tepat, seperti `superuser.admin`. Pengguna Amazon Redshift yang membuat klaster atau grup kerja memiliki `superuser` hak istimewa dan dapat membuat skema dan mengelola database Redshift. Untuk informasi selengkapnya tentang menghubungkan ke database dengan editor kueri v2, lihat [Menghubungkan ke database Amazon Redshift](#).

Membuat skema eksternal

Untuk membuat kueri data dalam danau data Amazon S3, buat skema eksternal. Skema eksternal referensi database eksternal di [AWS Glue Data Catalog](#).

1. Dalam tampilan Editor editor kueri v2,

pilih 

Buat, lalu pilih Skema.

2. Masukkan nama Skema.
3. Untuk jenis Skema, pilih Eksternal.
4. Dalam rincian Data Catalog, Region default ke Wilayah AWS tempat database Redshift Anda berada.

5. Pilih AWS Gluedatabase yang akan dipetakan oleh skema eksternal dan yang berisi referensi keAWS Glue tabel.
6. Pilih peran IAM untuk Amazon Redshift yang memiliki izin yang diperlukan untuk melakukan kueri data di Amazon S3.
7. Secara opsional, pilih peran IAM yang memiliki izin ke Katalog Data.
8. Pilih Buat skema.

Skema muncul di bawah database Anda di panel tampilan pohon.

Saat membuat skema, jika Anda menerima izin ditolak kesalahan untuk database Anda, periksa apakah pengguna yang terhubung memiliki hak database untuk membuat skema.

Mengkueri data di data lake Amazon S3 Anda

Anda menggunakan skema yang Anda buat dalam prosedur sebelumnya.

1. Di panel tampilan pohon, pilih skema.
2. Untuk melihat definisi tabel, pilih tabel. Kolom tabel dan tipe data ditampilkan.
3. Untuk query tabel, pilih tabel dan dalam menu konteks (klik kanan), pilih Pilih tabel untuk menghasilkan query.
4. Jalankan kueri di Editor.

Contoh berikut SQL dihasilkan oleh query editor v2 untuk query semua baris dalamAWS Glue tabel bernamaflightscsv. Kolom dan baris yang ditunjukkan dalam output dipotong agar memudahkan.

```
SELECT * FROM "dev"."mydatalake_schema"."flightscsv";
```

year	quarter	month	dom	day_of_week	fl_date	unique_carrier	airline_id
2016	4	10	19	3	10/19/16	00	20304
2016	4	10	19	3	10/19/16	00	20304
2016	4	10	19	3	10/19/16	00	20304
2016	4	10	19	3	10/19/16	00	20304

...

Bekerja dengan datashares

Anda dapat membuat datashare sehingga pengguna di cluster lain dapat melakukan query data. Cluster yang berisi data yang ingin Anda bagikan disebut cluster produser. Anda membuat datashare di cluster produser untuk objek database yang ingin Anda bagikan. Anda dapat berbagi skema, tabel, tampilan, dan fungsi yang ditentukan pengguna SQL (UDF). Cluster yang ingin Anda bagikan datanya disebut cluster konsumen. Pada cluster konsumen, Anda membuat database dari datashare. Kemudian, pengguna di cluster konsumen dapat melakukan query data. Untuk informasi selengkapnya, lihat [Memulai berbagi data](#) di Panduan Pengembang Database Amazon Redshift.

Membuat datashares

Anda membuat datashare pada cluster yang ingin Anda gunakan sebagai cluster produser. Untuk mempelajari lebih lanjut tentang pertimbangan data, lihat [Pertimbangan berbagi data di Amazon Redshift di](#) Panduan Pengembang Database Amazon Redshift.

1. Pilih database pada cluster produser yang ingin Anda gunakan.
2. Buat datashare. Sebagai contoh:

```
create datashare mysource;
```

3. Tetapkan izin pada datashare. Sebagai contoh:

```
grant alter, share on datashare mysource to admin;
```

4. Tetapkan izin pada objek database yang ingin Anda bagikan. Sebagai contoh:

```
alter datashare mysource add schema public;
```

```
alter datashare mysource add table public.event;
```

5. Tetapkan izin pada namespace cluster konsumen untuk mengakses datashare. Sebagai contoh:

```
grant usage on datashare mysource to namespace '2b12345-1234-5678-9012-  
bb1234567890';
```

Menampilkan datashares

Anda dapat menampilkan datashares yang telah Anda buat di cluster produser.

1. Pilih cluster produser.
2. Tampilkan datashares. Sebagai contoh:

```
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
```

Membuat database konsumen

Pada cluster konsumen, Anda membuat database dari datashare. Langkah-langkah ini menjelaskan cara berbagi data antara dua cluster di akun yang sama. Untuk informasi tentang berbagi data di seluruh AWS akun, lihat [Berbagi data di seluruh AWS akun](#) di Panduan Pengembang Database Amazon Redshift.

Anda dapat menggunakan perintah SQL atau panel tampilan pohon editor kueri v2 untuk membuat database.

Untuk menggunakan SQL

1. Buat database dari datashare untuk akun Anda dan namespace klaster produser. Sebagai contoh:

```
create database share_db from datashare mysource of account '123456789012'  
namespace 'p1234567-8765-4321-p10987654321';
```

2. Tetapkan izin sehingga pengguna dapat mengakses database dan skema. Sebagai contoh:

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

Untuk menggunakan panel tampilan pohon editor kueri v2

1. Pilih



Buat, lalu pilih Database.

2. Masukkan nama Database.
3. (Opsional) Pilih Pengguna dan grup, dan pilih pengguna Database.
4. Pilih Buat menggunakan datashare.
5. Pilih datashare.
6. Pilih Buat basis data.

Database



datashare baru ditampilkan di panel tampilan pohon editor kueri v2.

7. Tetapkan izin sehingga pengguna dapat mengakses database dan skema. Sebagai contoh:

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

Menanyakan objek datashare

Pada cluster konsumen, Anda dapat menanyakan objek datashare menggunakan nama objek yang sepenuhnya memenuhi syarat yang diekspresikan dengan notasi tiga bagian: database, skema, dan nama objek.

1. Di panel tampilan pohon editor kueri v2, pilih skema.
2. Untuk melihat definisi tabel, pilih tabel.

Kolom tabel dan tipe data ditampilkan.

3. Untuk menanyakan tabel, pilih tabel dan gunakan menu konteks (klik kanan) untuk memilih Pilih tabel.
4. Tabel kueri menggunakan perintah SELECT. Sebagai contoh:

```
select top 10 * from test_db.public.event;
```

Menjadwalkan kueri dengan editor kueri v2

Anda dapat membuat jadwal untuk menjalankan pernyataan SQL dengan editor kueri Amazon Redshift v2. Anda membuat jadwal untuk menjalankan pernyataan SQL Anda pada interval waktu yang sesuai dengan kebutuhan bisnis Anda. Saat kueri terjadwal berjalan, kueri dimulai oleh Amazon EventBridge dan menggunakan Amazon Redshift Data API.

Untuk membuat jadwal untuk menjalankan pernyataan SQL

1. Pada



tampilan Editor, pilih



Jadwal untuk membuat jadwal untuk menjalankan pernyataan SQL.

2. Ketika Anda menentukan jadwal, Anda memberikan informasi berikut.

- Peran IAM yang mengasumsikan izin yang diperlukan untuk menjalankan kueri. Peran IAM ini juga dilampirkan ke cluster atau workgroup Anda.
- Nilai otentikasi untuk salah satu AWS Secrets Manager atau kredensi sementara untuk mengotorisasi akses klaster atau grup kerja Anda. Metode otentikasi ini didukung oleh API Data. Untuk informasi selengkapnya, lihat [Mengautentikasi kueri terjadwal](#).
- Cluster atau workgroup tempat database Anda berada.
- Nama database yang berisi data yang akan ditanyakan.
- Nama kueri terjadwal dan deskripsinya. Editor kueri v2 mengawali nama kueri terjadwal yang Anda berikan dengan "QS2-". Editor kueri v1 mengawali nama kueri terjadwal dengan "QS-".
- Pernyataan SQL yang akan dijalankan pada jadwal.
- Frekuensi jadwal dan opsi pengulangan atau nilai diformat cron yang menentukan jadwal. Untuk informasi selengkapnya, lihat [Ekspresi Cron di Panduan Pengguna CloudWatch Acara Amazon](#).

- Secara opsional, Anda dapat mengaktifkan notifikasi Amazon SNS standar untuk memantau kueri terjadwal. Anda mungkin perlu mengonfirmasi alamat email yang Anda berikan ke notifikasi Amazon SNS. Periksa email Anda untuk tautan untuk mengonfirmasi alamat email untuk notifikasi Amazon SNS. Untuk informasi selengkapnya, lihat [Pemberitahuan email](#) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Jika kueri Anda sedang dijalankan tetapi Anda tidak melihat pesan yang dipublikasikan di topik SNS Anda, lihat [Aturan saya berjalan, tetapi saya tidak melihat pesan apa pun yang dipublikasikan ke topik Amazon SNS saya](#) di Panduan Pengguna EventBridge Amazon.
3. Pilih Jadwalkan kueri untuk menyimpan dan mengaktifkan jadwal dan menambahkan jadwal ke daftar kueri dalam tampilan Kueri terjadwal.



Tampil

kueri terjadwal mencantumkan semua kueri terjadwal untuk klaster dan grup kerja Anda. Dengan tampilan ini, Anda dapat menampilkan detail kueri jadwal, mengaktifkan atau menonaktifkan jadwal, mengedit jadwal, dan menghapus kueri terjadwal. Saat Anda melihat detail kueri, Anda juga dapat melihat riwayat menjalankan kueri dengan jadwal.

Note

Proses kueri jadwal hanya tersedia di daftar riwayat Jadwal selama 24 jam. Kueri yang berjalan pada jadwal tidak muncul di tampilan riwayat Kueri editor kueri v2.

Menyiapkan izin untuk menjadwalkan kueri

Untuk menjadwalkan kueri, pengguna AWS Identity and Access Management (IAM) yang menentukan jadwal dan peran IAM yang terkait dengan jadwal harus dikonfigurasi dengan izin IAM untuk menggunakan Amazon dan Amazon EventBridge Redshift Data API. Untuk menerima email dari kueri terjadwal, notifikasi Amazon SNS yang Anda tentukan secara opsional harus dikonfigurasi juga.

Berikut ini menjelaskan tugas untuk menggunakan kebijakan AWS terkelola untuk memberikan izin, tetapi tergantung pada lingkungan Anda, Anda mungkin ingin mengurangi izin yang diizinkan.

[Untuk pengguna IAM yang masuk ke editor kueri v2, edit pengguna IAM menggunakan konsol IAM \(https://console.aws.amazon.com/iam/\).](https://console.aws.amazon.com/iam/)

- Selain izin untuk menjalankan operasi Amazon Redshift dan editor kueri v2, lampirkan `AmazonEventBridgeFullAccess` kebijakan `AmazonRedshiftDataFullAccess` AWS dan terkelola ke pengguna IAM.
- Atau, tetapkan izin ke peran dan tetapkan peran tersebut kepada pengguna.

Lampirkan kebijakan yang mengizinkan `sts:AssumeRole` izin ke ARN sumber daya peran IAM yang Anda tentukan saat Anda menentukan kueri terjadwal. Untuk informasi selengkapnya tentang mengambil peran, lihat [Memberikan izin pengguna untuk beralih peran](#) di Panduan Pengguna IAM.

Contoh berikut menunjukkan kebijakan izin yang mengasumsikan peran IAM `myRedshiftRole` dalam akun. `123456789012` Peran IAM juga `myRedshiftRole` merupakan peran IAM yang dilampirkan ke cluster atau workgroup tempat kueri terjadwal berjalan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AssumeIAMRole",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::123456789012:role/myRedshiftRole"
      ]
    }
  ]
}
```

Perbarui kebijakan kepercayaan peran IAM yang digunakan untuk menjadwalkan kueri agar pengguna IAM mengasumsikan itu.

```
{
  "Sid": "AssumeRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:user/myIAMUsername"
  },
  "Action": "sts:AssumeRole"
}
```

[Untuk peran IAM yang Anda tentukan agar kueri terjadwal dijalankan, edit peran IAM menggunakan konsol IAM \(https://console.aws.amazon.com/iam/\).](https://console.aws.amazon.com/iam/)

- Lampirkan kebijakan AmazonRedshiftDataFullAccess dan AmazonEventBridgeFullAccess AWS terkelola ke peran IAM. Kebijakan AmazonRedshiftDataFullAccess terkelola hanya mengizinkan redshift-serverless:GetCredentials izin untuk grup kerja Redshift Tanpa Server yang ditandai dengan kunci. RedshiftDataFullAccess

Mengautentikasi kueri terjadwal

Saat menjadwalkan kueri, Anda menggunakan salah satu metode otentikasi berikut saat SQL berjalan. Setiap metode memerlukan kombinasi input yang berbeda pada editor kueri v2. Metode otentikasi ini didukung oleh Data API yang digunakan untuk menjalankan pernyataan SQL Anda.

Pengguna database atau peran yang digunakan untuk menjalankan query harus memiliki hak istimewa database yang diperlukan. Misalnya, untuk memberikan IAMR:MyRedshiftQEv2Scheduler hak istimewa ke tabelmytable, jalankan perintah SQL berikut.

```
GRANT all ON TABLE mytable TO "IAMR:MyRedshiftQEv2Scheduler";
```

Untuk melihat daftar pengguna database di cluster atau workgroup Anda, kueri tampilan PG_USER_INFO sistem.

Note

Setiap grup kerja Redshift Tanpa Server yang Anda jadwalkan kueri akan ditandai dengan kuncinya. RedshiftDataFullAccess Untuk informasi selengkapnya, lihat [Mengotorisasi akses ke API Data Amazon Redshift](#).

Sebagai alternatif untuk menandai workgroup, Anda dapat menambahkan kebijakan inline ke peran IAM (yang ditentukan dengan jadwal) yang memungkinkan. redshift-serverless:GetCredentials Sebagai contoh:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UseTemporaryCredentialsForAllServerlessWorkgroups",
      "Effect": "Allow",
```

```

    "Action": "redshift-serverless:GetCredentials",
    "Resource": [
      "arn:aws:redshift-serverless:*:*:workgroup/*"
    ]
  }
]
}

```

AWS Secrets Manager

Dengan metode ini, berikan nilai rahasia untuk rahasia-arn yang disimpan di AWS Secrets Manager. Rahasia ini berisi kredensial untuk terhubung ke database Anda. Anda mungkin telah membuat rahasia dengan kredensial yang tepat saat membuat kluster atau grup kerja. Rahasiannya harus ditandai dengan kuncinya `RedshiftDataFullAccess`. Jika kunci tag belum ada, gunakan AWS Secrets Manager konsol untuk menambahkannya. Untuk informasi tentang membuat rahasia, lihat [Membuat rahasia untuk kredensi koneksi database](#).

Untuk informasi selengkapnya tentang izin minimum, lihat [Membuat dan Mengelola Rahasia dengan AWS Secrets Manager](#) di Panduan AWS Secrets Manager Pengguna.

Kredensial sementara

Dengan metode ini, berikan nama Database dan nilai pengguna Database Anda saat menghubungkan ke database dalam sebuah cluster. Anda hanya perlu memberikan nama Database Anda saat menghubungkan ke database di workgroup.

Saat menyambung ke kluster, `AmazonRedshiftDataFullAccess` kebijakan tersebut mengizinkan `redshift_data_api_user` izin yang dinamai pengguna database `redshift:GetClusterCredentials`. Jika Anda ingin menggunakan pengguna database yang berbeda untuk menjalankan pernyataan SQL, tambahkan kebijakan ke peran IAM yang dilampirkan ke cluster Anda untuk mengizinkan `redshift:GetClusterCredentials`. Contoh kebijakan berikut memungkinkan pengguna database `awsuser` dan `myuser`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UseTemporaryCredentialsForAllDbUsers",
      "Effect": "Allow",

```

```

        "Action": "redshift:GetClusterCredentials",
        "Resource": [
            "arn:aws:redshift:*:*:dbuser:*/awsuser",
            "arn:aws:redshift:*:*:dbuser:*/myuser"
        ]
    }
]
}

```

Menyiapkan izin untuk melihat riwayat kueri jadwal

Untuk memungkinkan pengguna melihat riwayat kueri jadwal, edit peran IAM (yang ditentukan dengan jadwal) Hubungan kepercayaan untuk menambahkan izin.

Berikut ini adalah contoh kebijakan kepercayaan dalam peran IAM yang memungkinkan pengguna IAM *MyIamUsername* untuk melihat riwayat kueri jadwal. Alih-alih mengizinkan `sts:AssumeRole` izin pengguna IAM, Anda dapat memilih untuk mengizinkan peran IAM izin ini.

```

{
  "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"
  }
]
}

```

Memantau kueri terjadwal

Untuk topik Amazon SNS yang Anda tentukan untuk mengirim notifikasi email, buat topik Amazon SNS menggunakan editor kueri v2 dengan menavigasi ke bagian pemberitahuan SNS, Aktifkan pemantauan, dan buat topik dengan topik Buat SNS. Editor kueri v2 membuat topik Amazon SNS dan menambahkan prinsip layanan ke kebijakan akses untuk Amazon. EventBridge Berikut ini adalah contoh Kebijakan akses yang dibuat dalam topik Amazon SNS. Dalam contoh, topik Wilayah AWS *us-west-2*, Akun AWS *123456789012*, dan Amazon SNS digunakan. *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"
    }
  ]
}

```

Saat kueri terjadwal berjalan, Amazon SNS mengirimkan email AWS notifikasi. *Contoh berikut menunjukkan email yang dikirim ke myemail@example.com untuk kueri terjadwal QS2-May25A yang berjalan di Wilayah AWS eu-north-1 di Akun AWS 123456789012 menggunakan topik notifikasi Amazon SNS May25a-SNS.*

```

{"version":"0","id":"8e4323ec-5258-7138-181b-91290e30ff9b","detail-type":"Scheduled Event","source":"aws.events","account":"123456789012","time":"2023-05-25T15:22:00Z",

```

```
"region":"eu-north-1","resources":["arn:aws:events:eu-north-1:123456789012:rule/QS2-may25a"],"detail":{}}
```

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:

```
https://sns.eu-north-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:eu-north-1:123456789012:may25a-SNS:0c1a3d05-39c2-4507-bc3d-47250513d7b0&Endpoint=myemail@example.com
```

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>

Pemecahan masalah pengaturan penjadwalan kueri

Pertimbangkan hal berikut jika Anda memiliki masalah dalam menjadwalkan kueri.

Kueri tidak berjalan

Periksa apakah peran IAM yang digunakan dalam jadwal memiliki izin untuk mendapatkan kredensial cluster sementara. Izin untuk cluster yang disediakan adalah `redshift:GetClusterCredentialsWithIAM` Izin untuk grup kerja Redshift Serverless adalah `redshift-serverless:GetCredentials`

Riwayat terjadwal tidak ditampilkan

Pengguna IAM atau peran IAM yang digunakan untuk masuk ke AWS konsol tidak ditambahkan ke kebijakan kepercayaan peran IAM yang digunakan untuk menjadwalkan kueri.

Saat menggunakan AWS Secrets Manager kueri terjadwal untuk terhubung, konfirmasi kerahasiaan ditandai dengan kunci `RedshiftDataFullAccess`.

Jika kueri terjadwal menggunakan AWS Secrets Manager koneksi, peran IAM yang digunakan untuk menjadwalkan kueri harus memiliki kebijakan `SecretsManagerReadWrite` terkelola yang setara dengan peran tersebut.

Status riwayat kueri adalah **Failed**

Lihat tampilan sistem `SYS_QUERY_HISTORY` untuk detail tentang mengapa kueri gagal. Masalah umum adalah bahwa pengguna database atau peran yang digunakan untuk menjalankan kueri mungkin tidak memiliki hak istimewa yang diperlukan untuk menjalankan SQL. Untuk informasi selengkapnya, lihat [Mengautentikasi kueri terjadwal](#).

SQL berikut menanyakan tampilan SYS_QUERY_HISTORY untuk mengembalikan kueri yang gagal.

```
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';
```

Untuk mengetahui detail kueri terjadwal tertentu yang gagal, lihat [Menemukan detail tentang kueri terjadwal dengan AWS CloudShell](#).

Menemukan detail tentang kueri terjadwal dengan AWS CloudShell

Anda dapat menggunakan AWS CloudShell untuk mengetahui detail tentang kueri jadwal. Anda harus memiliki izin yang tepat untuk menjalankan AWS CLI perintah yang ditunjukkan dalam prosedur berikut.

Untuk melihat hasil kueri terjadwal

1. Di AWS konsol, buka prompt AWS CloudShell perintah. Untuk informasi selengkapnya AWS CloudShell, lihat [Apa yang ada AWS CloudShell](#) di Panduan AWS CloudShell Pengguna.
2. Asumsikan peran IAM dari kueri terjadwal. Untuk mengambil peran, temukan peran IAM yang terkait dengan kueri terjadwal di editor kueri v2 dan gunakan dalam AWS CLI perintah di AWS CloudShell. Misalnya, untuk peran scheduler masukkan AWS STS perintah untuk mengambil peran yang digunakan oleh kueri terjadwal.

```
aws sts assume-role --role-arn "arn:aws:iam::123456789012:role/scheduler" --role-session-name "scheduler-test"
```

Kredensi yang dikembalikan mirip dengan yang berikut ini.

```
"Credentials": {
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "SessionToken": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...",
  "Expiration": "2023-08-18T18:19:44+00:00"
},
"AssumedRoleUser": {
  "AssumedRoleId": "ARO35B2NH6WBTP70NL4E:scheduler-test",
```



```
"Arn": "arn:aws:sts::123456789012:assumed-role/scheduler/scheduler-test"
}
}
```

3. Buat variabel lingkungan dalam AWS CLI menggunakan kredensial yang ditampilkan dari asumsi peran IAM. Anda harus menggunakan token ini sebelum waktu kedaluwarsa. Misalnya, Anda memasukkan yang berikut ini AWS CloudShell.

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJa1rXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
export AWS_SESSION_TOKEN=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...
```

4. Untuk melihat kesalahan kueri yang gagal, jalankan AWS CLI perintah untuk mendeskripsikan pernyataan. Id pernyataan SQL berasal dari ID yang ditampilkan di bagian riwayat Jadwal dari kueri terjadwal di editor kueri v2.

```
aws redshift-data describe-statement --id 130d2620-05d2-439c-b7cf-815d9767f513
```

Dalam contoh ini, SQL terjadwal `select * from users limit 100` menghasilkan kesalahan SQL bahwa `users` tabel tidak ada.

```
{
  "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 penjadwalan kueri

Untuk demo penjadwalan kueri, tonton video berikut. [Demo video penjadwalan kueri](#).

Memvisualisasikan hasil kueri

Setelah Anda menjalankan kueri dan tampilan hasil, Anda dapat mengaktifkan Bagan untuk menampilkan visualisasi grafis dari halaman hasil saat ini. Anda dapat menggunakan kontrol berikut untuk menentukan konten, struktur, dan tampilan bagan Anda:



Jejak

Merupakan satu set tanda grafis terkait dalam bagan. Anda dapat menentukan beberapa jejak dalam bagan.

Tipe

Anda dapat menentukan jenis jejak untuk mewakili data sebagai salah satu dari berikut ini:

- Bagan sebar untuk plot pencar atau bagan gelembung.
- Bagan batang untuk mewakili kategori data dengan batang vertikal atau horizontal.
- Bagan area untuk menentukan area yang diisi.
- Histogram yang menggunakan bar untuk mewakili distribusi frekuensi.
- Diagram lingkaran untuk representasi melingkar data di mana setiap irisan mewakili persentase dari keseluruhan.
- Bagan Corong atau Area Corong untuk mewakili data melalui berbagai tahap proses.
- Grafik OHLC (open-high-low-close) sering digunakan untuk data keuangan untuk mewakili nilai terbuka, tinggi, rendah, dan dekat sepanjang sumbu x, yang biasanya mewakili interval waktu.
- Bagan kandil untuk mewakili rentang nilai untuk kategori di atas garis waktu.
- Bagan air terjun untuk mewakili bagaimana nilai awal meningkat atau menurun melalui serangkaian nilai menengah. Nilai dapat mewakili interval waktu atau kategori.
- Bagan garis untuk mewakili perubahan nilai dari waktu ke waktu.

Sumbu X

Anda menentukan kolom tabel yang berisi nilai-nilai untuk plot sepanjang sumbu X. Kolom yang berisi nilai deskriptif biasanya mewakili data dimensi. Kolom yang berisi nilai kuantitatif biasanya mewakili data faktual.

Sumbu Y

Anda menentukan kolom tabel yang berisi nilai-nilai untuk plot sepanjang sumbu Y. Kolom yang berisi nilai deskriptif biasanya mewakili data dimensi. Kolom yang berisi nilai kuantitatif biasanya mewakili data faktual.

Subplot

Anda dapat menentukan presentasi tambahan data bagan.

Transformasi

Anda dapat menentukan transformasi untuk memfilter data jejak. Anda menggunakan transformasi terpisah untuk menampilkan beberapa jejak dari satu jejak sumber. Anda menggunakan transformasi agregat untuk menyajikan jejak sebagai rata-rata atau minimum. Anda menggunakan transformasi semacam untuk mengurutkan jejak.

Penampilan umum

Anda dapat mengatur default untuk warna latar belakang, warna margin, skala warna untuk merancang palet, gaya dan ukuran teks, gaya dan ukuran judul, dan bilah mode. Anda dapat menentukan interaksi untuk seret, klik, dan arahkan kursor. Anda dapat menentukan teks meta. Anda dapat menentukan tampilan default untuk jejak, sumbu, legenda, dan anotasi.

Pilih Jejak untuk menampilkan hasil sebagai bagan. Untuk Type, pilih style chart sebagai Bar, Line, dan sebagainya. Untuk Orientasi, Anda dapat memilih Vertikal atau Horizontal. Untuk X, pilih kolom tabel yang ingin Anda gunakan untuk sumbu horizontal. Untuk Y, pilih kolom tabel yang ingin Anda gunakan untuk sumbu vertikal.

Pilih Segarkan untuk memperbarui tampilan bagan. Pilih Layar penuh untuk memperluas tampilan bagan.

Untuk membuat bagan

1. Jalankan kueri dan dapatkan hasil.
2. Aktifkan Bagan.
3. Pilih Trace dan mulai memvisualisasikan data Anda.
4. Pilih gaya bagan dari salah satu dari berikut ini:
 - Scatter

- Bar
 - Bidang
 - Histogram
 - Pie
 - Corong
 - Area Corong
 - OHLC (buka-tinggi-rendah-tutup)
 - Candlestick
 - Air Terjun
 - Baris
5. Pilih Gaya untuk menyesuaikan tampilan, termasuk warna, sumbu, legenda, dan anotasi. Anda dapat menambahkan teks, bentuk, dan gambar.
 6. Pilih Anotasi untuk menambahkan teks, bentuk, dan gambar.

Untuk menyimpan bagan

1. Pilih Simpan Bagan.
2. Masukkan nama untuk bagan Anda.
3. Pilih Simpan.

Untuk mengekspor bagan

1. Pilih Ekspor.
2. Pilih PNG atau JPEG.
3. Atur lebar dan tinggi untuk bagan Anda.
4. Pilih Ekspor.
5. Pilih untuk membuka file di aplikasi grafis default Anda atau menyimpan file dengan nama default.

Untuk menelusuri dan membuka bagan yang disimpan

1. Pilih tab Charts.
2. Buka grafik yang Anda inginkan.

Untuk mengatur bagan Anda ke dalam folder

1. Pilih Charts dari panel navigasi.
2. Pilih Folder baru dan beri nama folder.
3. Pilih Buat untuk membuat folder di tab Charts.

Anda dapat memindahkan grafik masuk dan keluar dari folder menggunakan drag-and-drop.

Contoh: Buat diagram lingkaran untuk memvisualisasikan hasil kueri

Contoh berikut menggunakan tabel Penjualan dari database sampel. Untuk informasi selengkapnya, lihat [Contoh database](#) di Panduan Pengembang Database Amazon Redshift.

Berikut ini adalah query yang Anda jalankan untuk memberikan data untuk pie chart.

```
select top 5 eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid group by eventname
order by 3;
```

Untuk membuat diagram lingkaran untuk acara teratas dengan total penjualan

1. Jalankan kueri.
2. Di area hasil kueri, aktifkan Bagan.
3. Pilih Jejak.
4. Untuk Jenis, pilih Pie.
5. Untuk Nilai, pilih totalsales.
6. Untuk Label, pilih eventname.
7. Pilih Style dan kemudian General.
8. Di bawah Colorscales, pilih Categorical dan kemudian Pastel2.



Contoh: Buat bagan kombinasi untuk membandingkan pendapatan dan penjualan

Lakukan langkah-langkah dalam contoh ini untuk membuat bagan yang menggabungkan diagram batang untuk data pendapatan dan grafik garis untuk data penjualan. Contoh berikut menggunakan tabel Penjualan database sampel tickit. Untuk informasi selengkapnya, lihat [Contoh database](#) di Panduan Pengembang Database Amazon Redshift.

Berikut ini adalah query yang Anda jalankan untuk memberikan data untuk grafik.

```
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;
```

Untuk membuat bagan kombinasi untuk membandingkan pendapatan dan penjualan

1. Jalankan kueri.
2. Di area hasil kueri, aktifkan Bagan.
3. Di bawah jejak o, untuk Jenis, pilih Bar.
4. Untuk X, pilih eventname.
5. Untuk Y, pilih total_price.

Bagan batang ditampilkan dengan nama acara di sepanjang sumbu X.

6. Di bawah Gaya, pilih Jejak.
7. Untuk Nama, masukkan Pendapatan.
8. Di bawah Style, pilih Axes.
9. Untuk Judul, pilih Y dan masukkan Pendapatan.

Label Pendapatan ditampilkan pada sumbu Y kiri.

10. Di bawah Struktur, pilih Jejak.
11. Pilih
+
Jejak.

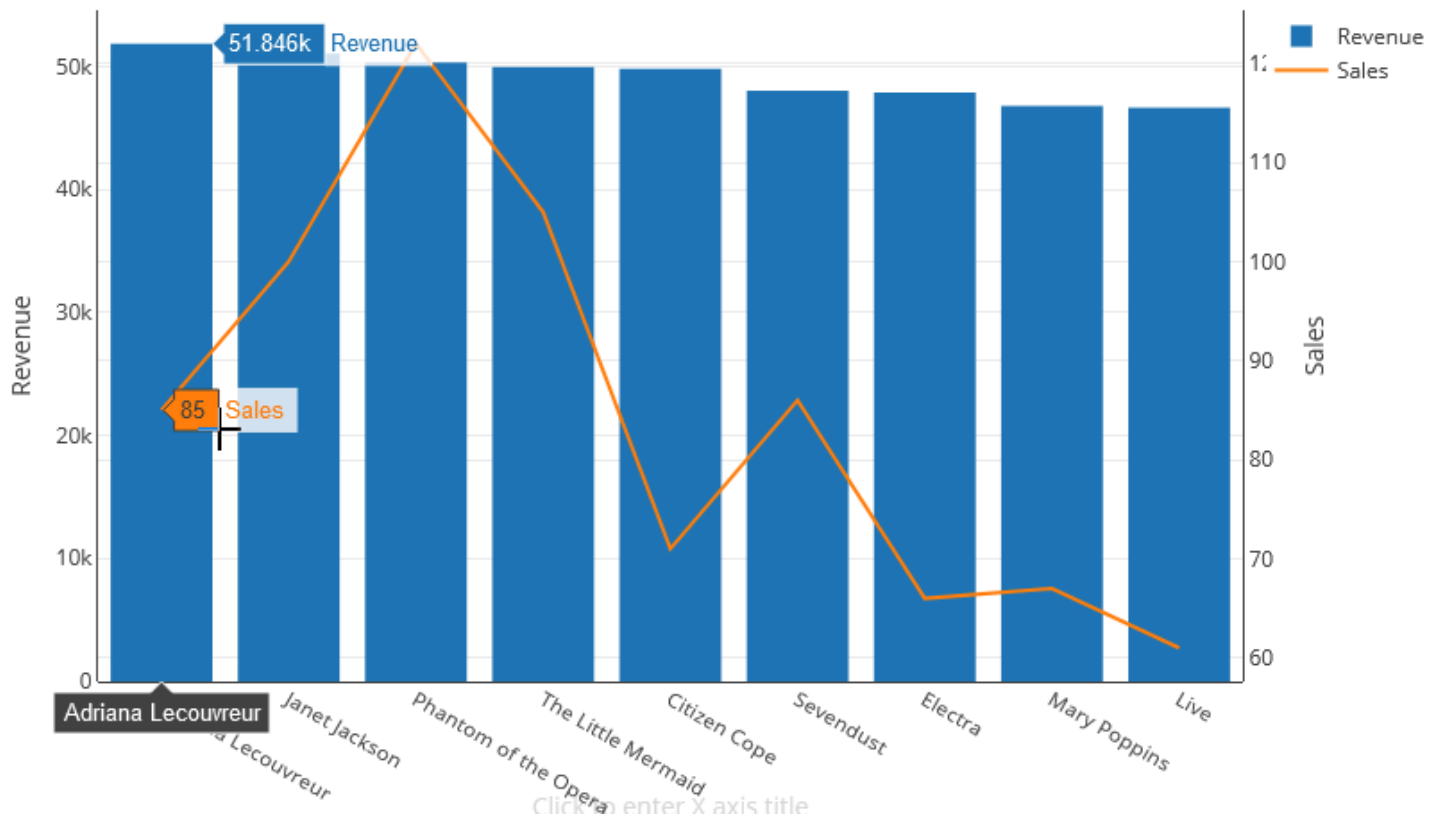
Tampilan opsi jejak 1.

12. Untuk Type, pilih Line.
13. Untuk X, pilih eventname.
14. Untuk Y, pilih total_qty_sold.
15. Di bawah Sumbu Untuk Digunakan, untuk Sumbu Y
pilih +

Sumbu Y menampilkan Y2.

16. Di bawah Style, pilih Axes.
17. Di bawah Judul, pilih Y2.
18. Untuk Nama, masukkan Penjualan.
19. Di bawah Garis, pilih Y: Penjualan.
20. Di bawah Garis Sumbu, pilih Tampilkan dan untuk Posisi, pilih Kanan.

Revenue and Sales



Demo: Bangun visualisasi menggunakan editor kueri Amazon Redshift v2

Untuk demo tentang cara membangun visualisasi, tonton video berikut. [Buat visualisasi menggunakan editor kueri Amazon Redshift v2.](#)

Berkolaborasi dan berbagi sebagai sebuah tim

Anda dapat berbagi pertanyaan dengan tim Anda.

Tim didefinisikan untuk sekumpulan pengguna yang berkolaborasi dan berbagi sumber daya editor kueri v2. Administrator dapat membuat tim dengan menambahkan tag ke peran IAM. Untuk informasi selengkapnya, lihat [Izin yang diperlukan untuk menggunakan editor kueri v2](#).

Menyimpan, menelusuri, dan menghapus kueri

Sebelum Anda dapat membagikan kueri Anda dengan tim Anda, simpan kueri Anda. Anda dapat melihat dan menghapus kueri yang disimpan.

Untuk menyimpan kueri

1. Siapkan kueri Anda dan pilih Simpan.
2. Masukkan judul untuk kueri Anda.
3. Pilih Simpan.

Untuk menelusuri kueri yang disimpan

1. Pilih Kueri dari panel navigasi.
2. Anda dapat melihat kueri yang merupakan kueri Saya, Dibagikan oleh saya, atau Dibagikan ke tim saya. Kueri ini dapat muncul sebagai kueri individual atau dalam folder yang Anda buat.

Untuk menghapus kueri yang disimpan

1. Buka menu konteks (klik kanan) untuk kueri yang disimpan.
2. Pilih Hapus dan konfirmasi tindakan.

Untuk mengatur kueri yang disimpan ke dalam folder

1. Pilih Kueri dari panel navigasi.
2. Pilih Folder baru dan beri nama folder.
3. Pilih Buat untuk membuat folder di tab Kueri.

Anda sekarang dapat memindahkan kueri masuk dan keluar dari folder menggunakan drag-and-drop.

Berbagi kueri

Anda dapat membagikan pertanyaan Anda dengan tim Anda. Anda juga dapat melihat riwayat kueri yang disimpan dan mengelola versi kueri.

Untuk berbagi kueri dengan tim Anda, pastikan bahwa Anda memiliki tag utama yang `sqlworkbench-team` disetel ke nilai yang sama dengan anggota tim lainnya di akun Anda. Misalnya, administrator mungkin menetapkan nilai `accounting-team` untuk semua orang di departemen akuntansi. Sebagai contoh, lihat [Izin yang diperlukan untuk menggunakan editor kueri v2](#).

Untuk berbagi kueri dengan tim

1. Pilih Kueri dari panel navigasi.
2. Buka menu konteks (klik kanan) kueri yang ingin Anda bagikan dan pilih Bagikan dengan tim saya.
3. Pilih tim atau tim yang ingin Anda bagikan kueri, lalu pilih opsi Simpan berbagi.

Setiap kali Anda menyimpan kueri SQL, editor kueri v2 menyimpannya sebagai versi baru. Anda dapat menelusuri versi kueri sebelumnya, menyimpan salinan kueri, atau memulihkan kueri.

Untuk mengelola versi kueri

1. Pilih Kueri dari panel navigasi.
2. Buka menu konteks (klik kanan) untuk kueri yang ingin Anda kerjakan.
3. Pilih Riwayat versi untuk membuka daftar versi kueri.
4. Pada halaman Riwayat versi, Anda dapat melakukan hal berikut:
 - Kembalikan ke yang dipilih - Kembalikan ke versi yang dipilih dan lanjutkan pekerjaan Anda dengan versi ini.
 - Simpan dipilih sebagai — Buat kueri baru di editor.

Menanyakan database menggunakan editor kueri

Menggunakan editor kueri adalah cara mudah untuk menjalankan kueri pada database yang dihosting oleh cluster Amazon Redshift Anda. Setelah membuat klaster, Anda dapat langsung menjalankan kueri dengan menggunakan editor kueri di konsol Amazon Redshift.

Note

Anda tidak dapat menanyakan data di Amazon Redshift Tanpa Server menggunakan editor kueri asli ini. Gunakan editor kueri Amazon Redshift v2 sebagai gantinya.

Pada Februari 2021, editor kueri yang diperbarui telah diterapkan dan izin otorisasi untuk menggunakan editor kueri diubah. Editor kueri baru menggunakan Amazon Redshift Data API untuk menjalankan kueri. `AmazonRedshiftQueryEditorKebijakan`, yang merupakan

kebijakan AWS terkelola AWS Identity and Access Management (IAM), telah diperbarui untuk menyertakan izin yang diperlukan. Jika Anda memiliki kebijakan IAM khusus, pastikan Anda memperbaruinya. Gunakan `AmazonRedshiftQueryEditor` sebagai panduan. Perubahan untuk `AmazonRedshiftQueryEditor` mencakup yang berikut:

- Izin untuk mengelola hasil pernyataan editor kueri memerlukan pengguna pemilik pernyataan.
- Izin untuk menggunakan Secrets Manager untuk terhubung ke database telah ditambahkan.

Untuk informasi selengkapnya, lihat [Izin diperlukan untuk menggunakan editor kueri konsol Amazon Redshift](#).

Ketika Anda terhubung ke cluster Anda dari editor kueri baru, Anda dapat menggunakan salah satu dari dua metode otentikasi, seperti yang dijelaskan dalam [Menghubungkan dengan editor kueri](#).

Menggunakan editor kueri, Anda dapat melakukan hal berikut:

- Jalankan kueri pernyataan SQL tunggal.
- Hasil unduhan menetapkan sebesar 100 MB ke file nilai dipisahkan koma (CSV).
- Simpan kueri untuk digunakan kembali. Anda tidak dapat menyimpan kueri di Wilayah Eropa (Paris), Wilayah Asia Pasifik (Osaka), Wilayah Asia Pasifik (Hong Kong), atau Wilayah Timur Tengah (Bahrain).
- Lihat detail runtime kueri untuk tabel yang ditentukan pengguna.
- Jadwalkan kueri untuk dijalankan di masa depan.
- Lihat riwayat kueri yang Anda buat di editor kueri.
- Jalankan kueri terhadap cluster menggunakan perutean VPC yang disempurnakan.

Pertimbangan editor kueri

Pertimbangkan hal berikut tentang bekerja dengan kueri saat Anda menggunakan editor kueri:

- Durasi maksimum kueri adalah 24 jam.
- Ukuran hasil kueri maksimum adalah 100 MB. Jika panggilan mengembalikan lebih dari 100 MB data respons, panggilan akan dihentikan.
- Waktu retensi maksimum untuk hasil kueri adalah 24 jam.
- Ukuran pernyataan kueri maksimum adalah 100 KB.

- Cluster harus berada di cloud pribadi virtual (VPC) berdasarkan layanan Amazon VPC.
- Anda tidak dapat menggunakan transaksi di editor kueri. Untuk informasi selengkapnya tentang transaksi, lihat [MULAI](#) di Panduan Pengembang Database Amazon Redshift.
- Anda dapat menyimpan kueri hingga 3.000 karakter.

Mengaktifkan akses ke editor kueri

Untuk mengakses editor kueri, Anda memerlukan izin. Untuk mengaktifkan akses, kami menyarankan Anda melampirkan kebijakan `AmazonRedshiftQueryEditor` dan `AmazonRedshiftReadOnlyAccess` AWS terkelola untuk izin IAM ke peran IAM yang Anda gunakan untuk mengakses klaster Anda. Kemudian, Anda dapat menetapkan peran ke pengguna. Anda dapat menggunakan konsol IAM (<https://console.aws.amazon.com/iam/>) untuk melampirkan kebijakan IAM. Untuk informasi selengkapnya, lihat [Menggunakan kebijakan berbasis identitas \(kebijakan IAM\) untuk Amazon Redshift](#).

Jika Anda telah membuat pengguna untuk mengakses Amazon Redshift, Anda dapat melampirkan kebijakan `AmazonRedshiftQueryEditor` dan `AmazonRedshiftReadOnlyAccess` AWS terkelola ke pengguna tersebut melalui peran yang ditetapkan. Jika Anda belum membuat pengguna, buat dan lampirkan kebijakan ke peran IAM dan tetapkan peran tersebut ke pengguna.

Kebijakan AWS terkelola `AmazonRedshiftQueryEditor` memungkinkan tindakan `redshift:GetClusterCredentials`, yang secara default memberikan akses superuser ke database. Untuk membatasi akses, Anda dapat melakukan salah satu hal berikut:

- Buat kebijakan kustom yang memungkinkan pemanggilan `redshift:GetClusterCredentials` dan batasi sumber daya ke nilai tertentu. `DbUser`
- Tambahkan kebijakan yang menolak izin. `redshift:GetClusterCredentials` Setiap pengguna yang diberi peran dengan izin terlampir ini harus masuk ke editor kueri dengan kredensi sementara. Kebijakan penolakan ini menggambarkan contohnya.

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

Untuk informasi selengkapnya tentang membuat peran dengan izin yang diperlukan, lihat [Buat peran IAM dengan izin untuk memanggil GetClusterCredentials](#).

Setiap pengguna yang diberikan akses ke editor kueri Amazon Redshift melalui kebijakan AWS terkelola `AmazonRedshiftQueryEditor` dapat mencantumkan semua rahasia. Namun, kebijakan ini memungkinkan pembuatan dan pengambilan hanya rahasia yang ditandai dengan kunci `RedshiftQueryOwner` dan nilainya. `${aws:userid}` Jika Anda membuat kunci dari editor kueri Amazon Redshift, kuncinya akan ditandai secara otomatis. Untuk menggunakan rahasia yang tidak dibuat dengan editor kueri Amazon Redshift, konfirmasi bahwa rahasia tersebut ditandai dengan kunci `RedshiftQueryOwner` dan nilai pengenal pengguna IAM unik Anda, misalnya, `AIDACKCEVSQ6C2EXAMPLE`

Izin yang diperlukan untuk menggunakan editor `AmazonRedshiftQueryEditor` kueri Amazon Redshift adalah `AmazonRedshiftReadOnlyAccess`

Untuk memberikan akses, tambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

Buat rangkaian izin. Ikuti petunjuk dalam [Buat set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

Buat peran untuk federasi identitas. Ikuti petunjuk dalam [Membuat peran untuk penyedia identitas pihak ketiga \(federasi\)](#) di Panduan Pengguna IAM.

- Pengguna IAM:

- Buat peran yang dapat diambil pengguna Anda. Ikuti petunjuk dalam [Membuat peran untuk pengguna IAM](#) dalam Panduan Pengguna IAM.
- (Tidak disarankan) Pasang kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk di [Menambahkan izin ke pengguna \(konsol\)](#) dalam Panduan Pengguna IAM.

Menghubungkan dengan editor kueri

Saat Anda terhubung ke cluster dengan editor kueri, Anda menggunakan salah satu metode otentikasi berikut. Setiap metode memerlukan kombinasi input yang berbeda dari konsol Amazon Redshift.

AWS Secrets Manager

Dengan metode ini, berikan nilai rahasia untuk `rahasia-arn` yang disimpan di AWS Secrets Manager. Rahasia ini berisi kredensial untuk terhubung ke database Anda.

Kredensial sementara

Dengan metode ini, berikan database dan nilai `db-user` Anda.

Menyimpan kredensi database di AWS Secrets Manager

Saat Anda memanggil editor kueri, Anda dapat meneruskan kredensial untuk cluster dengan menggunakan rahasia di AWS Secrets Manager. Untuk meneruskan kredensial dengan cara ini, Anda menentukan nama atau Nama Sumber Daya Amazon (ARN) dari rahasia tersebut.

Untuk informasi selengkapnya tentang izin minimum, lihat [Membuat dan Mengelola Rahasia dengan AWS Secrets Manager](#) di Panduan AWS Secrets Manager Pengguna.

Untuk menyimpan kredensial Anda secara rahasia untuk cluster Amazon Redshift

1. Gunakan AWS Secrets Manager untuk membuat rahasia yang berisi kredensial untuk cluster. Saat Anda memilih Simpan rahasia baru, pilih `Credentials for Redshift cluster`. Simpan nilai untuk nama Pengguna (pengguna database), Kata Sandi, dan cluster DB (pengidentifikasi cluster) dalam rahasia Anda.

Untuk instruksi, lihat [Membuat Rahasia Basic](#) di Panduan Pengguna AWS Secrets Manager .

2. Gunakan AWS Secrets Manager konsol untuk melihat detail rahasia yang Anda buat, atau jalankan `aws secretsmanager describe-secret` AWS CLI perintah.

Jika Anda memilih untuk menggunakan kredensial admin kluster AWS Secrets Manager, Anda dapat terhubung ke database menggunakan kredensial admin tersimpan Secrets Manager.

Menggunakan editor kueri

Dalam contoh berikut, Anda menggunakan editor kueri untuk melakukan tugas-tugas berikut:

- Jalankan perintah SQL.
- Lihat detail eksekusi kueri.
- Simpan kueri.

- Unduh set hasil kueri.

Untuk melengkapi contoh berikut, Anda memerlukan cluster Amazon Redshift yang ada. Jika Anda tidak memiliki cluster, buat satu dengan mengikuti prosedur yang dijelaskan di [Membuat klaster](#).

Untuk menggunakan editor kueri di konsol Amazon Redshift

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Editor kueri, lalu sambungkan ke database di cluster Anda.
3. Untuk Skema, pilih publik untuk membuat tabel baru berdasarkan skema itu.
4. Masukkan yang berikut ini di jendela editor kueri dan pilih Jalankan untuk membuat tabel baru.

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

5. Pilih Clear.
6. Masukkan perintah berikut di jendela editor kueri, dan pilih Jalankan untuk menambahkan baris ke tabel.

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

7. Pilih Clear.
8. Masukkan perintah berikut di jendela editor kueri dan pilih Jalankan untuk menanyakan tabel baru.

```
select * from shoes;
```

Hasil Query menampilkan hasilnya.

Jenis sepatu	Warna
sandal	hitam

Jenis sepatu	Warna
sepatu pantofel	cokelat

9. Pilih Eksekusi untuk melihat detail proses.
10. Pilih Data, lalu Ekspor untuk mengunduh hasil kueri sebagai file.

Menjadwalkan kueri

Important

Editor kueri Amazon Redshift v2 sekarang mendukung penjadwalan kueri. Kami merekomendasikan menggunakan editor kueri v2. Untuk informasi selengkapnya, lihat [Menjadwalkan kueri dengan editor kueri v2](#).

Untuk membuat jadwal untuk menjalankan pernyataan SQL, Anda dapat menggunakan editor kueri di konsol Amazon Redshift. Anda dapat membuat jadwal untuk menjalankan pernyataan SQL Anda pada interval waktu yang sesuai dengan kebutuhan bisnis Anda. Ketika tiba waktunya untuk menjalankan kueri terjadwal, Amazon EventBridge memulai kueri.

Untuk membuat jadwal untuk menjalankan pernyataan SQL

1. Buka konsol dan editor kueri seperti yang dijelaskan dalam [Menggunakan editor kueri](#). Anda hanya dapat menggunakan editor kueri ini dengan kluster yang disediakan.
2. Pilih Jadwal untuk membuat jadwal untuk menjalankan pernyataan SQL.

Ketika Anda menentukan jadwal, Anda memberikan informasi berikut:

- Peran IAM yang digunakan untuk mengasumsikan izin yang diperlukan untuk menjalankan kueri. Untuk informasi selengkapnya, lihat [Menyiapkan izin untuk menjadwalkan kueri](#).
- Nilai otentikasi untuk salah satu AWS Secrets Manager atau kredensi sementara untuk mengotorisasi akses kluster Anda. Untuk informasi selengkapnya, lihat [Mengautentikasi kueri terjadwal](#).
- Nama query terjadwal dan pernyataan SQL tunggal yang akan dijalankan.
- Frekuensi jadwal dan opsi pengulangan atau nilai yang diformat cron.

- Secara opsional, Anda dapat mengaktifkan notifikasi Amazon SNS untuk memantau kueri terjadwal. Jika kueri Anda sedang dijalankan tetapi Anda tidak melihat pesan yang dipublikasikan di topik SNS Anda, lihat [Aturan saya sedang dipicu tetapi saya tidak melihat pesan apa pun yang dipublikasikan ke topik Amazon SNS saya](#) di Panduan Pengguna EventBridge Amazon.

Anda juga dapat mengelola dan memperbarui kueri terjadwal menggunakan konsol Amazon Redshift. Bergantung pada versi konsol Anda, kueri terjadwal mungkin dicantumkan di tempat berikut:

- Pada tab Jadwal halaman detail klaster Anda.
- Pada tab Kueri terjadwal dari editor kueri.

Jika Anda memilih nama Jadwal dari salah satu lokasi ini, Anda dapat melihat dan mengedit definisi kueri terjadwal.

Menyiapkan izin untuk menjadwalkan kueri di konsol Amazon Redshift

Untuk menjadwalkan kueri, pengguna AWS Identity and Access Management (IAM) yang menentukan jadwal dan peran IAM yang terkait dengan jadwal harus dikonfigurasi sebagai berikut.

Untuk pengguna IAM yang masuk ke konsol Amazon Redshift, lakukan hal berikut:

- Lampirkan kebijakan `AmazonEventBridgeFullAccess` AWS terkelola ke peran IAM.
- Lampirkan kebijakan dengan `sts:AssumeRole` izin peran IAM yang Anda tentukan saat Anda menentukan pernyataan SQL terjadwal.

Contoh berikut menunjukkan kebijakan yang mengasumsikan peran IAM tertentu.

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

Untuk peran IAM yang Anda tentukan untuk mengaktifkan penjadwal menjalankan kueri, lakukan hal berikut:

- Pastikan bahwa peran IAM ini menentukan prinsip EventBridge layanan (`events.amazonaws.com`). Berikut ini adalah contoh hubungan kepercayaan.

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

Untuk informasi selengkapnya tentang cara membuat peran IAM untuk EventBridge acara, lihat [izin diperlukan untuk menggunakan penjadwal Amazon EventBridge](#).

- Lampirkan kebijakan `AmazonRedshiftDataFullAccess` AWS terkelola ke peran IAM.
- Untuk memungkinkan pengguna melihat riwayat jadwal, edit peran IAM untuk menambahkan `sts:AssumeRole` izin.

Berikut ini adalah contoh kebijakan kepercayaan dalam peran IAM.

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

```
    }  
  ]  
}
```

Mengautentikasi kueri terjadwal

Saat menjadwalkan kueri, Anda menggunakan salah satu metode otentikasi berikut saat kueri SQL berjalan. Setiap metode memerlukan kombinasi input yang berbeda dari konsol Amazon Redshift.

AWS Secrets Manager

Dengan metode ini, berikan nilai rahasia untuk `rahasia-arn` yang disimpan di AWS Secrets Manager. Rahasia ini berisi kredensial untuk terhubung ke database Anda. Rahasiannya harus ditandai dengan kunci `RedshiftDataFullAccess`.

Untuk informasi selengkapnya tentang izin minimum, lihat [Membuat dan Mengelola Rahasia dengan AWS Secrets Manager](#) di Panduan AWS Secrets Manager Pengguna.

Kredensial sementara

Dengan metode ini, berikan database dan nilai `db-user` Anda.

`AmazonRedshiftDataFullAccessKebijakan` ini memungkinkan `redshift_data_api_user` izin nama pengguna database untuk `redshift:GetClusterCredentials`. Jika Anda ingin menggunakan pengguna database yang berbeda untuk menjalankan pernyataan SQL, tambahkan kebijakan ke peran IAM untuk mengizinkan `redshift:GetClusterCredentials`. Contoh kebijakan berikut memungkinkan pengguna database `awsuser` dan `myuser`.

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

Buat EventBridge aturan Amazon yang berjalan saat kueri selesai

Anda dapat membuat aturan acara untuk mengirim pemberitahuan saat kueri selesai. Untuk prosedur menggunakan EventBridge konsol Amazon, lihat [Membuat EventBridge aturan Amazon yang bereaksi terhadap peristiwa](#) di Panduan EventBridge Pengguna Amazon. Untuk informasi selengkapnya tentang pola peristiwa, lihat [pola EventBridge peristiwa Amazon](#) di Panduan EventBridge Pengguna Amazon.

Misalnya, contoh peristiwa berikut dikirim ketika kueriFINISHED.

```
{
  "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
  }
}
```

Anda dapat membuat aturan pola acara untuk memfilter acara.

```
{
  "source": [
    "aws.redshift-data"
  ],
  "detail-type": [
    "Redshift Data Statement Status Change"
  ],
}
```

```
"detail": {
  "state": [
    "FINISHED"
  ]
}
```

Menyambung ke gudang data Amazon Redshift menggunakan alat klien SQL

Anda dapat terhubung ke gudang data Amazon Redshift dari alat klien SQL melalui koneksi Java Database Connectivity (JDBC), Python, dan Open Database Connectivity (ODBC). Amazon Redshift tidak menyediakan atau menginstal alat atau pustaka klien SQL apa pun. Untuk menggunakan alat atau pustaka ini untuk bekerja dengan data di gudang data Anda, instal di komputer klien Anda atau instans Amazon EC2. Anda dapat menggunakan sebagian besar alat klien SQL yang mendukung driver JDBC, Python, atau ODBC.

Gunakan daftar bagian di akhir topik ini untuk membantu Anda menelusuri proses mengonfigurasi komputer klien atau instans Amazon EC2 untuk menggunakan koneksi JDBC, Python, atau ODBC. Topik juga membahas opsi keamanan terkait untuk koneksi klien ke server. [Selain itu, temukan informasi tentang pengaturan dan koneksi dari alat klien SQL, seperti SQL Workbench/J, alat pihak ketiga, dan Amazon Redshift RSQL.](#) Anda dapat mencoba alat ini jika Anda belum memiliki alat intelijen bisnis untuk digunakan. Anda juga dapat menggunakan bagian ini untuk mempelajari tentang menghubungkan ke gudang data Anda secara terprogram. Terakhir, jika Anda mengalami masalah saat mencoba terhubung ke gudang data Anda, Anda dapat meninjau informasi pemecahan masalah untuk mengidentifikasi solusi.

Rekomendasi untuk menghubungkan dengan alat klien

Jika Anda terhubung ke kluster Redshift Anda menggunakan alamat IP, itu dapat mengakibatkan downtime tambahan ketika ada pemadaman atau kehilangan koneksi dan cluster dibawa online di Availability Zone (AZ) baru. Namun, jika Anda masih ingin aplikasi Anda terhubung ke Redshift menggunakan alamat IP, gunakan alamat IP pribadi yang dilampirkan ke titik akhir cluster (virtual-private-cloud VPC). Anda dapat menemukan ini di detail cluster di Jaringan dan keamanan, di bawah tab Properties.

Note

Jika aplikasi Anda menggunakan alamat IP node pemimpin untuk mengakses kluster Redshift, praktik terbaik yang disarankan adalah mengubahnya untuk menggunakan URL titik akhir cluster. Untuk informasi selengkapnya, lihat [Mengonfigurasi koneksi di Amazon Redshift](#).

Topik

- [Mengonfigurasi koneksi di Amazon Redshift](#)
- [Mengkonfigurasi opsi keamanan untuk koneksi](#)
- [Menghubungkan dari alat dan kode klien](#)
- [Menghubungkan dengan SQL Workbench/J](#)
- [Connect ke gudang data Anda secara terprogram](#)
- [Menggunakan profil otentikasi untuk terhubung ke Amazon Redshift](#)
- [Memecahkan masalah koneksi di Amazon Redshift](#)

Mengonfigurasi koneksi di Amazon Redshift

Di bagian berikut, pelajari cara mengkonfigurasi koneksi JDBC, Python, dan ODBC untuk terhubung ke cluster Anda dari alat klien SQL. Bagian ini menjelaskan cara mengatur koneksi JDBC, Python, dan ODBC. Ini juga menjelaskan cara menggunakan Secure Sockets Layer (SSL) dan sertifikat server untuk mengenkripsi komunikasi antara klien dan server.

Driver JDBC, Python, dan ODBC untuk Amazon Redshift

Untuk bekerja dengan data di cluster Anda, Anda harus memiliki driver JDBC, Python, atau ODBC untuk konektivitas dari komputer klien atau instance Anda. Kode aplikasi Anda untuk menggunakan operasi API akses data JDBC, Python, atau ODBC, dan gunakan alat klien SQL yang mendukung JDBC, Python, atau ODBC.

Amazon Redshift menawarkan driver JDBC, Python, dan ODBC untuk diunduh. Driver ini didukung oleh AWS Support. Driver PostgreSQL tidak diuji dan tidak didukung oleh tim Amazon Redshift. Gunakan driver khusus Amazon Redshift saat menyambungkan ke kluster Amazon Redshift. Driver Amazon Redshift memiliki keuntungan sebagai berikut:

- Support untuk IAM, SSO, dan otentikasi federasi.
- Support untuk tipe data Amazon Redshift baru.
- Support untuk profil otentikasi.
- Peningkatan kinerja dalam hubungannya dengan peningkatan Amazon Redshift.

Untuk informasi selengkapnya tentang cara mengunduh driver JDBC dan ODBC dan mengonfigurasi koneksi ke cluster Anda, lihat [Mengkonfigurasi koneksi untuk driver JDBC versi 2.1 untuk Amazon Redshift](#), [Mengonfigurasi konektor Amazon Redshift Python](#) dan [Mengkonfigurasi koneksi ODBC](#)

Untuk informasi selengkapnya tentang mengelola identitas IAM, termasuk praktik terbaik untuk peran IAM, lihat [Manajemen identitas dan akses di Amazon Redshift](#)

Menemukan string koneksi cluster Anda

Untuk terhubung ke cluster Anda dengan alat klien SQL Anda, Anda harus memiliki string koneksi cluster. Anda dapat menemukan string koneksi cluster di konsol Amazon Redshift, di halaman detail cluster.

Untuk menemukan string koneksi untuk sebuah cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, lalu pilih nama cluster dari daftar untuk membuka detailnya.
3. String koneksi URL JDBC dan URL ODBC tersedia, bersama dengan detail tambahan, di bagian Informasi umum. Setiap string didasarkan pada AWS Wilayah tempat cluster berjalan. Klik ikon di sebelah string koneksi yang sesuai untuk menyalinnya.

Untuk menyambung ke titik akhir klaster, Anda dapat menggunakan URL titik akhir klaster dari permintaan [DescribeClusters API](#). Berikut ini adalah contoh URL endpoint cluster.

```
mycluster.cmeaswqeuae.us-east-2.redshift.amazonaws.com
```

Jika Anda telah menyiapkan nama domain khusus untuk klaster Anda, Anda juga dapat menggunakannya untuk terhubung ke klaster Anda. Untuk informasi selengkapnya tentang membuat nama domain kustom, lihat [Menyiapkan nama domain kustom](#).

Note

Saat Anda terhubung, jangan gunakan alamat IP node cluster atau alamat IP titik akhir VPC. Selalu gunakan titik akhir Redshift untuk menghindari pemadaman yang tidak perlu. Satu-satunya pengecualian untuk menggunakan URL endpoint adalah ketika Anda menggunakan nama domain khusus. Untuk informasi selengkapnya, lihat [Menggunakan nama domain khusus untuk koneksi klien](#).

Mengkonfigurasi koneksi untuk driver JDBC versi 2.1 untuk Amazon Redshift

Anda dapat menggunakan koneksi driver JDBC versi 2.1 untuk terhubung ke cluster Amazon Redshift Anda dari banyak alat klien SQL pihak ketiga. Konektor Amazon Redshift JDBC menyediakan solusi open source. Anda dapat menelusuri kode sumber, meminta penyempurnaan, melaporkan masalah, dan memberikan kontribusi.

Untuk menggunakan koneksi JDBC, lihat bagian berikut.

Topik

- [Unduh driver Amazon Redshift JDBC, versi 2.1](#)
- [Menginstal driver Amazon Redshift JDBC, versi 2.1](#)
- [Mendapatkan URL JDBC](#)
- [Membangun URL koneksi](#)
- [Mengkonfigurasi keepalives TCP untuk koneksi JDBC Anda](#)
- [Mengkonfigurasi koneksi JDBC Anda dengan Apache Maven](#)
- [Mengkonfigurasi otentikasi dan SSL](#)
- [Mengkonfigurasi logging](#)
- [Mengonversi tipe data](#)
- [Menggunakan dukungan pernyataan yang disiapkan](#)
- [Perbedaan antara versi 2.1 dan 1.x dari driver JDBC](#)
- [Membuat file inisialisasi \(.ini\) untuk driver JDBC versi 2.1](#)
- [Opsi untuk konfigurasi driver JDBC versi 2.1](#)
- [Versi sebelumnya dari JDBC driver version 2.1](#)

Unduh driver Amazon Redshift JDBC, versi 2.1

Amazon Redshift menawarkan driver untuk alat yang kompatibel dengan JDBC 4.2 API. Nama kelas untuk pengemudi ini adalah `com.amazon.redshift.Driver`.

Untuk informasi rinci tentang cara menginstal driver JDBC, referensi perpustakaan driver JDBC, dan mendaftarkan kelas driver, lihat topik berikut.

Untuk setiap komputer tempat Anda menggunakan driver Amazon Redshift JDBC versi 2.1, pastikan Java Runtime Environment (JRE) 8.0 diinstal.

Jika Anda menggunakan driver Amazon Redshift JDBC untuk otentikasi database, pastikan Anda memiliki AWS SDK for Java 1.11.118 atau yang lebih baru di jalur kelas Java Anda. Jika Anda belum AWS SDK for Java menginstal, unduh file ZIP dengan pustaka yang bergantung pada driver dan driver yang kompatibel dengan JDBC 4.2 untuk SDK: AWS

- [JDBC 4.2—driver yang kompatibel dengan versi 2.1 dan pustaka yang bergantung pada driver AWS SDK Di Wilayah China \(Beijing\)](#), gunakan tautan berikut: [JDBC 4.2—driver yang kompatibel dengan versi 2.1 dan pustaka bergantung pada driver SDK AWS](#)

File ZIP ini berisi driver yang kompatibel dengan JDBC 4.2 versi 2.1 dan file pustaka yang bergantung pada driver SDK for AWS Java 1.x. Buka zip file jar dependen ke lokasi yang sama dengan driver JDBC. Hanya driver JDBC yang perlu berada di CLASSPATH.

File ZIP ini tidak menyertakan AWS SDK for Java 1.x lengkap. Namun, ini mencakup pustaka yang bergantung pada driver AWS SDK for Java 1.x yang diperlukan AWS Identity and Access Management untuk otentikasi database (IAM).

Gunakan driver Amazon Redshift JDBC ini dengan AWS SDK yang diperlukan untuk autentikasi database IAM.

Untuk menginstal AWS SDK for Java 1.x lengkap, [AWS lihat SDK for Java](#) AWS SDK for Java 1.x di Panduan Pengembang.

- [Driver yang kompatibel dengan JDBC 4.2 versi 2.1 \(tanpa AWS SDK\) Di Wilayah China \(Beijing\)](#), gunakan tautan berikut: [JDBC 4.2—driver](#) kompatibel dengan versi 2.1 (tanpa SDK) AWS

Tinjau lisensi perangkat lunak driver JDBC versi 2.1 dan ubah file log:

- [Lisensi driver JDBC versi 2.1](#)
- [Driver JDBC versi 2.1 mengubah log](#)

Driver JDBC versi 1.2.27.1051 dan yang lebih baru mendukung prosedur tersimpan Amazon Redshift. Untuk informasi selengkapnya, lihat [Membuat prosedur tersimpan di Amazon Redshift](#) di Panduan Pengembang Database Amazon Redshift.

Menginstal driver Amazon Redshift JDBC, versi 2.1

Untuk menginstal Amazon Redshift JDBC 4.2—driver yang kompatibel versi 2.1 dan library yang bergantung pada driver untuk AWS SDK, ekstrak file dari arsip ZIP ke direktori pilihan Anda.

Untuk menginstal driver yang kompatibel dengan Amazon Redshift JDBC 4.2 versi 2.1 (tanpa AWS SDK), salin file JAR ke direktori pilihan Anda.

Untuk mengakses penyimpanan data Amazon Redshift menggunakan driver Amazon Redshift JDBC, Anda perlu melakukan konfigurasi seperti yang dijelaskan berikut.

Topik

- [Mereferensikan pustaka driver JDBC](#)
- [Mendaftarkan kelas pengemudi](#)

Mereferensikan pustaka driver JDBC

Aplikasi JDBC atau kode Java yang Anda gunakan untuk terhubung ke data Anda harus mengakses file JAR driver. Dalam aplikasi atau kode, tentukan semua file JAR yang Anda ekstrak dari arsip ZIP.

Menggunakan driver dalam aplikasi JDBC

Aplikasi JDBC biasanya menyediakan serangkaian opsi konfigurasi untuk menambahkan daftar file pustaka driver. Gunakan opsi yang disediakan untuk menyertakan semua file JAR dari arsip ZIP sebagai bagian dari konfigurasi driver dalam aplikasi. Untuk informasi selengkapnya, lihat dokumentasi untuk aplikasi JDBC Anda.

Menggunakan driver dalam kode Java

Anda harus menyertakan semua file pustaka driver di jalur kelas. Ini adalah jalur yang Java Runtime Environment mencari kelas dan file sumber daya lainnya. Untuk informasi selengkapnya, lihat dokumentasi Java SE yang sesuai untuk mengatur jalur kelas untuk sistem operasi Anda.

- **Jendela:** <https://docs.oracle.com/javase/7/docs/technotes/tools/windows/classpath.html>
- **Linux dan Solaris:** <https://docs.oracle.com/javase/7/docs/technotes/tools/solaris/classpath.html>
- **macOS:** Jalur kelas macOS default adalah direktori tempat driver JDBC diinstal.

Mendaftarkan kelas pengemudi

Pastikan Anda mendaftarkan kelas yang sesuai untuk aplikasi Anda. Anda menggunakan kelas berikut untuk menghubungkan driver Amazon Redshift JDBC ke penyimpanan data Amazon Redshift:

- Driver kelas diperluas `java.sql.Driver`.
- DataSource kelas diperluas `javax.sql.DataSource` dan `javax.sql.ConnectionPoolDataSource`.

Driver mendukung nama kelas berkualifikasi penuh berikut yang independen dari versi JDBC:

- `com.amazon.redshift.jdbc.Driver`
- `com.amazon.redshift.jdbc.DataSource`

Contoh berikut menunjukkan bagaimana menggunakan DriverManager kelas untuk membuat koneksi untuk JDBC 4.2.

```
private static Connection connectViaDM() throws Exception
{
    Connection connection = null;
    connection = DriverManager.getConnection(CONNECTION_URL);
    return connection;
}
```

Contoh berikut menunjukkan bagaimana menggunakan DataSource kelas untuk membuat koneksi.

```
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;
}
```

Mendapatkan URL JDBC

Sebelum Anda dapat terhubung ke cluster Amazon Redshift Anda dari alat klien SQL, Anda perlu mengetahui URL JDBC klaster Anda. URL JDBC memiliki format berikut:

```
jdbc:redshift://endpoint:port/database
```

Bidang format sebelumnya memiliki nilai berikut.

Bidang	Nilai
<code>jdbc</code>	Protokol untuk koneksi.
<code>redshift</code>	Subprotokol yang menentukan untuk menggunakan driver Amazon Redshift untuk terhubung ke database.
<code><i>endpoint</i></code>	Titik akhir dari cluster Amazon Redshift.
<code><i>port</i></code>	Nomor port yang Anda tentukan saat meluncurkan cluster. Jika Anda memiliki firewall, pastikan port ini terbuka untuk Anda gunakan.
<code><i>database</i></code>	Database yang Anda buat untuk cluster Anda.

Berikut ini adalah contoh URL JDBC: `jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev`

Pastikan untuk memasukkan nilai URL, misalnya SessionToken nilai, dalam format URL yang dikodekan.

Untuk informasi tentang cara mendapatkan koneksi JDBC Anda, lihat [Menemukan string koneksi cluster Anda](#)

Jika komputer klien gagal terhubung ke database, Anda dapat memecahkan masalah yang mungkin terjadi. Untuk informasi selengkapnya, lihat [Memecahkan masalah koneksi di Amazon Redshift](#).

Membangun URL koneksi

Gunakan URL koneksi untuk memasok informasi koneksi ke penyimpanan data yang Anda akses. Berikut ini adalah format URL koneksi untuk driver Amazon Redshift JDBC versi 2.1. Di sini, [Host]

titik akhir server Amazon Redshift dan [Port] adalah jumlah port Transmission Control Protocol (TCP) yang digunakan server untuk mendengarkan permintaan klien.

```
jdbc:redshift://[Host]:[Port]
```

Berikut ini adalah format URL koneksi yang menentukan beberapa pengaturan opsional.

```
jdbc:redshift://[Host]:[Port]/[database];[Property1]=[Value];  
[Property2]=[Value];
```

Misalnya, misalkan Anda ingin terhubung ke port 9000 pada cluster Amazon Redshift di Wilayah AS Barat (California Utara) aktif. AWS Anda juga ingin mengakses database bernama dev dan mengotentikasi koneksi menggunakan nama pengguna database dan kata sandi. Dalam hal ini, Anda menggunakan URL koneksi berikut.

```
jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/  
dev;UID=amazon;PWD=amazon
```

Anda dapat menggunakan karakter berikut untuk memisahkan opsi konfigurasi dari sisa string URL:

- ;
- ?

Misalnya, string URL berikut setara:

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

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

Anda dapat menggunakan karakter berikut untuk memisahkan opsi konfigurasi satu sama lain dalam string URL:

- ;
- &

Misalnya, string URL berikut setara:

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

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

Contoh URL berikut menentukan tingkat log 6 dan jalur untuk log.

```
jdbc:redshift://redshift.amazonaws.com:5439/dev;DSILogLevel=6;LogPath=/home/user/logs;
```

Jangan duplikat properti di URL koneksi.

Untuk daftar lengkap opsi konfigurasi yang dapat Anda tentukan, lihat [Opsi untuk konfigurasi driver JDBC versi 2.1](#).

Note

Saat Anda terhubung, jangan gunakan alamat IP node cluster atau alamat IP titik akhir VPC. Selalu gunakan titik akhir Redshift untuk menghindari pemadaman yang tidak perlu. Satu-satunya pengecualian untuk menggunakan URL endpoint adalah ketika Anda menggunakan nama domain khusus. Untuk informasi selengkapnya, lihat [Menggunakan nama domain khusus untuk koneksi klien](#).

Mengkonfigurasi keepalives TCP untuk koneksi JDBC Anda

Secara default, driver Amazon Redshift JDBC dikonfigurasi untuk menggunakan keepalives TCP untuk mencegah koneksi dari kehabisan waktu. Anda dapat menentukan kapan driver mulai mengirim paket keepalive atau mematikan fitur dengan mengatur properti yang relevan di URL koneksi. Untuk informasi selengkapnya tentang sintaks URL koneksi, lihat [Membangun URL koneksi](#).

Properti	Deskripsi
TCPKeepAlive	Untuk mematikan keepalives TCP, setel properti ini ke. FALSE

Mengkonfigurasi koneksi JDBC Anda dengan Apache Maven

Apache Maven adalah perangkat lunak manajemen proyek dan alat pemahaman. AWS SDK for Java Mendukung proyek Apache Maven. Untuk informasi selengkapnya, lihat [Menggunakan SDK dengan Apache Maven](#) di Panduan Pengembang.AWS SDK for Java

Jika Anda menggunakan Apache Maven, Anda dapat mengonfigurasi dan membangun proyek Anda untuk menggunakan driver Amazon Redshift JDBC untuk terhubung ke cluster Amazon Redshift Anda. Untuk melakukan ini, tambahkan driver JDBC sebagai dependensi dalam file proyek Anda. `pom.xml` Jika Anda menggunakan Maven untuk membangun proyek Anda dan ingin menggunakan koneksi JDBC, ambil langkah-langkah di bagian berikut.

Mengkonfigurasi driver JDBC sebagai ketergantungan Maven

Untuk mengkonfigurasi driver JDBC sebagai ketergantungan Maven

1. Tambahkan repositori Amazon atau repositori Maven Central ke bagian repositori file Anda. `pom.xml`

Note

URL dalam contoh kode berikut mengembalikan kesalahan jika digunakan dalam browser. Gunakan URL ini hanya dalam konteks proyek Maven.

Untuk repositori Amazon Maven, gunakan yang berikut ini.

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

Untuk terhubung menggunakan Secure Sockets Layer (SSL), tambahkan repositori berikut ke file Anda. `pom.xml`

```
<repositories>
  <repository>
```

```

    <id>redshift</id>
    <url>https://s3.amazonaws.com/redshift-maven-repository/release</url>
  </repository>
</repositories>

```

Untuk repositori Maven Central, tambahkan berikut ini ke file Anda. `pom.xml`

```

<repositories>
  <repository>
    <id>redshift</id>
    <url>https://repo1.maven.org/maven2</url>
  </repository>
</repositories>

```

2. Deklarasikan versi driver yang ingin Anda gunakan di bagian dependensi file Anda. `pom.xml`

Amazon Redshift menawarkan driver untuk alat yang kompatibel dengan JDBC 4.2 API. Untuk informasi tentang fungsionalitas yang didukung oleh driver ini, lihat [Unduh driver Amazon Redshift JDBC, versi 2.1](#).

Tambahkan ketergantungan untuk driver seperti yang ditunjukkan berikut.

Ganti *driver-version* dalam contoh berikut dengan versi driver Anda, misalnya `2.1.0.1`.

Untuk driver yang kompatibel dengan JDBC 4.2, gunakan yang berikut ini.

```

<dependency>
  <groupId>com.amazon.redshift</groupId>
  <artifactId>redshift-jdbc42</artifactId>
  <version>driver-version</version>
</dependency>

```

Nama kelas untuk pengemudi ini adalah `com.amazon.redshift.Driver`.

Driver Amazon Redshift Maven memerlukan dependensi opsional berikut saat Anda menggunakan otentikasi database IAM.

```

<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-core</artifactId>
  <version>1.12.23</version>

```



```
<scope>runtime</scope>
<optional>true</optional>
</dependency>
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-redshift</artifactId>
  <version>1.12.23</version>
  <scope>runtime</scope>
  <optional>true</optional>
</dependency>
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-sts</artifactId>
  <version>1.12.23</version>
  <scope>runtime</scope>
  <optional>true</optional>
</dependency>
```

Upgrade driver ke versi terbaru

Untuk memutakhirkan atau mengubah driver Amazon Redshift JDBC ke versi terbaru, pertama-tama ubah bagian versi dependensi ke versi driver terbaru. Kemudian bersihkan proyek Anda dengan Plugin Maven Clean, seperti yang ditunjukkan berikut.

```
mvn clean
```

Mengkonfigurasi otentikasi dan SSL

Untuk melindungi data dari akses yang tidak sah, penyimpanan data Amazon Redshift memerlukan semua koneksi untuk diautentikasi menggunakan kredensial pengguna. Beberapa penyimpanan data juga memerlukan koneksi yang harus dibuat melalui protokol Secure Sockets Layer (SSL), baik dengan atau tanpa otentikasi satu arah.

Driver Amazon Redshift JDBC versi 2.1 memberikan dukungan penuh untuk protokol otentikasi ini.

Versi SSL yang didukung driver tergantung pada versi JVM yang Anda gunakan. Untuk informasi tentang versi SSL yang didukung oleh setiap versi Java, lihat [Mendiagnosis TLS, SSL, dan HTTPS](#) di Blog Manajemen Produk Grup Platform Java.

Versi SSL yang digunakan untuk koneksi adalah versi tertinggi yang didukung oleh driver dan server, yang ditentukan pada waktu koneksi.

Konfigurasi driver Amazon Redshift JDBC versi 2.1 untuk mengautentikasi koneksi Anda sesuai dengan persyaratan keamanan server Redshift yang Anda sambungkan.

Anda harus selalu memberikan nama pengguna dan kata sandi Redshift Anda untuk mengautentikasi koneksi. Bergantung pada apakah SSL diaktifkan dan diperlukan di server, Anda mungkin juga perlu mengonfigurasi driver untuk terhubung melalui SSL. Atau Anda mungkin menggunakan otentikasi SSL satu arah sehingga klien (driver itu sendiri) memverifikasi identitas server.

Anda memberikan informasi konfigurasi ke driver di URL koneksi. Untuk informasi selengkapnya tentang sintaks URL koneksi, lihat [Membangun URL koneksi](#).

SSL menunjukkan TLS/SSL, baik Transport Layer Security dan Secure Sockets Layer. Driver mendukung versi standar industri TLS/SSL.

Hanya menggunakan nama pengguna dan kata sandi

Jika server yang Anda sambungkan tidak menggunakan SSL, maka Anda hanya perlu memberikan nama pengguna dan kata sandi Redshift Anda untuk mengautentikasi koneksi.

Untuk mengonfigurasi autentikasi hanya menggunakan nama pengguna dan kata sandi Redshift

1. Setel UID properti ke nama pengguna Redshift Anda untuk mengakses server Amazon Redshift.
2. Setel properti PWD ke kata sandi yang sesuai dengan nama pengguna Redshift Anda.

Menggunakan SSL tanpa verifikasi identitas

Jika server yang Anda sambungkan menggunakan SSL tetapi tidak memerlukan verifikasi identitas, maka Anda dapat mengonfigurasi driver untuk menggunakan pabrik SSL yang tidak memvalidasi.

Untuk mengonfigurasi koneksi SSL tanpa verifikasi identitas

1. Setel UID properti ke nama pengguna Redshift Anda untuk mengakses server Amazon Redshift.
2. Atur PWD properti ke kata sandi yang sesuai dengan nama pengguna Redshift Anda.
3. Atur `SSLFactory` properti ke `com.amazon.redshift.ssl.NonValidatingFactory`.

Menggunakan otentikasi SSL satu arah

Jika server yang Anda sambungkan menggunakan SSL dan memiliki sertifikat, maka Anda dapat mengonfigurasi driver untuk memverifikasi identitas server menggunakan otentikasi satu arah.

Otentikasi satu arah memerlukan sertifikat SSL yang ditandatangani dan tepercaya untuk memverifikasi identitas server. Anda dapat mengonfigurasi driver untuk menggunakan sertifikat tertentu atau mengakses TrustStore yang berisi sertifikat yang sesuai. Jika Anda tidak menentukan sertifikat atau TrustStore, maka driver menggunakan Java default TrustStore (biasanya salah satu `jssecacerts` atau `caacerts`).

Untuk mengonfigurasi otentikasi SSL satu arah

1. Setel properti UID ke nama pengguna Redshift Anda untuk mengakses server Amazon Redshift.
2. Setel properti PWD ke kata sandi yang sesuai dengan nama pengguna Redshift Anda.
3. Setel properti SSL ke `true`.
4. Setel `RootCert` properti SSL ke lokasi sertifikat CA root Anda.
5. Jika Anda tidak menggunakan salah satu Java default TrustStores, lakukan salah satu hal berikut:
 - Untuk menentukan sertifikat server, atur `RootCert` properti SSL ke jalur lengkap sertifikat.
 - Untuk menentukan TrustStore, lakukan hal berikut:
 - a. Gunakan program `keytool` untuk menambahkan sertifikat server ke TrustStore yang ingin Anda gunakan.
 - b. Tentukan TrustStore dan kata sandi yang akan digunakan saat memulai aplikasi Java menggunakan driver. Sebagai contoh:

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

6. Pilih salah satu:
 - Untuk memvalidasi sertifikat, setel properti `SSLMode` ke `verify-ca`.
 - Untuk memvalidasi sertifikat dan memverifikasi nama host dalam sertifikat, setel properti `SSLMode` ke `verify-full`.

Mengkonfigurasi otentikasi IAM

Jika Anda terhubung ke server Amazon Redshift menggunakan autentikasi IAM, setel properti berikut sebagai bagian dari string koneksi sumber data Anda.

Untuk informasi selengkapnya tentang autentikasi IAM, lihat [Manajemen identitas dan akses di Amazon Redshift](#)

Untuk menggunakan otentikasi IAM, gunakan salah satu format string koneksi berikut:

String koneksi	Deskripsi
<code>jdbc:redshift:iam:// [host]:[port]/[db]</code>	String koneksi biasa. Pengemudi menyimpulkan clusterID dan Region dari host.
<code>jdbc:redshift:iam:// [cluster-id]: [region]/[db]</code>	Pengemudi mengambil informasi host, mengingat ClusterID dan Region.
<code>jdbc:redshift:iam:// [host]/[db]</code>	Driver default ke port 5439, dan menyimpulkan ClusterID dan Region dari host. Bergantung pada port yang Anda pilih saat membuat, memodifikasi, atau memigrasi klaster, izinkan akses ke port yang dipilih.

Menentukan profil

Jika Anda menggunakan otentikasi IAM, Anda dapat menentukan properti koneksi tambahan yang diperlukan atau opsional di bawah nama profil. Dengan melakukan ini, Anda dapat menghindari meletakkan informasi tertentu secara langsung di string koneksi. Anda menentukan nama profil dalam string koneksi Anda menggunakan properti Profil.

Profil dapat ditambahkan ke file AWS kredensial. Lokasi default untuk file ini adalah: `~/.aws/credentials`

Anda dapat mengubah nilai default dengan mengatur jalur dalam variabel lingkungan berikut: `AWS_CREDENTIAL_PROFILES_FILE`

Untuk informasi selengkapnya tentang profil, lihat [Bekerja dengan AWS Kredensial di AWS SDK for Java](#)

Menggunakan kredensial profil instance

Jika Anda menjalankan aplikasi pada instans Amazon EC2 yang dikaitkan dengan peran IAM, Anda dapat terhubung menggunakan kredensial profil instans.

Untuk melakukan ini, gunakan salah satu format string koneksi IAM di tabel sebelumnya, dan atur properti koneksi dbuser ke nama pengguna Amazon Redshift yang Anda sambungkan sebagai.

Untuk informasi selengkapnya tentang profil instans, lihat [Manajemen Akses](#) di Panduan Pengguna IAM.

Menggunakan penyedia kredensi

Driver juga mendukung plugin penyedia kredensial dari layanan berikut:

- Layanan Federasi Direktori Aktif (ADFS)
- Layanan Token Web JSON (JWT)
- Layanan Microsoft Azure Active Directory (AD) dan Layanan Browser Microsoft Azure Active Directory (AD)
- Layanan Okta
- PingFederate Layanan
- Browser SAMP untuk layanan SAMP seperti Okta, Ping, atau ADFS

Jika Anda menggunakan salah satu layanan ini, URL koneksi perlu menentukan properti berikut:

- `Plugin_Name` - Jalur kelas yang sepenuhnya memenuhi syarat untuk kelas plugin penyedia kredensial Anda.
- `IDP_host`: — Host untuk layanan yang Anda gunakan untuk mengautentikasi ke Amazon Redshift.
- `IDP_port` — Port tempat host untuk layanan otentikasi mendengarkan. Tidak diperlukan untuk Okta.
- `User` - Nama pengguna untuk server `idp_host`.
- `Kata sandi` — Kata sandi yang terkait dengan nama pengguna `idp_host`.
- `DbUser`— Nama pengguna Amazon Redshift yang Anda sambungkan sebagai.
- `SSL_insecure` - Menunjukkan apakah sertifikat server IDP harus diverifikasi.
- `Client_ID` — ID klien yang terkait dengan nama pengguna di portal Azure AD. Hanya digunakan untuk Azure AD.
- `Client_Secret` — Rahasia klien yang terkait dengan ID klien di portal Azure AD. Hanya digunakan untuk Azure AD.
- `IDP_Tenant` - ID penyewa Azure AD untuk aplikasi Amazon Redshift Anda. Hanya digunakan untuk Azure AD.
- `App_ID` — ID aplikasi Okta untuk aplikasi Amazon Redshift Anda. Hanya digunakan untuk Okta.

- `App_Name` — Nama aplikasi Okta opsional untuk aplikasi Amazon Redshift Anda. Hanya digunakan untuk Okta.
- `Partner_SPID` — Nilai SPID mitra opsional (ID penyedia layanan). Hanya digunakan untuk PingFederate.

Jika Anda menggunakan plugin browser untuk salah satu layanan ini, URL koneksi juga dapat mencakup:

- `Login_URL` — URL untuk sumber daya di situs web penyedia identitas saat menggunakan layanan Security Assertion Markup Language (SAMP) atau Azure AD melalui plugin browser. Parameter ini diperlukan jika Anda menggunakan plugin browser.
- `Listen_Port` — Port yang digunakan driver untuk mendapatkan respons SAMP dari penyedia identitas saat menggunakan layanan SAMP atau Azure AD melalui plugin browser.
- `IDP_Response_Timeout` — Jumlah waktu, dalam hitungan detik, driver menunggu respons SAMP dari penyedia identitas saat menggunakan layanan SAMP atau Azure AD melalui plugin browser.

Untuk informasi tentang properti string koneksi tambahan, lihat [Opsi untuk konfigurasi driver JDBC versi 2.1](#).

Mengkonfigurasi logging

Anda dapat mengaktifkan masuk ke driver untuk membantu mendiagnosis masalah.

Anda dapat mencatat informasi driver dengan menggunakan metode berikut:

- Untuk menyimpan informasi yang dicatat dalam `file.log`, lihat [Menggunakan file log](#).
- Untuk mengirim informasi yang dicatat ke LogStream atau LogWriter ditentukan dalam DriverManager, lihat [Menggunakan LogStream atau LogWriter](#).

Anda memberikan informasi konfigurasi ke driver di URL koneksi. Untuk informasi selengkapnya tentang sintaks URL koneksi, lihat [Membangun URL koneksi](#).

Menggunakan file log

Aktifkan logging cukup lama untuk menangkap masalah. Logging mengurangi kinerja dan dapat mengkonsumsi sejumlah besar ruang disk.

Atur LogLevel kunci di URL koneksi Anda untuk mengaktifkan logging dan tentukan jumlah detail yang disertakan dalam file log. Tabel berikut mencantumkan level logging yang disediakan oleh driver Amazon Redshift JDBC versi 2.1, dalam urutan dari yang paling sedikit bertele-tele hingga yang paling bertele-tele.

LogLevel nilai	Deskripsi
1	Log peristiwa kesalahan parah yang akan menyebabkan pengemudi membatalkan.
2	Peristiwa kesalahan log yang memungkinkan driver untuk terus berjalan.
3	Log peristiwa yang mungkin mengakibatkan kesalahan jika tindakan tidak diambil. Tingkat logging dan tingkat logging di atas level ini juga mencatat kueri pengguna.
4	Log informasi umum yang menjelaskan kemajuan pengemudi.
5	Log informasi terperinci yang berguna untuk men-debug driver.
6	Catat semua aktivitas pengemudi.

Untuk mengatur logging yang menggunakan file log

1. Atur LogLevel properti ke tingkat informasi yang diinginkan untuk disertakan dalam file log.
2. Atur LogPath properti ke jalur lengkap ke folder tempat Anda ingin menyimpan file log.

Misalnya, URL koneksi berikut memungkinkan logging level 3 dan menyimpan file log di folder C:\temp: `jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/Default;DSILogLevel=3; LogPath=C:\temp`

3. Untuk memastikan bahwa pengaturan baru berlaku, restart aplikasi JDBC Anda dan sambungkan kembali ke server.

Driver Amazon Redshift JDBC menghasilkan file log berikut di lokasi yang ditentukan dalam properti: LogPath

- File `redshift_jdbc.log` yang mencatat aktivitas driver yang tidak spesifik untuk koneksi.
- `redshift_jdbc_connection_[Number].log` file untuk setiap koneksi yang dibuat ke database, di mana [Number] adalah nomor yang mengidentifikasi setiap file log. File ini mencatat aktivitas driver yang khusus untuk koneksi.

Jika LogPath nilainya tidak valid, maka driver mengirimkan informasi yang dicatat ke aliran keluaran standar () `System.out`

Menggunakan LogStream atau LogWriter

Aktifkan logging cukup lama untuk menangkap masalah. Logging mengurangi kinerja dan dapat mengkonsumsi sejumlah besar ruang disk.

Atur LogLevel kunci di URL koneksi Anda untuk mengaktifkan logging dan tentukan jumlah detail yang dikirim ke LogStream atau LogWriter ditentukan dalam file DriverManager.

Untuk mengaktifkan logging yang menggunakan LogStream atau LogWriter:

1. Untuk mengonfigurasi driver untuk mencatat informasi umum yang menjelaskan kemajuan driver, atur LogLevel properti ke 1 atau INFO.
2. Untuk memastikan bahwa pengaturan baru berlaku, restart aplikasi JDBC Anda dan sambungkan kembali ke server.

Untuk mematikan logging yang menggunakan LogStream atau LogWriter:

1. Hapus LogLevel properti dari URL koneksi.
2. Untuk memastikan bahwa pengaturan baru berlaku, restart aplikasi JDBC Anda dan sambungkan kembali ke server.

Mengonversi tipe data

Driver Amazon Redshift JDBC versi 2.1 mendukung banyak format data umum, mengonversi antara jenis data Amazon Redshift, SQL, dan Java.

Tabel berikut mencantumkan pemetaan tipe data yang didukung.

Jenis Amazon Redshift	Jenis SQL	Jenis Java
BIGINT	SQL_BIGINT	Long
BOOLEAN	SQL_BIT	Boolean
CHAR	SQL_CHAR	String
DATE	SQL_TYPE_DATE	java.sql.date
DECIMAL	SQL_NUMERIK	BigDecimal
DOUBLE PRECISION	SQL_GANDA	Ganda
GEOMETRY	SQL_LONGVARBINARY	byte []
INTEGER	SQL_INTEGER	Bilangan Bulat
OID	SQL_BIGINT	Long
SUPER	SQL_LONGVARCHAR	String
REAL	SQL_REAL	Desimal
SMALLINT	SQL_SMALLINT	Pendek
TEXT	SQL_VARCHAR	String
TIME	SQL_TYPE_TIME	java.sql.waktu
JADWAL	SQL_TYPE_TIME	java.sql.waktu
TIMESTAMP	STEMPEL WAKTU SQL_TYPE_	java.sql.TimeStamp

Jenis Amazon Redshift	Jenis SQL	Jenis Java
TIMESTAMPTZ	STEMPEL WAKTU SQL_TYPE_	java.sql.TimeStamp
VARCHAR	SQL_VARCHAR	String

Menggunakan dukungan pernyataan yang disiapkan

Driver Amazon Redshift JDBC mendukung pernyataan yang disiapkan. Anda dapat menggunakan pernyataan yang disiapkan untuk meningkatkan kinerja kueri berparameter yang perlu dijalankan beberapa kali selama koneksi yang sama.

Pernyataan yang disiapkan adalah pernyataan SQL yang dikompilasi di sisi server tetapi tidak segera dijalankan. Pernyataan yang dikompilasi disimpan di server sebagai `PreparedStatement` objek sampai Anda menutup objek atau koneksi. Sementara objek itu ada, Anda dapat menjalankan pernyataan yang disiapkan sebanyak yang diperlukan menggunakan nilai parameter yang berbeda, tanpa harus mengkompilasi pernyataan lagi. Overhead yang dikurangi ini memungkinkan kumpulan kueri dijalankan lebih cepat.

Untuk informasi lebih lanjut tentang pernyataan yang disiapkan, lihat “Menggunakan Pernyataan yang Disiapkan” di [tutorial JDBC Basics dari Oracle](#).

Anda dapat menyiapkan pernyataan yang berisi beberapa kueri. Misalnya, pernyataan disiapkan berikut berisi dua query INSERT:

```
PreparedStatement pstmt = conn.prepareStatement("INSERT INTO
MyTable VALUES (1, 'abc'); INSERT INTO CompanyTable VALUES
(1, 'abc');");
```

Berhati-hatilah agar kueri ini tidak bergantung pada hasil kueri lain yang ditentukan dalam pernyataan yang disiapkan yang sama. Karena kueri tidak berjalan selama langkah persiapan, hasilnya belum dikembalikan, dan tidak tersedia untuk kueri lain dalam pernyataan yang disiapkan yang sama.

Misalnya, pernyataan yang disiapkan berikut, yang membuat tabel dan kemudian menyisipkan nilai ke dalam tabel yang baru dibuat, tidak diperbolehkan:

```
PreparedStatement pstmt = conn.prepareStatement("CREATE
```

```
TABLE MyTable(col1 int, col2 varchar); INSERT INTO myTable
VALUES (1, 'abc');");
```

Jika Anda mencoba menyiapkan pernyataan ini, server mengembalikan kesalahan yang menyatakan bahwa tabel tujuan (MyTable) belum ada. Query CREATE harus dijalankan sebelum query INSERT dapat disiapkan.

Perbedaan antara versi 2.1 dan 1.x dari driver JDBC

Bagian ini menjelaskan perbedaan informasi yang dikembalikan oleh versi 2.1 dan 1.x dari driver JDBC. Driver JDBC versi 1.x dihentikan.

Tabel berikut mencantumkan DatabaseMetadata informasi yang dikembalikan oleh fungsi `getDatabaseProduct Name ()` dan `getDatabaseProduct Version ()` untuk setiap versi driver JDBC. Driver JDBC versi 2.1 memperoleh nilai saat membuat koneksi. Driver JDBC versi 1.x memperoleh nilai sebagai hasil dari kueri.

Versi driver JDBC	dapatkan DatabaseProduct Nama () hasil	dapatkan hasil DatabaseProduct Version ()
2.1	Redshift	8.0.2
1.x	PostgreSQL	08.00.0002

Tabel berikut mencantumkan DatabaseMetadata informasi yang dikembalikan oleh `getTypeInfo` fungsi untuk setiap versi driver JDBC.

Versi driver JDBC	getTypeInfo hasil
2.1	Konsisten dengan tipe data Redshift
1.x	Konsisten dengan tipe data PostgreSQL

Membuat file inisialisasi (.ini) untuk driver JDBC versi 2.1

Dengan menggunakan file inisialisasi (.ini) untuk driver Amazon Redshift JDBC versi 2.1, Anda dapat menentukan parameter konfigurasi tingkat sistem. Misalnya, parameter otentikasi IDP federasi

dapat bervariasi untuk setiap aplikasi. File ini menyediakan lokasi umum untuk klien SQL untuk mendapatkan parameter konfigurasi yang diperlukan.

Anda dapat membuat file inisialisasi versi 2.1 driver JDBC (.ini) yang berisi opsi konfigurasi untuk klien SQL. Nama default file tersebut adalah `rsjdbc.ini`. Driver JDBC versi 2.1 memeriksa file ini di lokasi berikut, tercantum dalam urutan prioritas:

- `IniFile` parameter di URL koneksi atau di kotak dialog properti koneksi klien SQL. Pastikan `IniFile` parameter berisi path lengkap ke file ini, termasuk nama file. Untuk informasi tentang `IniFile` parameter, lihat [IniFile](#). Jika `IniFile` parameter salah menentukan lokasi file ini, kesalahan akan ditampilkan.
- Variabel lingkungan seperti `AMAZON_REDSHIFT_JDBC_INI_FILE` dengan path lengkap, termasuk nama file. Anda dapat menggunakan `rsjdbc.ini` atau menentukan nama file. Jika variabel lingkungan `AMAZON_REDSHIFT_JDBC_INI_FILE` salah menentukan lokasi file ini, kesalahan akan ditampilkan.
- Direktori tempat file JAR driver berada.
- Direktori home pengguna.
- Direktori temp dari sistem.

Anda dapat mengatur file ini menjadi beberapa bagian, misalnya `[DRIVER]`. Setiap bagian berisi pasangan kunci-nilai yang menentukan berbagai parameter koneksi. Anda dapat menggunakan `IniSection` parameter untuk menentukan bagian dalam file ini. Untuk informasi tentang `IniSection` parameter, lihat [IniSection](#).

Berikut ini adalah contoh dari format file ini, dengan bagian untuk `[DRIVER]`, `[DEV]`, `[QA]`, dan `[PROD]`. Bagian `[DRIVER]` dapat diterapkan ke koneksi apa pun.

```
[DRIVER]
key1=val1
key2=val2

[DEV]
key1=val1
key2=val2

[QA]
key1=val1
key2=val2
```

```
[PROD]
key1=val1
key2=val2
```

Driver JDBC versi 2.1 memuat parameter konfigurasi dari lokasi berikut, tercantum dalam urutan prioritas:

- Parameter konfigurasi default dalam kode aplikasi.
- Properti bagian [DRIVER] dari file.ini, jika disertakan.
- Parameter konfigurasi bagian kustom, jika `IniSection` opsi disediakan di URL koneksi atau di kotak dialog properti koneksi klien SQL.
- Properti dari objek properti koneksi yang ditentukan dalam `getConnection` panggilan.
- Parameter konfigurasi dipercepat dalam URL koneksi.

Opsi untuk konfigurasi driver JDBC versi 2.1

Berikut ini, Anda dapat menemukan deskripsi untuk opsi yang dapat Anda tentukan untuk driver Amazon Redshift JDBC versi 2.1. Opsi konfigurasi tidak peka huruf besar/kecil.

Anda dapat mengatur properti konfigurasi menggunakan URL koneksi. Untuk informasi selengkapnya, lihat [Membangun URL koneksi](#).

Topik

- [AccessKeyID](#)
- [AllowDB UserOverride](#)
- [App_ID](#)
- [App_Nama](#)
- [ApplicationName](#)
- [AuthProfile](#)
- [AutoCreate](#)
- [Client_ID](#)
- [Klien_Rahasia](#)
- [ClusterID](#)
- [Kompresi](#)

- [ConnectTimeout](#)
- [ConnectionTimeZone](#)
- [basis data MetadataCurrent DbOnly](#)
- [DbUser](#)
- [DbGroups](#)
- [DBNAME](#)
- [RowFetchUkuran default](#)
- [DisablesValidQuery](#)
- [aktifkan FetchRing Buffer](#)
- [aktifkan MultiSql Support](#)
- [ambil Ukuran RingBuffer](#)
- [ForceLowercase](#)
- [GroupFederation](#)
- [HOST](#)
- [IAM DisableCache](#)
- [IamDuration](#)
- [Identity_Namespace](#)
- [IDP_host](#)
- [IDP_port](#)
- [IDP_penyewa](#)
- [IDP_Response_Timeout](#)
- [IniFile](#)
- [IniSection](#)
- [IServerless](#)
- [Login_URL](#)
- [loginTimeout](#)
- [Login ToRp](#)
- [LogLevel](#)
- [LogPath](#)

- [OverrideSchemaPatternType](#)
- [Partner_SPID](#)
- [Kata sandi](#)
- [Plugin_Nama](#)
- [PELABUHAN](#)
- [Diutamakan_Peran](#)
- [Profil](#)
- [PWD](#)
- [QueryGroup](#)
- [ReadOnly](#)
- [Wilayah](#)
- [WriteBatchedSisipan ulang](#)
- [kembali WriteBatched InsertsSize](#)
- [roleArn](#)
- [peran SessionName](#)
- [cakupan](#)
- [SecretAccessKunci](#)
- [SessionToken](#)
- [tanpa server AcctId](#)
- [tanpa server WorkGroup](#)
- [SocketFactory](#)
- [socketTimeout](#)
- [SSL](#)
- [SSL_tidak aman](#)
- [SSLCert](#)
- [SSLFactory](#)
- [SSLKey](#)
- [SSLMode](#)
- [SSLPassword](#)
- [SSL RootCert](#)

- [StsEndpointUrl](#)
- [tcp KeepAlive](#)
- [token](#)
- [token_type](#)
- [UID](#)
- [Pengguna](#)
- [web IdentityToken](#)

AccessKeyID

- Nilai Default - Tidak Ada
- Tipe Data - String

Anda dapat menentukan parameter ini untuk memasukkan kunci akses IAM untuk pengguna atau peran. Anda biasanya dapat menemukan kunci dengan melihat dan string atau profil pengguna yang ada. Jika Anda menentukan parameter ini, Anda juga harus menentukan `SecretAccessKey` parameter. Jika diteruskan dalam URL JDBC, `AccessKey ID` harus dikodekan URL.

Parameter ini bersifat opsional.

AllowDB UserOverride

- Nilai Default - 0
- Tipe Data - String

Opsi ini menentukan apakah driver menggunakan `DbUser` nilai dari pernyataan SAMP atau nilai yang ditentukan dalam properti `DbUser` koneksi di URL koneksi.

Parameter ini bersifat opsional.

1

Pengemudi menggunakan `DbUser` nilai dari pernyataan SAMP.

Jika pernyataan SAMP tidak menentukan nilai untuk `DBUser`, driver menggunakan nilai yang ditentukan dalam properti koneksi. `DBUser` Jika properti koneksi juga tidak menentukan nilai, driver menggunakan nilai yang ditentukan dalam profil koneksi.

0

Driver menggunakan DBUser nilai yang ditentukan dalam properti DBUser koneksi.

Jika properti DBUser koneksi tidak menentukan nilai, driver menggunakan nilai yang ditentukan dalam profil koneksi. Jika profil koneksi juga tidak menentukan nilai, driver menggunakan nilai dari pernyataan SAMP.

App_ID

- Nilai Default - Tidak Ada
- Tipe Data - String

ID unik yang disediakan OKTA yang terkait dengan aplikasi Amazon Redshift Anda.

Parameter ini diperlukan jika mengautentikasi melalui layanan Okta.

App_Nama

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama aplikasi Okta yang Anda gunakan untuk mengautentikasi koneksi ke Amazon Redshift.

Parameter ini bersifat opsional.

ApplicationName

- Nilai Default - null
- Tipe Data - String

Nama aplikasi untuk diteruskan ke Amazon Redshift untuk tujuan audit.

Parameter ini bersifat opsional.

AuthProfile

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama profil otentikasi yang akan digunakan untuk menghubungkan ke Amazon Redshift.

Parameter ini bersifat opsional.

AutoCreate

- Nilai Default - false
- Tipe Data - Boolean

Opsi ini menentukan apakah driver menyebabkan pengguna baru dibuat ketika pengguna tertentu tidak ada.

Parameter ini bersifat opsional.

true

Jika pengguna yang ditentukan oleh salah satu `DBUser` atau ID unik (UID) tidak ada, pengguna baru dengan nama itu akan dibuat.

false

Driver tidak menyebabkan pengguna baru dibuat. Jika pengguna yang ditentukan tidak ada, otentikasi gagal.

Client_ID

- Nilai Default - Tidak Ada
- Tipe Data - String

ID klien yang akan digunakan saat mengautentikasi koneksi menggunakan layanan Azure AD.

Parameter ini diperlukan jika mengautentikasi melalui layanan Azure AD.

Klien_Rahasia

- Nilai Default - Tidak Ada
- Tipe Data - String

Rahasia Klien untuk digunakan saat mengautentikasi koneksi menggunakan layanan Azure AD.

Parameter ini diperlukan jika mengautentikasi melalui layanan Azure AD.

ClusterID

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama cluster Amazon Redshift yang ingin Anda sambungkan. Pengemudi mencoba mendeteksi parameter ini dari host yang diberikan. Jika Anda menggunakan Network Load Balancer (NLB) dan terhubung melalui IAM, driver akan gagal mendeteksinya, sehingga Anda dapat mengaturnya menggunakan opsi koneksi ini.

Parameter ini bersifat opsional.

Kompresi

- Nilai Default - off
- Tipe Data - String

Metode kompresi yang digunakan untuk komunikasi protokol kawat antara server Amazon Redshift dan klien atau driver.

Parameter ini bersifat opsional.

Anda dapat menentukan salah satu nilai berikut:

- lz4

Menetapkan metode kompresi yang digunakan untuk komunikasi protokol kawat dengan Amazon Redshift ke lz4.

- off

Tidak menggunakan kompresi untuk komunikasi protokol kawat dengan Amazon Redshift.

ConnectTimeout

- Nilai Default - 10
- Tipe Data - Integer

Nilai batas waktu yang digunakan untuk operasi koneksi soket. Jika waktu yang diperlukan untuk membuat koneksi Amazon Redshift melebihi nilai ini, koneksi dianggap tidak tersedia. Batas waktu ditentukan dalam hitungan detik. Nilai 0 berarti tidak ada batas waktu yang ditentukan.

Parameter ini bersifat opsional.

ConnectionTimeZone

- Nilai Default - LOKAL
- Tipe Data - String

Zona waktu tingkat sesi.

Parameter ini bersifat opsional.

Anda dapat menentukan salah satu nilai berikut:

LOKAL

Mengonfigurasi zona waktu tingkat sesi ke zona waktu JVM LOKAL.

PELADEN

Mengonfigurasi zona waktu tingkat sesi ke zona waktu yang ditetapkan untuk pengguna di server Amazon Redshift. Anda dapat mengonfigurasi zona waktu tingkat sesi untuk pengguna dengan perintah berikut:

```
ALTER USER  
[...]  
SET TIMEZONE TO [...];
```

basis data MetadataCurrent DbOnly

- Nilai Default - benar
- Tipe Data - Boolean

Opsi ini menentukan apakah API metadata mengambil data dari semua database yang dapat diakses atau hanya dari database yang terhubung.

Parameter ini bersifat opsional.

Anda dapat menentukan salah satu nilai berikut:

`true`

Aplikasi mengambil metadata dari database tunggal.

`false`

Aplikasi mengambil metadata dari semua database yang dapat diakses.

`DbUser`

- Nilai Default - Tidak Ada
- Tipe Data - String

ID pengguna untuk digunakan dengan akun Amazon Redshift Anda. Anda dapat menggunakan ID yang saat ini tidak ada jika Anda telah mengaktifkan `AutoCreate` properti.

Parameter ini bersifat opsional.

`DbGroups`

- Nilai Default - PUBLIK
- Tipe Data - String

Daftar dipisahkan koma dari nama grup database yang ada yang `DBUser1` bergabung untuk sesi saat ini.

Parameter ini bersifat opsional.

`DBNAME`

- Nilai Default - null
- Tipe Data - String

Nama database untuk terhubung ke. Anda dapat menggunakan opsi ini untuk menentukan nama database di URL koneksi JDBC.

Parameter ini diperlukan. Anda harus menentukan nama database, baik di URL koneksi atau di properti koneksi aplikasi klien.

RowFetchUkuran default

- Nilai Default - 0
- Tipe Data - Integer

Opsi ini menentukan nilai default untuk `getFetchSize`.

Parameter ini bersifat opsional.

Anda dapat menentukan salah satu nilai berikut:

0

Ambil semua baris dalam satu operasi.

Integer positif

Jumlah baris yang akan diambil dari database untuk setiap iterasi pengambilan. `ResultSet`

DisableIsValidQuery

- Nilai Default - Salah
- Tipe Data - Boolean

Opsi ini menentukan apakah driver mengirimkan query database baru saat menggunakan metode `connection.isValid ()` untuk menentukan apakah koneksi database aktif.

Parameter ini bersifat opsional.

true

Driver tidak mengirimkan kueri saat menggunakan `Connection.isValid ()` untuk menentukan apakah koneksi database aktif. Hal ini dapat menyebabkan driver salah mengidentifikasi koneksi database sebagai aktif jika server database telah dimatikan secara tak terduga.

false

Driver mengirimkan kueri saat menggunakan `connection.isValid ()` untuk menentukan apakah koneksi database aktif.

aktifkan FetchRing Buffer

- Nilai Default - benar
- Tipe Data - Boolean

Opsi ini menentukan bahwa driver mengambil baris menggunakan buffer cincin pada utas terpisah. Parameter `fetchRingBuffer Ukuran` menentukan ukuran buffer cincin.

Jika transaksi mendeteksi Pernyataan yang berisi beberapa perintah SQL yang dipisahkan oleh titik koma, buffer ring fetch untuk transaksi tersebut disetel ke false. `enableFetchRingNilai` buffer tidak berubah.

Parameter ini bersifat opsional.

aktifkan MultiSql Support

- Nilai Default - benar
- Tipe Data - Boolean

Opsi ini menentukan apakah akan memproses beberapa perintah SQL dipisahkan oleh titik koma dalam Pernyataan.

Parameter ini bersifat opsional.

Anda dapat menentukan salah satu nilai berikut:

`true`

Driver memproses beberapa perintah SQL, dipisahkan oleh titik koma, dalam objek Pernyataan.

`false`

Driver mengembalikan kesalahan untuk beberapa perintah SQL dalam satu Pernyataan.

ambil Ukuran RingBuffer

- Nilai Default - 1G
- Tipe Data - String

Opsi ini menentukan ukuran buffer cincin yang digunakan saat mengambil set hasil. Anda dapat menentukan ukuran dalam byte, misalnya 1K untuk 1 KB, 5000 untuk 5.000 byte, 1M untuk 1 MB, 1G untuk 1 GB, dan seterusnya. Anda juga dapat menentukan persentase memori heap. Pengemudi berhenti mengambil baris setelah mencapai batas. Mengambil dilanjutkan saat aplikasi membaca baris dan membebaskan ruang di buffer ring.

Parameter ini bersifat opsional.

ForceLowercase

- Nilai Default - false
- Tipe Data - Boolean

Opsi ini menentukan apakah driver huruf kecil semua grup database (DbGroups) yang dikirim dari penyedia identitas ke Amazon Redshift saat menggunakan autentikasi masuk tunggal.

Parameter ini bersifat opsional.

true

Driver huruf kecil semua grup database yang dikirim dari penyedia identitas.

false

Pengemudi tidak mengubah grup basis data.

GroupFederation

- Nilai Default - false
- Tipe Data - Boolean

Opsi ini menentukan apakah akan menggunakan grup IDP Amazon Redshift. Ini didukung oleh API GetClusterCredentials V2.

Parameter ini bersifat opsional.

true

Gunakan grup Amazon Redshift Identity Provider (IDP).

false

Gunakan STS API dan `GetClusterCredentials` untuk federasi pengguna dan tentukan secara eksplisit `DbGroups` untuk koneksi.

HOST

- Nilai Default - null
- Tipe Data - String

Nama host dari server Amazon Redshift untuk terhubung. Anda dapat menggunakan opsi ini untuk menentukan nama host di URL koneksi JDBC.

Parameter ini diperlukan. Anda harus menentukan nama host, baik di URL koneksi atau di properti koneksi aplikasi klien.

IAM DisableCache

- Nilai Default - false
- Tipe Data - Boolean

Opsi ini menentukan apakah kredensial IAM di-cache.

Parameter ini bersifat opsional.

true

Kredensial IAM tidak di-cache.

false

Kredensi IAM di-cache. Ini meningkatkan kinerja saat permintaan ke gateway API dibatasi, misalnya.

IamDuration

- Nilai Default - 900
- Tipe Data - Integer

Lamanya waktu, dalam hitungan detik, hingga kredensi IAM sementara kedaluwarsa.

- Nilai minimum - 900
- Nilai maksimum - 3.600

Parameter ini bersifat opsional.

Identity_Namespace

- Nilai Default - Tidak Ada
- Tipe Data - String

Namespace identitas yang akan digunakan saat mengautentikasi menggunakan.

IdpTokenAuthPlugin Ini membantu Redshift menentukan instance IAM Identity Center mana yang akan digunakan.

Jika hanya ada satu instance IAM Identity Center yang ada atau jika namespace identitas default disetel, maka parameter ini opsional, jika tidak diperlukan.

IDP_host

- Nilai Default - Tidak Ada
- Tipe Data - String

Host IDP (penyedia identitas) yang Anda gunakan untuk mengautentikasi ke Amazon Redshift. Ini dapat ditentukan baik dalam string koneksi atau dalam profil.

Parameter ini bersifat opsional.

IDP_port

- Nilai Default - Tidak Ada
- Tipe Data - String

Port yang digunakan oleh IDP (penyedia identitas). Anda dapat menentukan port baik dalam string koneksi atau dalam profil. Port default adalah 5439. Bergantung pada port yang Anda pilih saat membuat, memodifikasi, atau memigrasi klaster, izinkan akses ke port yang dipilih.

Parameter ini bersifat opsional.

IDP_penyewa

- Nilai Default - Tidak Ada
- Tipe Data - String

ID penyewa Azure AD untuk aplikasi Amazon Redshift Anda.

Parameter ini diperlukan jika mengautentikasi melalui layanan Azure AD.

IDP_Response_Timeout

- Nilai Default - 120
- Tipe Data - Integer

Jumlah waktu, dalam hitungan detik, driver menunggu respons SAMP dari penyedia identitas saat menggunakan layanan SAMP atau Azure AD melalui plugin browser.

Parameter ini bersifat opsional.

IniFile

- Nilai Default - Tidak Ada
- Tipe Data - String

Jalur lengkap dari file.ini, termasuk nama file. Sebagai contoh:

```
IniFile="C:\tools\rjdbc.ini"
```

Untuk informasi tentang file.ini, lihat [Membuat file inisialisasi \(.ini\) untuk driver JDBC versi 2.1.](#)

Parameter ini bersifat opsional.

IniSection

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama bagian dalam file.ini yang berisi opsi konfigurasi. Untuk informasi tentang file.ini, lihat [Membuat file inisialisasi \(.ini\) untuk driver JDBC versi 2.1](#).

Contoh berikut menentukan bagian [Prod] dari file.ini:

```
IniSection="Prod"
```

Parameter ini bersifat opsional.

ISServerless

- Nilai Default - false
- Tipe Data - Boolean

Opsi ini menentukan apakah host endpoint Amazon Redshift adalah instance tanpa server. Pengemudi mencoba mendeteksi parameter ini dari host yang diberikan. Jika Anda menggunakan Network Load Balancer (NLB), driver akan gagal mendeteksinya, sehingga Anda dapat mengaturnya di sini.

Parameter ini bersifat opsional.

true

Host endpoint Amazon Redshift adalah instance tanpa server.

false

Host endpoint Amazon Redshift adalah cluster yang disediakan.

Login_URL

- Nilai Default - Tidak Ada
- Tipe Data - String

URL untuk sumber daya di situs web penyedia identitas saat menggunakan layanan SAMP atau Azure AD melalui plugin browser.

Parameter ini diperlukan jika mengautentikasi dengan layanan SAMP atau Azure AD melalui plugin browser.

loginTimeout

- Nilai Default - 0
- Tipe Data - Integer

Jumlah detik untuk menunggu sebelum waktu habis saat menghubungkan dan mengautentikasi ke server. Jika membuat koneksi membutuhkan waktu lebih lama dari ambang ini, maka koneksi dibatalkan.

Ketika properti ini disetel ke 0, koneksi tidak akan habis waktu.

Parameter ini bersifat opsional.

Login ToRp

- Nilai Default - `urn:amazon:webservices`
- Tipe Data - String

Pihak yang mengandalkan percaya bahwa Anda ingin menggunakan untuk jenis otentikasi AD FS.

Parameter ini bersifat opsional.

LogLevel

- Nilai Default - 0
- Tipe Data - Integer

Gunakan properti ini untuk mengaktifkan atau mematikan logging di driver dan untuk menentukan jumlah detail yang disertakan dalam file log.

Aktifkan logging hanya cukup lama untuk menangkap masalah. Logging mengurangi kinerja dan dapat mengkonsumsi sejumlah besar ruang disk.

Parameter ini bersifat opsional.

Atur parameter ke salah satu nilai berikut:

0

Nonaktifkan semua logging.

1

Aktifkan logging pada level FATAL, yang mencatat peristiwa kesalahan yang sangat parah yang akan menyebabkan pengemudi membatalkan.

2

Aktifkan logging pada level ERROR, yang mencatat peristiwa kesalahan yang mungkin masih memungkinkan driver untuk terus berjalan.

3

Aktifkan pencatatan pada tingkat PERINGATAN, yang mencatat peristiwa yang mungkin mengakibatkan kesalahan jika tindakan tidak dilakukan.

4

Aktifkan logging pada tingkat INFO, yang mencatat informasi umum yang menjelaskan kemajuan driver.

5

Aktifkan logging pada level DEBUG, yang mencatat informasi terperinci yang berguna untuk men-debug driver.

6

Aktifkan logging pada level TRACE, yang mencatat semua aktivitas driver.

Saat logging diaktifkan, driver menghasilkan file log berikut di lokasi yang ditentukan dalam LogPath properti:

- **redshift_jdbc.log**— File yang mencatat aktivitas driver yang tidak spesifik untuk koneksi.
- **redshift_jdbc_connection_[Number].log**— File untuk setiap koneksi yang dibuat ke database, di mana [Number] adalah nomor yang membedakan setiap file log dari yang lain. File ini mencatat aktivitas driver yang khusus untuk koneksi.

Jika LogPath nilainya tidak valid, driver mengirimkan informasi yang dicatat ke aliran output standar, System.out

LogPath

- Nilai Default - Direktori kerja saat ini.

- Tipe Data - String

Jalur lengkap ke folder tempat driver menyimpan file log saat LogLevel properti DSI diaktifkan.

Untuk memastikan bahwa URL koneksi kompatibel dengan semua aplikasi JDBC, kami sarankan Anda melarikan diri dari garis miring terbalik (\) di jalur file Anda dengan menyetik garis miring terbalik lainnya.

Parameter ini bersifat opsional.

OverrideSchemaPatternType

- Nilai Default - null
- Tipe Data - Integer

Opsi ini menentukan apakah akan mengganti jenis query yang digunakan dalam panggilan getTables.

0

Tidak ada Skema Universal Query

1

Kueri Skema Lokal

2

Kueri Skema Eksternal

Parameter ini bersifat opsional.

Partner_SPID

- Nilai Default - Tidak Ada
- Tipe Data - String

Nilai SPID mitra (ID penyedia layanan) yang akan digunakan saat mengautentikasi koneksi menggunakan layanan. PingFederate

Parameter ini bersifat opsional.

Kata sandi

- Nilai Default - Tidak Ada
- Tipe Data - String

Saat menghubungkan menggunakan otentikasi IAM melalui IDP, ini adalah kata sandi untuk server IDP_Host. Saat menggunakan otentikasi standar, ini dapat digunakan untuk kata sandi database Amazon Redshift alih-alih PWD.

Parameter ini bersifat opsional.

Plugin_Nama

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama kelas yang sepenuhnya memenuhi syarat untuk mengimplementasikan plugin penyedia kredensial tertentu.

Parameter ini bersifat opsional.

Opsi penyedia berikut didukung:

- **AdfsCredentialsProvider**— Layanan Federasi Direktori Aktif.
- **AzureCredentialsProvider**— Layanan Microsoft Azure Active Directory (AD).
- **BasicJwtCredentialsProvider**— Layanan Token Web JSON (JWT).
- **BasicSamlCredentialsProvider**— Kredensial Security Assertion Markup Language (SAMP) yang dapat Anda gunakan dengan banyak penyedia layanan SAMP.
- **BrowserAzureCredentialsProvider**— Browser Layanan Microsoft Azure Active Directory (AD).
- **BrowserAzureOauth2CredentialsProvider**— Layanan Browser Microsoft Azure Active Directory (AD) untuk Otentikasi Asli.
- **BrowserSamlCredentialsProvider**— Browser SAMP untuk layanan SAMP seperti Okta, Ping, atau ADFS.

- **IdpTokenAuthPlugin**- Plugin otorisasi yang menerima token IAM Identity Center atau OpenID Connect (OIDC) JSON berbasis token identitas (JWT) dari penyedia identitas web mana pun yang terhubung ke IAM Identity Center.
- **OktaCredentialsProvider**— Layanan Okta.
- **PingCredentialsProvider**— PingFederate Layanan.

PELABUHAN

- Nilai Default - null
- Tipe Data - Integer

Port server Amazon Redshift untuk terhubung. Anda dapat menggunakan opsi ini untuk menentukan port di URL koneksi JDBC.

Parameter ini bersifat opsional.

Diutamakan_Peran

- Nilai Default - Tidak Ada
- Tipe Data - String

Peran IAM yang ingin Anda asumsikan selama koneksi ke Amazon Redshift.

Parameter ini bersifat opsional.

Profil

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama profil yang akan digunakan untuk otentikasi IAM. Profil ini berisi properti koneksi tambahan yang tidak ditentukan dalam string koneksi.

Parameter ini bersifat opsional.

PWD

- Nilai Default - Tidak Ada

- Tipe Data - String

Kata sandi yang sesuai dengan nama pengguna Amazon Redshift yang Anda berikan menggunakan UID properti.

Parameter ini bersifat opsional.

QueryGroup

- Nilai Default - null
- Tipe Data - String

Opsi ini menetapkan kueri ke antrian saat runtime dengan menetapkan kueri Anda ke grup kueri yang sesuai. Grup kueri diatur untuk sesi. Semua kueri yang berjalan pada koneksi milik grup kueri ini.

Parameter ini bersifat opsional.

ReadOnly

- Nilai Default - false
- Tipe Data - Boolean

Properti ini menentukan apakah driver dalam mode read-only.

Parameter ini bersifat opsional.

true

Koneksi dalam mode read-only dan tidak dapat menulis ke penyimpanan data.

false

Koneksi tidak dalam mode read-only dan dapat menulis ke penyimpanan data.

Wilayah

- Nilai Default - null
- Tipe Data - String

Opsi ini menentukan AWS Wilayah di mana cluster berada. Jika Anda menentukan StsEndPoint opsi, opsi Wilayah diabaikan. Operasi Redshift GetClusterCredentials API juga menggunakan opsi Region.

Parameter ini bersifat opsional.

WriteBatchedSisipan ulang

- Nilai Default - false
- Tipe Data - Boolean

Opsi ini memungkinkan pengoptimalan untuk menulis ulang dan menggabungkan pernyataan INSERT yang kompatibel ke dalam batch.

Parameter ini bersifat opsional.

kembali WriteBatched InsertsSize

- Nilai Default - 128
- Tipe Data - Integer

Opsi ini memungkinkan pengoptimalan untuk menulis ulang dan menggabungkan pernyataan INSERT yang kompatibel ke dalam batch. Nilai ini harus meningkat secara eksponensial dengan kekuatan 2.

Parameter ini bersifat opsional.

roleArn

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama Sumber Daya Amazon (ARN) peran. Pastikan untuk menentukan parameter ini saat Anda menentukan opsi BasicJwtCredentialsProvider Plugin_Name. Anda menentukan ARN dalam format berikut:

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

Parameter ini diperlukan jika Anda menentukan BasicJwtCredentialsProvider untuk opsi Plugin_Name.

peran SessionName

- Nilai default - `jwt_redshift_session`
- Tipe Data - String

Sebuah pengenal untuk sesi peran yang diambil. Biasanya, Anda melewati nama atau pengenal yang terkait dengan pengguna aplikasi Anda. Kredensial keamanan sementara yang digunakan aplikasi Anda terkait dengan pengguna tersebut. Anda dapat menentukan parameter ini ketika Anda menentukan `BasicJwtCredentialsProvider` untuk opsi `Plugin_Name`.

Parameter ini bersifat opsional.

cakupan

- Nilai Default - Tidak Ada
- Tipe Data - String

Daftar cakupan yang dipisahkan ruang yang dapat disetujui pengguna. Anda menentukan parameter ini sehingga aplikasi Microsoft Azure Anda bisa mendapatkan persetujuan untuk API yang ingin Anda panggil. Anda dapat menentukan parameter ini ketika Anda menentukan `BrowserAzure OAuth2 CredentialsProvider` untuk opsi `Plugin_Name`.

Parameter ini diperlukan untuk plug-in `BrowserAzure OAuth2CredentialsProvider`.

SecretAccessKunci

- Nilai Default - Tidak Ada
- Tipe Data - String

Kunci akses IAM untuk pengguna atau peran. Jika ini ditentukan, maka `AccessKey ID` juga harus ditentukan. Jika diteruskan dalam URL JDBC, `SecretAccessKey` harus dikodekan URL.

Parameter ini bersifat opsional.

SessionToken

- Nilai Default - Tidak Ada
- Tipe Data - String

Token sesi IAM sementara yang terkait dengan peran IAM yang Anda gunakan untuk mengautentikasi. Jika diteruskan dalam URL JDBC, token sesi IAM sementara harus dikodekan URL.

Parameter ini bersifat opsional.

tanpa server AcctId

- Nilai Default - null
- Tipe Data - String

ID akun Tanpa Server Amazon Redshift. Pengemudi mencoba mendeteksi parameter ini dari host yang diberikan. Jika Anda menggunakan Network Load Balancer (NLB), driver akan gagal mendeteksinya, sehingga Anda dapat mengaturnya di sini.

Parameter ini bersifat opsional.

tanpa server WorkGroup

- Nilai Default - null
- Tipe Data - String

Nama workgroup Amazon Redshift Tanpa Server. Pengemudi mencoba mendeteksi parameter ini dari host yang diberikan. Jika Anda menggunakan Network Load Balancer (NLB), driver akan gagal mendeteksinya, sehingga Anda dapat mengaturnya di sini.

Parameter ini bersifat opsional.

SocketFactory

- Nilai Default - null
- Tipe Data - String

Opsi ini menentukan pabrik soket untuk pembuatan soket.

Parameter ini bersifat opsional.

socketTimeout

- Nilai Default - 0

- Tipe Data - Integer

Jumlah detik untuk menunggu selama operasi pembacaan soket sebelum waktu habis. Jika operasi memakan waktu lebih lama dari ambang ini, maka koneksi ditutup. Ketika properti ini disetel ke 0, koneksi tidak akan habis waktu.

Parameter ini bersifat opsional.

SSL

- Nilai Default - TRUE
- Tipe Data - String

Gunakan properti ini untuk mengaktifkan atau mematikan SSL untuk koneksi.

Parameter ini bersifat opsional.

Anda dapat menentukan salah satu nilai berikut:

BETUL

Driver terhubung ke server melalui SSL.

SALAH

Driver terhubung ke server tanpa menggunakan SSL. Opsi ini tidak didukung dengan otentikasi IAM.

Atau, Anda dapat mengkonfigurasi AuthMech properti.

SSL_tidak aman

- Nilai Default - benar
- Tipe Data - String

Properti ini menunjukkan apakah sertifikat server host IDP harus diverifikasi.

Parameter ini bersifat opsional.

Anda dapat menentukan salah satu nilai berikut:

true

Pengemudi tidak memeriksa keaslian sertifikat server IDP.

false

Pengemudi memeriksa keaslian sertifikat server IDP.

SSLCert

- Nilai Default - Tidak Ada
- Tipe Data - String

Jalur lengkap file.pem atau .crt yang berisi sertifikat CA tepercaya tambahan untuk memverifikasi instance server Amazon Redshift saat menggunakan SSL.

Parameter ini diperlukan jika SSLKey ditentukan.

SSLFactory

- Nilai Default - Tidak Ada
- Tipe Data - String

Pabrik SSL untuk digunakan saat menghubungkan ke server melalui TLS/SSL tanpa menggunakan sertifikat server.

SSLKey

- Nilai Default - Tidak Ada
- Tipe Data - String

Jalur lengkap file.der yang berisi file kunci PKCS8 untuk memverifikasi sertifikat yang ditentukan dalam SSLCert.

Parameter ini diperlukan jika SSLCert ditentukan.

SSLMode

- Nilai default - verify-ca

- Tipe Data - String

Gunakan properti ini untuk menentukan bagaimana driver memvalidasi sertifikat saat TLS/SSL diaktifkan.

Parameter ini bersifat opsional.

Anda dapat menentukan salah satu nilai berikut:

`verify-ca`

Pengemudi memverifikasi bahwa sertifikat tersebut berasal dari otoritas sertifikat tepercaya (CA).

`verify-full`

Pengemudi memverifikasi bahwa sertifikat berasal dari CA tepercaya dan bahwa nama host dalam sertifikat cocok dengan nama host yang ditentukan dalam URL koneksi.

`SSLPassword`

- Nilai Default - 0
- Tipe Data - String

Kata sandi untuk file kunci terenkripsi yang ditentukan dalam `SSLKey`.

Parameter ini diperlukan jika `SSLKey` ditentukan dan file kunci dienkripsi.

`SSL RootCert`

- Nilai Default - Tidak Ada
- Tipe Data - String

Jalur lengkap file.pem atau .crt yang berisi sertifikat CA root untuk memverifikasi instance Amazon Redshift Server saat menggunakan SSL.

`StsEndpointUrl`

- Nilai Default - null
- Tipe Data - String

Anda dapat menentukan titik akhir AWS Security Token Service (AWS STS). Jika Anda menentukan opsi ini, opsi Wilayah diabaikan. Anda hanya dapat menentukan protokol aman (HTTPS) untuk titik akhir ini.

tcp KeepAlive

- Nilai Default - TRUE
- Tipe Data - String

Gunakan properti ini untuk mengaktifkan atau mematikan keepalives TCP.

Parameter ini bersifat opsional.

Anda dapat menentukan salah satu nilai berikut:

BETUL

Driver menggunakan TCP keepalives untuk mencegah koneksi dari timing out.

SALAH

Driver tidak menggunakan keepalives TCP.

token

- Nilai Default - Tidak Ada
- Tipe Data - String

Pusat Identitas IAM menyediakan token akses atau OpenID Connect (OIDC) JSON Web Token (JWT) yang disediakan oleh penyedia identitas web yang terhubung dengan IAM Identity Center. Aplikasi Anda harus menghasilkan token ini dengan mengautentikasi pengguna aplikasi Anda dengan IAM Identity Center atau penyedia identitas yang ditautkan dengan IAM Identity Center.

Parameter ini bekerja dengan `IdpTokenAuthPlugin`.

token_type

- Nilai Default - Tidak Ada
- Tipe Data - String

Jenis token yang digunakan di `IdpTokenAuthPlugin`.

Anda dapat menentukan salah satu nilai berikut:

`ACCESS_TOKEN`

Masukkan ini jika Anda menggunakan token akses yang disediakan Pusat Identitas IAM.

`EXT_JWT`

Masukkan ini jika Anda menggunakan OpenID Connect (OIDC) JSON Web Token (JWT) yang disediakan oleh penyedia identitas berbasis web yang terintegrasi dengan IAM Identity Center.

Parameter ini bekerja dengan `IdpTokenAuthPlugin`.

`UID`

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama pengguna database yang Anda gunakan untuk mengakses database.

Parameter ini diperlukan.

`Pengguna`

- Nilai Default - Tidak Ada
- Tipe Data - String

Saat menghubungkan menggunakan otentikasi IAM melalui IDP, ini adalah nama pengguna untuk server `idp_host`. Saat menggunakan otentikasi standar, ini dapat digunakan untuk nama pengguna database Amazon Redshift.

Parameter ini bersifat opsional.

`web IdentityToken`

- Nilai Default - Tidak Ada
- Tipe Data - String

Token akses OAuth 2.1 atau token ID OpenID Connect yang disediakan oleh penyedia identitas. Aplikasi Anda harus mendapatkan token ini dengan mengautentikasi pengguna aplikasi Anda dengan penyedia identitas web. Pastikan untuk menentukan parameter ini saat Anda menentukan opsi `BasicJwtCredentialsProvider Plugin_Name`.

Parameter ini diperlukan jika Anda menentukan `BasicJwtCredentialsProvider` untuk opsi `Plugin_Name`.

Versi sebelumnya dari JDBC driver version 2.1

Unduh versi sebelumnya dari driver Amazon Redshift JDBC versi 2.1 hanya jika alat Anda memerlukan versi driver tertentu.

Ini adalah driver JDBC versi 2.1 yang kompatibel dengan JDBC 4.2 sebelumnya:

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.28/redshift-jdbc42-2.1.0.28.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.26/redshift-jdbc42-2.1.0.26.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.25/redshift-jdbc42-2.1.0.25.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.24/redshift-jdbc42-2.1.0.24.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.23/redshift-jdbc42-2.1.0.23.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.22/redshift-jdbc42-2.1.0.22.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.21/redshift-jdbc42-2.1.0.21.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.20/redshift-jdbc42-2.1.0.20.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.19/redshift-jdbc42-2.1.0.19.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.18/redshift-jdbc42-2.1.0.18.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.17/redshift-jdbc42-2.1.0.17.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.16/redshift-jdbc42-2.1.0.16.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.15/redshift-jdbc42-2.1.0.15.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.14/redshift-jdbc42-2.1.0.14.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.13/redshift-jdbc42-2.1.0.13.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.12/redshift-jdbc42-2.1.0.12.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.11/redshift-jdbc42-2.1.0.11.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.10/redshift-jdbc42-2.1.0.10.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.9/redshift-jdbc42-2.1.0.9.zip>

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.8/redshift-jdbc42-2.1.0.8.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.7/redshift-jdbc42-2.1.0.7.zip>

Mengonfigurasi konektor Amazon Redshift Python

Dengan menggunakan konektor Amazon Redshift untuk Python, Anda dapat mengintegrasikan pekerjaan dengan [AWS SDK for Python \(Boto3\)](#), dan juga [panda](#) dan [Numerical Python \(.\)](#). NumPy Untuk informasi lebih lanjut tentang panda, lihat repositori [panda GitHub](#). Untuk informasi lebih lanjut tentang NumPy, lihat [NumPy GitHubrepositori](#).

Konektor Amazon Redshift Python menyediakan solusi open source. Anda dapat menelusuri kode sumber, meminta penyempurnaan, melaporkan masalah, dan memberikan kontribusi.

Untuk menggunakan konektor Amazon Redshift Python, pastikan Anda memiliki Python versi 3.6 atau yang lebih baru. Untuk informasi selengkapnya, lihat [perjanjian SIM Amazon Redshift Python](#).

Konektor Amazon Redshift Python menyediakan yang berikut:

- AWS Identity and Access Management (IAM) otentikasi. Untuk informasi selengkapnya, lihat [Manajemen identitas dan akses di Amazon Redshift](#).
- Otentikasi penyedia identitas menggunakan akses API federasi. Akses API federasi didukung untuk penyedia identitas perusahaan seperti berikut ini:
 - Azure AD. Untuk informasi selengkapnya, lihat postingan blog AWS Big Data Akses [Federate Amazon Redshift dengan sistem masuk tunggal Microsoft Azure AD](#).
 - Layanan Federasi Direktori Aktif. Untuk informasi selengkapnya, lihat posting blog AWS Big Data [akses Federasi ke klaster Amazon Redshift Anda dengan Active Directory Federation Services \(AD FS\): Bagian 1](#).
 - Okta. Untuk informasi lebih lanjut, lihat posting blog AWS Big Data [akses Federate Amazon Redshift dengan Okta sebagai](#) penyedia identitas.
 - PingFederate. Untuk informasi lebih lanjut, lihat [PingFederate situs](#).
 - JumpCloud. Untuk informasi lebih lanjut, lihat [JumpCloudsitus](#).
- Jenis data Amazon Redshift.

Konektor Amazon Redshift Python mengimplementasikan Python Database API Specification 2.0. Untuk informasi selengkapnya, lihat [PEP 249—Spesifikasi API Database Python v2.0](#) di situs web Python.

Topik

- [Memasang konektor Amazon Redshift Python](#)
- [Opsi konfigurasi untuk konektor Amazon Redshift Python](#)
- [Mengimpor konektor Python](#)
- [Mengintegrasikan konektor Python dengan NumPy](#)
- [Mengintegrasikan konektor Python dengan panda](#)
- [Menggunakan plugin penyedia identitas](#)
- [Contoh penggunaan konektor Amazon Redshift Python](#)
- [Referensi API untuk konektor Amazon Redshift Python](#)

Memasang konektor Amazon Redshift Python

Anda dapat menggunakan salah satu metode berikut untuk menginstal konektor Amazon Redshift Python:

- Indeks Package Python (PyPI)
- Conda
- Mengkloning repositori GitHub

Menginstal konektor Python dari PyPI

Untuk menginstal konektor Python dari Python Package Index (PyPI), Anda dapat menggunakan pip. Untuk melakukan ini, jalankan perintah berikut.

```
>>> pip install redshift_connector
```

Anda dapat menginstal konektor dalam lingkungan virtual. Untuk melakukan ini, jalankan perintah berikut.

```
>>> pip install redshift_connector
```

Secara opsional, Anda dapat menginstal panda dan NumPy dengan konektor.

```
>>> pip install "redshift_connector[full]"
```

Untuk informasi lebih lanjut tentang pip, lihat situs [pip](#).

Menginstal konektor Python dari Conda

Anda dapat menginstal konektor Python dari Anaconda.org.

```
>>>conda install -c conda-forge redshift_connector
```

Menginstal konektor Python dengan mengkloning repositori dari GitHub AWS

Untuk menginstal konektor Python dari sumber, kloning repositori dari GitHub AWS Setelah Anda menginstal Python dan virtualenv, atur lingkungan Anda dan instal dependensi yang diperlukan dengan menjalankan perintah berikut.

```
$ 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
```

Opsi konfigurasi untuk konektor Amazon Redshift Python

Berikut ini, Anda dapat menemukan deskripsi untuk opsi yang dapat Anda tentukan untuk konektor Amazon Redshift Python.

access_key_id

- Nilai default - Tidak ada
- Tipe data - String

Kunci akses untuk peran IAM atau pengguna yang dikonfigurasi untuk otentikasi database IAM.

Parameter ini bersifat opsional.

allow_db_user_override

- Nilai default - Salah
- Tipe data — Boolean

True

Menentukan bahwa konektor menggunakan DbUser nilai dari pernyataan Security Assertion Markup Language (SAMP).

False

Menentukan bahwa nilai dalam parameter DbUser koneksi digunakan.

Parameter ini bersifat opsional.

app_name

- Nilai default - Tidak ada
- Tipe data - String

Nama aplikasi penyedia identitas (IDP) yang digunakan untuk otentikasi.

Parameter ini bersifat opsional.

auth_profil

- Nilai default - Tidak ada
- Tipe data - String

Nama profil otentikasi Amazon Redshift yang memiliki properti koneksi sebagai JSON. Untuk informasi selengkapnya tentang penamaan parameter koneksi, lihat `RedshiftProperty` kelas. `RedshiftPropertyKelas` menyimpan parameter koneksi yang disediakan oleh pengguna akhir dan, jika berlaku, dihasilkan selama proses otentikasi IAM (misalnya, kredensial IAM sementara). Untuk informasi lebih lanjut, lihat [RedshiftProperty kelas](#).

Parameter ini bersifat opsional.

auto_create

- Nilai default - Salah
- Tipe data — Boolean

Nilai yang menunjukkan apakah akan membuat pengguna jika pengguna tidak ada.

Parameter ini bersifat opsional.

`client_id`

- Nilai default - Tidak ada
- Tipe data - String

ID klien dari Azure iDP.

Parameter ini bersifat opsional.

`client_secret`

- Nilai default - Tidak ada
- Tipe data - String

Rahasia klien dari Azure iDP.

Parameter ini bersifat opsional.

`cluster_identifier`

- Nilai default - Tidak ada
- Tipe data - String

Pengidentifikasi cluster dari cluster Amazon Redshift.

Parameter ini bersifat opsional.

`credentials_provider`

- Nilai default - Tidak ada
- Tipe data - String

IDP yang digunakan untuk otentikasi dengan Amazon Redshift. Berikut ini adalah nilai yang valid:

- `AdfsCredentialsProvider`
- `AzureCredentialsProvider`
- `BrowserAzureCredentialsProvider`

- `BrowserAzureOauth2CredentialsProvider`
- `BrowserSamlCredentialsProvider`
- `IdpTokenAuthPlugin`- Plugin otorisasi yang menerima token Identity Center (IDC) atau token identitas berbasis JSON (OIDC) OpenID Connect (OIDC) dari penyedia identitas web mana pun yang ditautkan ke IDC.
- `PingCredentialsProvider`
- `OktaCredentialsProvider`

Parameter ini bersifat opsional.

basis data

- Nilai default - Tidak ada
- Tipe data - String

Nama database yang ingin Anda sambungkan.

Parameter ini diperlukan.

`database_metadata_current_db_only`

- Nilai default - Benar
- Tipe data — Boolean

Nilai yang menunjukkan apakah aplikasi mendukung katalog datashare multidatabase. Nilai default True menunjukkan bahwa aplikasi tidak mendukung katalog datashare multidatabase untuk kompatibilitas mundur.

Parameter ini bersifat opsional.

`db_group`

- Nilai default - Tidak ada
- Tipe data - String

Daftar dipisahkan koma dari nama grup database yang ada yang ditunjukkan oleh pengguna dengan `DbUser` bergabung untuk sesi saat ini.

Parameter ini bersifat opsional.

db_pengguna

- Nilai default - Tidak ada
- Tipe data - String

ID pengguna untuk digunakan dengan Amazon Redshift.

Parameter ini bersifat opsional.

endpoint_url

- Nilai default - Tidak ada
- Tipe data - String

URL titik akhir Amazon Redshift. Opsi ini hanya untuk penggunaan AWS internal.

Parameter ini bersifat opsional.

group_federasi

- Nilai default - Salah
- Tipe data — Boolean

Opsi ini menentukan apakah akan menggunakan grup IDP Amazon Redshift.

Parameter ini bersifat opsional.

true

Gunakan grup Amazon Redshift Identity Provider (IDP).

false

Gunakan STS API dan GetClusterCredentials untuk federasi pengguna dan tentukan db_groups untuk koneksi.

host

- Nilai default - Tidak ada

- Tipe data - String

Nama host dari cluster Amazon Redshift.

Parameter ini bersifat opsional.

iam

- Nilai default - Salah
- Tipe data — Boolean

Autentikasi IAM diaktifkan.

Parameter ini diperlukan.

iam_disable_cache

- Nilai default - Salah
- Tipe data — Boolean

Opsi ini menentukan apakah kredensial IAM di-cache. Secara default, kredensial IAM di-cache. Ini meningkatkan kinerja saat permintaan ke gateway API dibatasi.

Parameter ini bersifat opsional.

identity_namespace

- Nilai default - null
- Tipe data - String

Namespace identitas yang akan digunakan saat mengautentikasi menggunakan.

IdpTokenAuthPlugin Ini membantu Redshift memutuskan instance Identity Center mana yang akan digunakan.

Jika hanya ada satu instance Pusat Identitas yang ada atau jika namespace identitas default disetel, maka parameter ini opsional. Sebaliknya, hal itu tidak diperlukan.

IDPport

- Nilai default - 7890

- Tipe data - Integer

Port mendengarkan tempat iDP mengirimkan pernyataan SAMP.

Parameter ini diperlukan.

`idp_response_timeout`

- Nilai default - 120
- Tipe data - Integer

Batas waktu untuk mengambil pernyataan SAMP dari iDP.

Parameter ini diperlukan.

`idp_penyewa`

- Nilai default - Tidak ada
- Tipe data - String

Penyewa IDP.

Parameter ini bersifat opsional.

`listen_port`

- Nilai default - 7890
- Tipe data - Integer

Port mendengarkan tempat iDP mengirimkan pernyataan SAMP.

Parameter ini bersifat opsional.

`login_url`

- Nilai default - Tidak ada
- Tipe data - String

Url masuk tunggal untuk iDP.

Parameter ini bersifat opsional.

`max_prepared_statement`

- Nilai default - 1000
- Tipe data - Integer

Jumlah maksimum pernyataan yang disiapkan yang dapat dibuka secara bersamaan.

Parameter ini diperlukan.

`numeric_to_float`

- Nilai default - Salah
- Tipe data — Boolean

Opsi ini menentukan apakah konektor mengkonversi nilai tipe data numerik dari Decimal.Decimal untuk float. Secara default, konektor menerima nilai tipe data numerik sebagai desimal. Desimal dan tidak mengonversinya.

Kami tidak menyarankan mengaktifkan `numeric_to_float` untuk kasus penggunaan yang memerlukan presisi, karena hasilnya dapat dibulatkan.

Untuk informasi lebih lanjut tentang desimal. Desimal dan pengorbanan antara itu dan float, lihat desimal [— Titik tetap desimal](#) dan aritmatika floating point di situs web Python.

Parameter ini bersifat opsional.

`partner_sp_id`

- Nilai default - Tidak ada
- Tipe data - String

ID SP Mitra yang digunakan untuk otentikasi dengan Ping.

Parameter ini bersifat opsional.

`password`

- Nilai default - Tidak ada

- Tipe data - String

Kata sandi yang digunakan untuk otentikasi.

Parameter ini bersifat opsional.

port

- Nilai default - 5439
- Tipe data - Integer

Nomor port cluster Amazon Redshift.

Parameter ini diperlukan.

preferred_role

- Nilai default - Tidak ada
- Tipe data - String

Peran IAM lebih disukai untuk koneksi saat ini.

Parameter ini bersifat opsional.

principal_arn

- Nilai default - Tidak ada
- Tipe data - String

Nama Sumber Daya Amazon (ARN) dari pengguna atau peran IAM tempat Anda membuat kebijakan. Anda disarankan untuk melampirkan kebijakan ke peran dan kemudian menetapkan peran tersebut ke pengguna Anda, untuk akses.

Parameter ini bersifat opsional.

profile

- Nilai default - Tidak ada
- Tipe data - String

Nama profil dalam file AWS kredensial yang berisi AWS kredensial.

Parameter ini bersifat opsional.

`provider_name`

- Nilai default - Tidak ada
- Tipe data - String

Nama Penyedia Otentikasi Asli Redshift.

Parameter ini bersifat opsional.

`region`

- Nilai default - Tidak ada
- Tipe data - String

Di Wilayah AWS mana cluster berada.

Parameter ini bersifat opsional.

`role_arn`

- Nilai default - Tidak ada
- Tipe data - String

Nama Sumber Daya Amazon (ARN) dari peran yang diasumsikan oleh penelepon. Parameter ini digunakan oleh penyedia yang ditunjukkan oleh `JwtCredentialsProvider`.

Untuk `JwtCredentialsProvider` penyedia, parameter ini wajib. Jika tidak, parameter ini opsional.

`role_session_name`

- Nilai default - `jwt_redshift_session`
- Tipe data - String

Sebuah pengenal untuk sesi peran yang diambil. Biasanya, Anda meneruskan nama atau pengenal yang terkait dengan pengguna yang menggunakan aplikasi Anda. Kredensial keamanan sementara

yang digunakan aplikasi Anda terkait dengan pengguna tersebut. Parameter ini digunakan oleh penyedia yang ditunjukkan oleh `JwtCredentialsProvider`.

Parameter ini bersifat opsional.

cakupan

- Nilai default - Tidak ada
- Tipe data - String

Daftar cakupan yang dipisahkan ruang yang dapat disetujui pengguna. Anda menentukan parameter ini sehingga aplikasi Anda bisa mendapatkan persetujuan untuk API yang ingin Anda panggil. Anda dapat menentukan parameter ini ketika Anda menentukan `BrowserAzure OAuth2 CredentialsProvider` untuk opsi `credentials_provider`.

Parameter ini diperlukan untuk plug-in `BrowserAzure OAuth2CredentialsProvider` .

`secret_access_key_id`

- Nilai default - Tidak ada
- Tipe data - String

Kunci akses rahasia untuk peran IAM atau pengguna yang dikonfigurasi untuk otentikasi database IAM.

Parameter ini bersifat opsional.

`session_token`

- Nilai default - Tidak ada
- Tipe data - String

Kunci akses untuk peran IAM atau pengguna yang dikonfigurasi untuk otentikasi database IAM. Parameter ini diperlukan jika AWS kredensial sementara sedang digunakan.

Parameter ini bersifat opsional.

`serverless_acct_id`

- Nilai default - Tidak ada

- Tipe data - String

ID akun Tanpa Server Amazon Redshift.

Parameter ini bersifat opsional.

`serverless_work_group`

- Nilai default - Tidak ada
- Tipe data - String

Nama workgroup Amazon Redshift Tanpa Server.

Parameter ini bersifat opsional.

`ssl`

- Nilai default - Benar
- Tipe data — Boolean

Secure Sockets Layer (SSL) diaktifkan.

Parameter ini diperlukan.

`ssl_insecure`

- Nilai default - Benar
- Tipe data — Boolean

Nilai yang menentukan apakah sertifikat server host iDP akan diverifikasi.

Parameter ini bersifat opsional.

`sslmode`

- Nilai default - verify-ca
- Tipe data - String

Keamanan koneksi ke Amazon Redshift. Anda dapat menentukan salah satu dari berikut ini:

- `verify-ca`
- `verify-full`

Parameter ini diperlukan.

batas waktu

- Nilai default - Tidak ada
- Tipe data - Integer

Jumlah detik sebelum koneksi ke server habis.

Parameter ini bersifat opsional.

token

- Nilai Default - Tidak Ada
- Tipe Data - String

Pusat Identitas IAM menyediakan token akses atau OpenID Connect (OIDC) JSON Web Token (JWT) yang disediakan oleh penyedia identitas web yang terhubung dengan IAM Identity Center. Aplikasi Anda harus menghasilkan token ini dengan mengautentikasi pengguna aplikasi Anda dengan IAM Identity Center atau penyedia identitas yang ditautkan dengan IAM Identity Center.

Parameter ini bekerja dengan `IdpTokenAuthPlugin`.

`token_type`

- Nilai Default - Tidak Ada
- Tipe Data - String

Jenis token yang digunakan di `IdpTokenAuthPlugin`.

Anda dapat menentukan salah satu nilai berikut:

`ACCESS_TOKEN`

Masukkan ini jika Anda menggunakan token akses yang disediakan Pusat Identitas IAM.

EXT_JWT

Masukkan ini jika Anda menggunakan OpenID Connect (OIDC) JSON Web Token (JWT) yang disediakan oleh penyedia identitas berbasis web yang terintegrasi dengan IAM Identity Center.

Parameter ini bekerja dengan `IdpTokenAuthPlugin`.

`user`

- Nilai default - Tidak ada
- Tipe data - String

Nama pengguna yang digunakan untuk otentikasi.

Parameter ini bersifat opsional.

`web_identity_token`

- Nilai default - Tidak ada
- Tipe data - String

Token akses OAuth 2.0 atau token ID OpenID Connect yang disediakan oleh penyedia identitas. Pastikan aplikasi Anda mendapatkan token ini dengan mengautentikasi pengguna yang menggunakan aplikasi Anda dengan penyedia identitas web. Penyedia yang ditunjukkan dengan `JwtCredentialsProvider` menggunakan parameter ini.

Untuk `JwtCredentialsProvider` penyedia, parameter ini wajib. Jika tidak, parameter ini opsional.

Mengimpor konektor Python

Untuk mengimpor konektor Python, jalankan perintah berikut.

```
>>> import redshift_connector
```

Mengimpor NumPy dan menghubungkan ke Amazon Redshift

Untuk mengimpor konektor Amazon Redshift Python dan Numerical Python (`numpy`), jalankan perintah berikut.

```
import redshift_connector
import numpy
```

Untuk menyambung ke klaster Amazon Redshift menggunakan AWS kredensial, jalankan perintah berikut.

```
conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
)
```

Mengintegrasikan konektor Python dengan NumPy

Berikut ini adalah contoh mengintegrasikan konektor Python dengan 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)
```

Berikut ini adalah hasilnya.

```
[['One Hundred Years of Solitude' 'Gabriel García Márquez']]
```

```
['A Brief History of Time' 'Stephen Hawking']]
```

Mengintegrasikan konektor Python dengan panda

Berikut ini adalah contoh mengintegrasikan konektor Python dengan panda.

```
>>> 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)
```

Menggunakan plugin penyedia identitas

Untuk informasi umum tentang cara menggunakan plugin penyedia identitas, lihat [Opsi untuk memberikan kredensial IAM](#). Untuk informasi selengkapnya tentang mengelola identitas IAM, termasuk praktik terbaik untuk peran IAM, lihat [Manajemen identitas dan akses di Amazon Redshift](#)

Otentikasi menggunakan plugin penyedia identitas ADFS

Berikut ini adalah contoh penggunaan plugin penyedia identitas Active Directory Federation Service (ADFS) untuk mengautentikasi pengguna yang terhubung ke database Amazon Redshift.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
```

```
credentials_provider='AdfsCredentialsProvider',
user='brooke@myadfshostname.com',
password='Hunter2',
idp_host='myadfshostname.com'
)
```

Otentikasi menggunakan plugin penyedia identitas Azure

Berikut ini adalah contoh otentikasi menggunakan plugin penyedia identitas Azure. Anda dapat membuat nilai untuk `client_id` dan `client_secret` untuk aplikasi Azure Enterprise seperti yang ditunjukkan berikut.

```
>>> 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'
)
```

Otentikasi menggunakan plugin penyedia identitas Azure Browser

Berikut ini adalah contoh penggunaan plugin penyedia identitas Azure Browser untuk mengautentikasi pengguna yang terhubung ke database Amazon Redshift.

Otentikasi multi-faktor terjadi di browser, di mana kredensi masuk disediakan oleh pengguna.

```
>>> 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',
)
```

Otentikasi menggunakan plugin penyedia identitas Okta

Berikut ini adalah contoh otentikasi menggunakan plugin penyedia identitas Okta. Anda dapat memperoleh nilai untuk `idp_host`, `app_id` dan `app_name` melalui aplikasi Okta.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='OktaCredentialsProvider',
    user='brooke@myazure.org',
    password='hunter2',
    idp_host='my_idp_host',
    app_id='my_first_appetizer',
    app_name='dinner_party'
)
```

Otentikasi menggunakan JumpCloud dengan plugin penyedia identitas browser SAMP generik

Berikut ini adalah contoh penggunaan JumpCloud dengan plugin penyedia identitas browser SAMP generik untuk otentikasi.

Parameter kata sandi diperlukan. Namun, Anda tidak perlu memasukkan parameter ini karena otentikasi multi-faktor terjadi di browser.

```
>>> 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'
)
```

Contoh penggunaan konektor Amazon Redshift Python

Berikut ini adalah contoh cara menggunakan konektor Amazon Redshift Python. Untuk menjalankannya, Anda harus menginstal konektor Python terlebih dahulu. Untuk informasi

selengkapnya tentang menginstal konektor Amazon Redshift Python, lihat. [Memasang konektor Amazon Redshift Python](#) Untuk informasi lebih lanjut tentang opsi konfigurasi yang dapat Anda gunakan dengan konektor Python, lihat. [Opsi konfigurasi untuk konektor Amazon Redshift Python](#)

Topik

- [Menyambung ke dan menanyakan klaster Amazon Redshift menggunakan kredensial AWS](#)
- [Mengaktifkan komit otomatis](#)
- [Mengkonfigurasi paramstyle kursor](#)
- [Menggunakan COPY untuk menyalin data dari bucket Amazon S3 dan UNLOAD untuk menulis data ke dalamnya](#)

Menyambung ke dan menanyakan klaster Amazon Redshift menggunakan kredensial AWS

Contoh berikut memandu Anda untuk menghubungkan ke klaster Amazon Redshift menggunakan AWS kredensial Anda, lalu menanyakan tabel dan mengambil hasil kueri.

```
#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' ])
```


Mengaktifkan komit otomatis

Properti autocommit dinonaktifkan secara default, mengikuti Spesifikasi API Database Python. Anda dapat menggunakan perintah berikut untuk mengaktifkan properti autocommit koneksi setelah melakukan perintah rollback untuk memastikan bahwa transaksi tidak sedang berlangsung.

```
#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
```

Mengkonfigurasi paramstyle kursor

Paramstyle untuk kursor dapat dimodifikasi melalui `cursor.paramstyle`. Paramstyle default yang digunakan adalah `format`. Nilai yang valid untuk paramstyle adalah `qmark`, `numeric`, `namedformat`, dan `pyformat`.

Berikut ini adalah contoh menggunakan berbagai paramstyles untuk meneruskan parameter ke pernyataan SQL sampel.

```
# 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"})

```

Menggunakan COPY untuk menyalin data dari bucket Amazon S3 dan UNLOAD untuk menulis data ke dalamnya

Contoh berikut menunjukkan cara menyalin data dari bucket Amazon S3 ke dalam tabel dan kemudian membongkar dari tabel itu kembali ke bucket.

File teks bernama `category_csv.txt` berisi data berikut diunggah ke bucket Amazon S3:.

```

12,Shows,Musicals,Musical theatre
13,Shows,Plays,"All ""non-musical"" theatre"
14,Shows,Opera,"All opera, light, and ""rock"" opera"
15,Concerts,Classical,"All symphony, concerto, and choir concerts"

```

Berikut ini adalah contoh kode Python, yang pertama kali terhubung ke database Amazon Redshift. Kemudian membuat tabel yang disebut `category` dan menyalin data CSV dari bucket S3 ke dalam tabel.

```

#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'])
```

Jika Anda belum `autocommit` menyetel ke `true`, komit dengan `conn.commit()` setelah menjalankan `execute()` pernyataan.

Data diturunkan ke file `unloaded_category_csv.text0000_part00` di bucket S3, dengan konten berikut:

```
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"
```

Referensi API untuk konektor Amazon Redshift Python

Berikut ini, Anda dapat menemukan deskripsi operasi API konektor Amazon Redshift Python.

`redshift_connector`

Berikut ini, Anda dapat menemukan deskripsi operasi `redshift_connector` API.

```
connect(user, database, password[, port, ...])
```

Membuat koneksi ke cluster Amazon Redshift. Fungsi ini memvalidasi input pengguna, secara opsional mengautentikasi menggunakan plugin penyedia identitas, dan kemudian membangun objek koneksi.

`apilevel`

Level DBAPI didukung, saat ini "2.0".

```
paramstyle, str(object='') -> str str(bytes_or_buffer[, encoding[, errors]])
-> str
```

Gaya parameter API database untuk digunakan secara global.

Koneksi

Berikut ini, Anda dapat menemukan deskripsi operasi API koneksi untuk konektor Amazon Redshift Python.

```
__init__(user, password, database[, host, ...])
```

Menginisialisasi objek koneksi mentah.

```
cursor
```

Membuat objek kursor terikat pada koneksi ini.

```
commit
```

Melakukan transaksi database saat ini.

```
rollback
```

Menggulung kembali transaksi database saat ini.

```
close
```

Menutup koneksi database.

```
execute(cursor, operation, vals)
```

Menjalankan perintah SQL yang ditentukan. Anda dapat memberikan parameter sebagai urutan atau sebagai pemetaan, tergantung pada nilai `redshift_connector.paramstyle`

```
run(sql[, stream])
```

Menjalankan perintah SQL yang ditentukan. Secara opsional, Anda dapat menyediakan aliran untuk digunakan dengan perintah COPY.

```
xid(format_id, global_transaction_id, ...)
```

Buat ID transaksi. Hanya `global_transaction_id` parameter yang digunakan di postgres. `format_id` dan `branch_qualifier` tidak digunakan di postgres. `global_transaction_id` Dapat berupa pengidentifikasi string apa pun yang didukung oleh postgres yang mengembalikan tuple (`format_id`, `global_transaction_id`). `branch_qualifier`

`tpc_begin(xid)`

Memulai transaksi TPC dengan ID transaksi `xid` yang terdiri dari ID format, ID transaksi global, dan kualifikasi cabang.

`tpc_prepare`

Melakukan fase pertama transaksi yang dimulai dengan `tpc_begin`.

`tpc_commit([xid])`

Ketika dipanggil tanpa argumen, `tpc_commit` melakukan transaksi TPC yang sebelumnya disiapkan dengan `tpc_prepare` ().

`tpc_rollback([xid])`

Ketika dipanggil tanpa argumen, `tpc_rollback` mengembalikan transaksi TPC.

`tpc_recover`

Mengembalikan daftar ID transaksi tertunda yang cocok untuk digunakan dengan `tpc_commit(xid)` atau `tpc_rollback(xid)`.

Kursor

Berikut ini, Anda dapat menemukan deskripsi operasi API kursor.

`__init__(connection[, paramstyle])`

Menginisialisasi objek kursor mentah.

`insert_data_bulk(filename, table_name, parameter_indices, column_names, delimiter, batch_size)`

Menjalankan pernyataan INSERT massal.

`execute(operation[, args, stream, ...])`

Menjalankan operasi database.

`executemany(operation, param_sets)`

Mempersiapkan operasi database, dan kemudian menjalankannya untuk semua urutan parameter atau pemetaan yang disediakan.

`fetchone`

Mengambil baris berikutnya dari hasil kueri set.

```
fetchmany([num])
```

Mengambil set baris berikutnya dari hasil query.

```
fetchall
```

Mengambil semua baris yang tersisa dari hasil query.

```
close
```

Tutup kursor sekarang.

```
__iter__
```

Sebuah objek kursor dapat diiterasi untuk mengambil baris dari query.

```
fetch_dataframe([num])
```

Mengembalikan kerangka data dari hasil query terakhir.

```
write_dataframe(df, table)
```

Menulis kerangka data struktur yang sama ke dalam database Amazon Redshift.

```
fetch_numpy_array([num])
```

Mengembalikan NumPy array hasil query terakhir.

```
get_catalogs
```

Amazon Redshift tidak mendukung beberapa katalog dari satu koneksi. Amazon Redshift hanya mengembalikan katalog saat ini.

```
get_tables([catalog, schema_pattern, ...])
```

Mengembalikan tabel publik unik yang ditentukan pengguna dalam sistem.

```
get_columns([catalog, schema_pattern, ...])
```

Mengembalikan daftar semua kolom dalam tabel tertentu dalam database Amazon Redshift.

AdfsCredentialsProvider plugin

Berikut ini adalah sintaks untuk operasi API AdfsCredentialsProvider plugin untuk konektor Amazon Redshift Python.

```
redshift_connector.plugin.AdfsCredentialsProvider()
```

AzureCredentialsProvider plugin

Berikut ini adalah sintaks untuk operasi API AzureCredentialsProvider plugin untuk konektor Amazon Redshift Python.

```
redshift_connector.plugin.AzureCredentialsProvider()
```

BrowserAzureCredentialsProvider plugin

Berikut ini adalah sintaks untuk operasi API BrowserAzureCredentialsProvider plugin untuk konektor Amazon Redshift Python.

```
redshift_connector.plugin.BrowserAzureCredentialsProvider()
```

BrowserSamlCredentialsProvider plugin

Berikut ini adalah sintaks untuk operasi API BrowserSamlCredentialsProvider plugin untuk konektor Amazon Redshift Python.

```
redshift_connector.plugin.BrowserSamlCredentialsProvider()
```

OktaCredentialsProvider plugin

Berikut ini adalah sintaks untuk operasi API OktaCredentialsProvider plugin untuk konektor Amazon Redshift Python.

```
redshift_connector.plugin.OktaCredentialsProvider()
```

PingCredentialsProvider plugin

Berikut ini adalah sintaks untuk operasi API PingCredentialsProvider plugin untuk konektor Amazon Redshift Python.

```
redshift_connector.plugin.PingCredentialsProvider()
```

SamlCredentialsProvider plugin

Berikut ini adalah sintaks untuk operasi API SamlCredentialsProvider plugin untuk konektor Amazon Redshift Python.

```
redshift_connector.plugin.SamlCredentialsProvider()
```

Integrasi Amazon Redshift untuk Apache Spark

[Percikan Apache](#) adalah kerangka pemrosesan terdistribusi dan model pemrograman yang membantu Anda melakukan pembelajaran mesin, pemrosesan aliran, atau analisis grafik. Mirip dengan Apache Hadoop, Spark merupakan sistem pemrosesan terdistribusi sumber terbuka, yang biasa digunakan untuk beban kerja big data. Spark memiliki grafik asiklik terarah yang dioptimalkan (DAG) mesin eksekusi dan secara aktif menyimpan data dalam memori. Ini dapat meningkatkan kinerja, terutama untuk algoritma tertentu dan kueri interaktif.

Integrasi ini memberi Anda konektor Spark yang dapat Anda gunakan untuk membangun aplikasi Apache Spark yang membaca dan menulis ke data di Amazon Redshift dan Amazon Redshift Serverless. Aplikasi ini tidak berkompromi pada kinerja aplikasi atau konsistensi transaksional data. Integrasi ini secara otomatis disertakan dalam [EMR](#) dan [AWS Glue](#), sehingga Anda dapat segera menjalankan pekerjaan Apache Spark yang mengakses dan memuat data ke Amazon Redshift sebagai bagian dari pipa penyerapan dan transformasi data Anda.

Saat ini, Anda dapat menggunakan versi 3.3.0, 3.3.1, 3.3.2, dan 3.4.0 dari Spark dengan integrasi ini.

Integrasi ini memberikan yang berikut:

- AWS Identity and Access Management (IAM). Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).
- Predikat dan kueri pushdown untuk meningkatkan kinerja.
- Jenis data Amazon Redshift.
- Konektivitas ke Amazon Redshift dan Amazon Redshift Tanpa Server.

Pertimbangan dan batasan saat menggunakan konektor Spark

- URI tempdir menunjuk ke lokasi Amazon S3. Direktori temp ini tidak dibersihkan secara otomatis dan dapat menambah biaya tambahan. Kami merekomendasikan penggunaan [Kebijakan siklus](#)

[hidup Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon untuk menentukan aturan retensi untuk bucket Amazon S3.

- Secara default, salinan antara Amazon S3 dan Redshift tidak berfungsi jika bucket S3 dan cluster Redshift berbeda AWS Daerah. Untuk menggunakan terpisah AWS Daerah, atur `tempdir_region` parameter ke wilayah bucket S3 yang digunakan untuk `tempdir`.
- Cross-Region menulis antara S3 dan Redshift jika menulis data Parquet menggunakan `tempformat` parameter.
- Kami merekomendasikan penggunaan [Enkripsi sisi server Amazon S3](#) untuk mengenkripsi ember Amazon S3 yang digunakan.
- Kami merekomendasikan [memblokir akses publik ke bucket Amazon S3](#).
- Kami menyarankan agar cluster Amazon Redshift tidak dapat diakses oleh publik.
- Kami merekomendasikan untuk menyalakan [Pencatatan audit Amazon Redshift](#).
- Kami merekomendasikan untuk menyalakan [Enkripsi saat istirahat Amazon Redshift](#).
- Sebaiknya aktifkan SSL untuk koneksi JDBC dari Spark di Amazon EMR ke Amazon Redshift.
- Kami merekomendasikan untuk meneruskan peran IAM menggunakan parameter `aws_iam_role` untuk parameter otentikasi Amazon Redshift.

Otentikasi dengan konektor Spark

Diagram berikut menjelaskan otentikasi antara Amazon S3, Amazon Redshift, driver Spark, dan pelaksana Spark.

Otentikasi antara Redshift dan Spark

Anda dapat menggunakan driver JDBC versi 2 yang disediakan Amazon Redshift untuk terhubung ke Amazon Redshift dengan konektor Spark dengan menentukan kredensial masuk. Untuk menggunakan IAM, [konfigurasi url JDBC Anda untuk menggunakan otentikasi IAM](#). Untuk terhubung ke kluster Redshift dari Amazon EMR atau AWS Glue, pastikan IAM role Anda memiliki izin yang diperlukan untuk mengambil IAM role sementara. Daftar berikut menjelaskan semua izin yang diperlukan peran IAM Anda untuk mengambil kredensial dan menjalankan operasi Amazon S3.

- [Pergeseran merah: GetClusterCredentials](#) (untuk cluster Redshift yang disediakan)
- [Pergeseran merah: DescribeClusters](#) (untuk cluster Redshift yang disediakan)
- [Pergeseran merah: GetWorkgroup](#) (untuk grup kerja Amazon Redshift Tanpa Server)

- [Pergeseran merah:GetCredentials](#)(untuk grup kerja Amazon Redshift Tanpa Server)
- [s3:ListBucket](#)
- [s3:GetBucket](#)
- [s3:GetObject](#)
- [s3:PutObject](#)
- [s3:GetBucketLifecycleConfiguration](#)

Untuk informasi lebih lanjut tentang GetClusterCredentials, lihat [Kebijakan sumber daya GetClusterCredentials](#).

Anda juga harus memastikan bahwa Amazon Redshift dapat mengambil peran IAM selama COPY dan UNLOAD operasi.

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

Jika Anda menggunakan driver JDBC terbaru, driver akan secara otomatis mengelola transisi dari sertifikat yang ditandatangani sendiri Amazon Redshift ke sertifikat ACM. Namun, Anda harus [tentukan opsi SSL ke url JDBC](#).

Berikut ini adalah contoh cara menentukan URL driver JDBC dan `aws_iam_role` untuk terhubung ke Amazon Redshift.

```
df.write \
  .format("io.github.spark_redshift_community.spark.redshift ") \
  .option("url", "jdbc:redshift:iam://<the-rest-of-the-connection-string>") \
  .option("dbtable", "<your-table-name>") \
  .option("tempdir", "s3a://<your-bucket>/<your-directory-path>") \
```

```
.option("aws_iam_role", "<your-aws-role-arn>") \
.mode("error") \
.save()
```

Otentikasi antara Amazon S3 dan Spark

Jika Anda menggunakan peran IAM untuk mengautentikasi antara Spark dan Amazon S3, gunakan salah satu metode berikut:

- TheAWSSDK for Java akan secara otomatis mencoba menemukanAWSkredensi dengan menggunakan rantai penyedia kredensi default yang diimplementasikan oleh DefaultAWSCredentialsProviderChain kelas. Untuk informasi selengkapnya, lihat[Menggunakan Rantai Penyedia Kredensyal Default](#).
- Anda dapat menentukanAWSkunci[Properti konfigurasi Hadoop](#). Misalnya, jika tempdirkonfigurasi menunjuk ke as3n://sistem file, aturfs.s3n.awsAccessKeyIddanfs.s3n.awsSecretAccessKeyproperti dalam file konfigurasi XMLHadoop atau panggilansc.hadoopConfiguration.set()untuk mengubah konfigurasi Hadoop global Spark.

Misalnya, jika Anda menggunakan sistem file s3n, tambahkan:

```
sc.hadoopConfiguration.set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3n.awsSecretAccessKey", "YOUR_SECRET_ACCESS_KEY")
```

Untuk sistem file s3a, tambahkan:

```
sc.hadoopConfiguration.set("fs.s3a.access.key", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3a.secret.key", "YOUR_SECRET_ACCESS_KEY")
```

Jika Anda menggunakan Python, gunakan operasi berikut:

```
sc._jsc.hadoopConfiguration().set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc._jsc.hadoopConfiguration().set("fs.s3n.awsSecretAccessKey",
"YOUR_SECRET_ACCESS_KEY")
```

- Encode kunci otentikasi ditempdirURL. Misalnya, URIs3n://ACCESSKEY:SECRETKEY@bucket/path/to/temp/dirmengkodekan key pair (ACCESSKEY,SECRETKEY).

Otentikasi antara Redshift dan Amazon S3

Jika Anda menggunakan perintah COPY dan UNLOAD dalam kueri, Anda juga harus memberikan Amazon S3 akses ke Amazon Redshift untuk menjalankan kueri atas nama Anda. Untuk melakukannya, pertama [memberi wewenang kepada Amazon Redshift untuk mengakses lainnya AWS S3](#), kemudian mengotorisasi [Operasi COPY dan UNLOAD menggunakan peran IAM](#).

Sebagai praktik terbaik, kami merekomendasikan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).

Integrasi dengan AWS Secrets Manager

Anda dapat mengambil nama pengguna Redshift dan kredensial kata sandi Anda dari rahasia yang tersimpan di AWS Secrets Manager. Untuk secara otomatis menyediakan kredensi Redshift, gunakan `secret.id` parameter. Untuk informasi selengkapnya tentang cara membuat rahasia kredensial Redshift, lihat [Buat sebuah AWS Secrets Manager rahasia basis data](#).

GroupID	ArtefactID	Revisi yang Didukung	Deskripsi
com.amazonaws.secretsmanager	aws-secretsmanager-jdbc	1.0.12	The AWS Secrets Manager SQL Connection Library for Java memungkinkan Pengembang Java untuk dengan mudah terhubung ke database SQL menggunakan rahasia yang disimpan di AWS Secrets Manager.

Note

Pengakuan: Dokumentasi ini berisi kode contoh dan bahasa yang dikembangkan oleh [Yayasan Perangkat Lunak Apache](#) berlisensi di bawah [Lisensi Apache 2.0](#).

Peningkatan kinerja dengan pushdown

Konektor Spark secara otomatis menerapkan predikat dan pushdown kueri untuk mengoptimalkan kinerja. Dukungan ini berarti bahwa jika Anda menggunakan fungsi yang didukung dalam kueri Anda, konektor Spark akan mengubah fungsi menjadi kueri SQL dan menjalankan kueri di Amazon Redshift. Optimalisasi ini menghasilkan lebih sedikit data yang diambil, sehingga Apache Spark dapat memproses lebih sedikit data dan memiliki kinerja yang lebih baik. Secara default, pushdown diaktifkan secara otomatis. Untuk menonaktifkannya, atur `autopushdown` ke `false`.

```
import sqlContext.implicits._val
sample= sqlContext.read
  .format("io.github.spark_redshift_community.spark.redshift")
  .option("url",jdbcURL )
  .option("tempdir", tempS3Dir)
  .option("dbtable", "event")
  .option("autopushdown", "false")
  .load()
```

Fungsi-fungsi berikut didukung dengan pushdown. Jika Anda menggunakan fungsi yang tidak ada dalam daftar ini, konektor Spark akan menjalankan fungsi di Spark alih-alih Amazon Redshift, menghasilkan kinerja yang tidak dioptimalkan. Untuk daftar lengkap fungsi di Spark, lihat [Fungsi Bawaan](#).

- Fungsi agregasi
 - rata-rata
 - count
 - max
 - min
 - sum
 - stddev_samp
 - stddev_pop
 - var_samp
 - var_pop
- Operator Boolean
 - in
 - isnull

- isnotnull
- mengandung
- berakhir dengan
- mulaidengan
- Operator logistik
 - and
 - or
 - tidak (atau!)
- Fungsi matematika
 - +
 - -
 - *
 - /
 - - (unary)
 - perut
 - acos
 - asin
 - atan
 - ceil
 - cos
 - exp
 - lantai
 - terbesar
 - paling sedikit
 - log10
 - pi
 - pow
 - bulat
 - dosa
- sqrt

- tan
- Fungsi lain-lain
 - melemparkan
 - coalesce
 - decimal
 - jika
 - in
- Operator relasional
 - !=
 - =
 - >
 - >=
 - <
 - <=
- Fungsi string
 - ascii
 - lpad
 - rpad
 - menerjemahkan
 - atas
 - menurunkan
 - length
 - memangkas
 - ltrim
 - rtrim
 - suka
 - substring
 - concat
- Fungsi waktu dan tanggal
 - add_months

- tanggal
- date_add
- date_sub
- date_trunc
- timestamp
- batang
- Operasi matematika
 - CheckOverflow
 - PromotePrecision
- Operasi relasional
 - Alias (misalnya, AS)
 - CaseWhen
 - Berbeda
 - InSet
 - Bergabung dan bergabung silang
 - Batas
 - Serikat pekerja, serikat semua
 - ScalarSubquery
 - Sortir (naik dan turun)
 - UnscaledValue

Opsi konfigurasi lainnya

Ubah ukuran maksimum kolom string

Redshift membuat kolom string sebagai kolom teks saat membuat tabel, yang disimpan sebagai VARCHAR (256). Jika Anda menginginkan kolom yang mendukung ukuran yang lebih besar, Anda dapat menggunakan maxlength untuk menentukan panjang maksimum kolom string. Berikut ini adalah contoh cara menentukan maxlength.

```
columnLengthMap.foreach { case (colName, length) =>
  val metadata = new MetadataBuilder().putLong("maxlength", length).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
```



```
}

```

Mengatur jenis kolom

Untuk mengatur jenis kolom, gunakan `redshift_type` bidang.

```
columnTypeMap.foreach { case (colName, colType) =>
  val metadata = new MetadataBuilder().putString("redshift_type", colType).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

Mengatur pengkodean kompresi pada kolom

Untuk menggunakan pengkodean kompresi tertentu pada kolom, gunakan bidang pengkodean.

Untuk daftar lengkap penyandian kompresi dukungan, lihat [Pengkodean kompresi](#).

Mengatur deskripsi untuk kolom

Untuk mengatur deskripsi, gunakan `description` bidang.

Otentikasi antara Redshift dan Amazon S3

Secara default, hasilnya diturunkan ke Amazon S3 dalam format `parquet`. Untuk membongkar hasilnya sebagai file teks yang dibatasi pipa, tentukan opsi berikut.

```
.option("unload_s3_format", "TEXT")
```

Jalankan pernyataan pushdown dengan malas

Parameter	Diperlukan	Bawaan	Deskripsi
<code>spark.datasource.redshift.community.autoPushdown.lazyMode</code>	Tidak	Benar	Menentukan apakah konektor harus malas menjalankan pernyataan pushdown Redshift. Jika benar, konektor percikan mengambil semua model dan informasi terkait

Parameter	Diperlukan	Bawaan	Deskripsi
			<p>sebelum menjalankan kueri, yang umumnya menghasilkan kinerja yang lebih baik.</p> <p>Jika salah, konektor percikan menjalankan pernyataan pushdown segera di atas driver Spark utama dan diserialisasikan di seluruh ekspresi.</p>

Parameter konektor

Peta parameter atau `OPTIONS` di Spark SQL mendukung pengaturan berikut.

Parameter	Diperlukan	Bawaan	Deskripsi
<code>dbtable</code>	Ya, kecuali kueri ditentukan	T/A	Tabel untuk membuat atau membaca dari Redshift. Parameter ini diperlukan saat menyimpan data kembali ke Redshift.
<code>kueri</code>	Ya, kecuali <code>dbtable</code> ditentukan	T/A	Kueri untuk dibaca di Redshift.
<code>pengguna</code>	Tidak	T/A	Nama pengguna Redshift. Harus digunakan dengan parameter kata

Parameter	Diperlukan	Bawaan	Deskripsi
			sandi. Hanya berlaku jika pengguna dan kata sandi bukan parameter dalam URL. Menggunakan keduanya akan menyebabkan kesalahan.
kata sandi	Tidak	T/A	Kata sandi Redshift. Harus digunakan dengan parameter pengguna. Hanya berlaku jika pengguna dan kata sandi bukan parameter dalam URL. Menggunakan keduanya akan menyebabkan kesalahan.

Parameter	Diperlukan	Bawaan	Deskripsi
url	Tidak	T/A	<p>URL JDBC. Formatnya adalah <code>jdbc:subprotocol://host:port/database?user=username&password=password</code>.</p> <p>Subprotokol dapat berupa <code>postgres</code> atau <code>Redshift</code>, tergantung pada driver JDBC mana yang telah Anda muat. Perhatikan bahwa satu driver yang kompatibel dengan Redshift harus berada di classpath dan cocok dengan URL ini.</p> <p>Host dan port harus mengarah ke node master Redshift, jadi Anda harus mengonfigurasi grup keamanan dan/atau VPC untuk mengizinkan akses dari aplikasi driver Anda.</p> <p>Database adalah nama database Redshift.</p>

Parameter	Diperlukan	Bawaan	Deskripsi
			Pengguna dan kata sandi adalah kredensial untuk mengakses database, yang harus disematkan dalam URL ini untuk JDBC, dan pengguna database harus memiliki izin yang diperlukan untuk mengakses tabel.
aws_iam_role	Hanya jika menggunakan peran IAM untuk mengotorisasi operasi SALIN/BONGKAR Redshift	T/A	ARN yang ditentukan sepenuhnya dari IAM role yang dilampirkan ke cluster Redshift.

Parameter	Diperlukan	Bawaan	Deskripsi
<code>forward_spark_s3_credentials</code>	Tidak	Salah	Menunjukkan apakah pustaka ini akan secara otomatis menemukan kredensial yang digunakan Spark untuk terhubung ke Amazon S3, dan apakah akan meneruskan kredensialnya ke Redshift melalui driver JDBC. Kredensial ini dikirim sebagai bagian dari kueri JDBC. Oleh karena itu kami menyarankan Anda mengaktifkan enkripsi SSL dengan koneksi JDBC saat menggunakan opsi ini.
<code>temporary_aws_access_key_id</code>	Tidak	T/A	AWSkunci akses. Harus memiliki izin menulis ke bucket S3.
<code>temporary_aws_secret_access_key</code>	Tidak	T/A	AWSkunci akses rahasia yang sesuai dengan kunci akses.

Parameter	Diperlukan	Bawaan	Deskripsi
temporary_aws_session_token	Tidak	T/A	AWSToken sesi sesuai dengan kunci akses yang disediakan.
tempdir	Tidak	T/A	Lokasi yang dapat ditulis di Amazon S3. Digunakan untuk membongkar data saat membaca dan data Avro untuk dimuat ke Redshift saat menulis. Jika Anda menggunakan sumber data Redshift untuk Spark sebagai bagian dari pipeline ETL biasa, akan berguna untuk menyetel kebijakan siklus pada ember dan gunakan itu sebagai lokasi sementara untuk data ini.

Parameter	Diperlukan	Bawaan	Deskripsi
jdbcdriver	Tidak	Ditentukan oleh subprotokol URL JDBC	Nama kelas driver JDBC untuk digunakan. Kelas ini harus berada di classpath. Dalam kebanyakan kasus, tidak perlu menentukan opsi ini, karena nama kelas driver yang sesuai harus secara otomatis ditentukan oleh subprotokol URL JDBC.
diststyle	Tidak	Bahkan	Pergeseran Merah Gaya Distribusi untuk digunakan saat membuat tabel. Opsi yang valid adalah EVEN, KEY atau ALL. Saat menggunakan KEY, Anda juga harus mengatur kunci distribusi dengan opsi distkey.
distkey	Tidak, kecuali menggunakan DISTYLE_KEY	T/A	Nama kolom dalam tabel untuk digunakan sebagai kunci distribusi saat membuat tabel.

Parameter	Diperlukan	Bawaan	Deskripsi
sortkeyspec	Tidak	T/A	Redshift penuh Sortir definisi.
include_column_list	Tidak	Salah	Menunjukkan apakah pustaka ini harus secara otomatis mengekstrak kolom dari skema dan menambahkannya ke perintah COPY sesuai dengan Opsi pemetaan kolom .
deskripsi	Tidak	T/A	Deskripsi tabel. Deskripsi diatur dengan perintah SQL COMMENT, dan muncul di sebagian besar alat kueri. Lihat <code>descripti on</code> metadata untuk mengatur deskripsi pada kolom individual.

Parameter	Diperlukan	Bawaan	Deskripsi
preaksi	Tidak	T/A	Sebuah daftar perintah SQL yang dibatasi titik koma untuk dijalankan sebelum memuat perintah COPY. Mungkin berguna untuk menjalankan perintah DELETE atau serupa sebelum memuat data baru. Jika perintah berisi %s, nama tabel akan diformat sebelum runtime (jika Anda menggunakan tabel pementasan). Jika perintah ini gagal, itu diperlakukan sebagai pengecualian. Jika Anda menggunakan tabel pementasan, perubahan akan dikembalikan dan mengembalikan tabel cadangan jika preaksi gagal.

Parameter	Diperlukan	Bawaan	Deskripsi
ekstrakoopiopsi	Tidak	T/A	<p>Daftar opsi tambahan untuk ditambahkan ke perintah Redshift COPY saat memuat data (seperti TRUNCATE COLUMN atau MAXERROR). Lihat Parameter opsional untuk daftar lengkap parameter yang tersedia.</p> <p>Perhatikan bahwa karena opsi ini ditambahkan ke akhir COPY perintah, Anda hanya dapat menggunakan opsi yang masuk akal di akhir perintah. Itu harus mencakup sebagian besar kasus penggunaan yang mungkin.</p>

Parameter	Diperlukan	Bawaan	Deskripsi
sse_kms_key	Tidak	T/A	TheAWS KMSkunci ID yang digunakan untuk enkripsi sisi server di S3 selama operasi Redshift UNLOAD daripadaAWSenkripsi. IAM role Redshift harus memiliki akses ke kunci KMS untuk menulis dengannya, dan IAM role Spark harus memiliki akses ke kunci untuk operasi baca. Membaca data terenkripsi tidak memerlukan perubahan (AWSmenangani ini) selama peran IAM Spark memiliki akses yang tepat.
tempformat	Tidak	AVRO	Format untuk menyimpan file sementara di Amazon S3 saat menulis ke Redshift. Nilai yang valid adalah AVRO, CSV, dan CSV GZIP (CSV terkompresi).

Parameter	Diperlukan	Bawaan	Deskripsi
csvnullstring (eksperimental)	Tidak	No	Nilai string untuk menulis untuk nol saat menggunakan tempformat CSV. Ini harus menjadi nilai yang tidak muncul dalam data aktual Anda.
autopushdown	Tidak	Benar	Menunjukkan apakah akan menerapkan predikat dan pushdown kueri dengan menangkap dan menganalisis rencana logis Spark untuk operasi SQL. Operasi diterjemahkan ke dalam kueri SQL dan kemudian dijalankan di Redshift untuk meningkatkan kinerja.

Parameter	Diperlukan	Bawaan	Deskripsi
autopushdown.s3_result_cache	Tidak	Salah	Cache SQL kueri untuk membongkar data pemetaan jalur Amazon S3 di memori, sehingga kueri yang sama tidak perlu dijalankan lagi dalam sesi Spark yang sama. Hanya didukung saat autopushdown dihidupkan. Kami tidak menyarankan menggunakan parameter ini saat mencampur operasi baca dan tulis karena hasil cache mungkin berisi informasi basi.
unload_s3_format	Tidak	Parquet:	Format yang digunakan untuk membongkar hasil kueri. Opsi yang valid adalah Parquet dan Teks, yang menentukan untuk membongkar hasil kueri dalam format teks yang dibatasi pipa.

Parameter	Diperlukan	Bawaan	Deskripsi
extraunloadoptions	Tidak	T/A	Opsi tambahan untuk ditambahkan ke Redshift MEMBONGKAR perintah. Tidak semua opsi dijamin berfungsi karena beberapa opsi mungkin bertentangan dengan opsi lain yang ditetapkan dalam konektor.
copydelay	Tidak	30000	Penundaan (dalam ms) antara percobaan ulang untuk operasi Redshift COPY.
copyretrycount	Tidak	2	Berapa kali untuk mencoba lagi operasi Redshift COPY.

Parameter	Diperlukan	Bawaan	Deskripsi
tempdir_region	Tidak	T/A	<p>TheAWSwilayah di manatempdirterletak. Menyetel opsi ini meningkatkan kinerja konektor untuk interaksi dengantempdirserta secara otomatis memberikan nilai ini sebagai bagian dari operasi COPY dan UNLOAD selama operasi baca dan tulis konektor.</p> <p>Pengaturan ini direkomendasikan dalam situasi berikut:</p> <ol style="list-style-type: none"> 1) Saat konektor berjalan di luarAWS, karena penemuan Wilayah otomatis akan gagal dan berdampak negatif pada kinerja konektor. 2) Kapantempdirberada di Wilayah yang berbeda dari cluster Redshift, karena menggunakan an pengaturan

Parameter	Diperlukan	Bawaan	Deskripsi
			<p>ini mengurangi kebutuhan untuk memasok Wilayah secara manual menggunakan <code>anextracopy options danextraunlo adoptions</code> parameter <code>.tempdir</code> tidak bisa berada di Wilayah yang berbeda dari cluster Redshift saat menggunakan <code>anPARQUET</code> sebagai <code>tempformat</code> bahkan jika ini menggunakan parameter ini.</p> <p>3) Ketika konektor berjalan di Wilayah yang berbeda dari <code>tempdir</code>, karena meningkatkan kinerja akses konektor <code>tempdir</code>.</p>

Parameter	Diperlukan	Bawaan	Deskripsi
rahasia.id	Tidak	T/A	Nama atau ARN rahasia Anda disimpan diAWS Secrets Manager. Anda dapat menggunakan parameter ini untuk secara otomatis menyediakan kredensi Redshift, tetapi hanya jika pengguna, kata sandi, danDbUserkredensya tidak diteruskan ke URL JDBC atau sebagai opsi lain.

Parameter	Diperlukan	Bawaan	Deskripsi
secret.region	Tidak	T/A	<p>PrimerAWSwilayah, seperti US East (N. Virginia), untuk mencari <code>secret.id</code> nilai.</p> <p>Jika Anda tidak menentukan wilayah ini, konektor akan mencoba untuk menggunakan Rantai penyedia kredensya I default untuk menyelesaikan Wilayah <code>secret.id</code>. Dalam beberapa kasus, seperti jika Anda menggunakan konektor di luar konektor tidak akan dapat menemukan Wilayah. Sebaiknya gunakan pengaturan ini dalam situasi berikut:</p> <ol style="list-style-type: none">1) Saat konektor berjalan di luarAWS, karena penemuan Wilayah otomatis akan gagal dan mencegah otentikasi dengan Redshift

Parameter	Diperlukan	Bawaan	Deskripsi
			Ketika konektor berjalan di Wilayah yang berbeda dari <code>secret.id</code> , karena meningkatkan kinerja akses konektor rahasia.
<code>rahasia.vpcEndpointUrl</code>	Tidak	T/A	The PrivateLink URL endpoint DNSAWS Secrets Managers atau mengesampingkan Rantai penyedia kredensial default .
<code>rahasia.vpcEndpointRegion</code>	Tidak	T/A	The PrivateLink Wilayah endpoint DNS untuk AWS Secrets Managers atau mengesampingkan Rantai penyedia kredensial default .

Parameter	Diperlukan	Bawaan	Deskripsi
jdbc. *	Tidak	T/A	Parameter tambahan untuk diteruskan ke driver JDBC yang mendasarinya di mana wildcard adalah nama parameter JDBC, seperti jdbc.ssl. Perhatikan bahwa jdbcawalan akan dihapus sebelum diteruskan ke driver JDBC. Untuk melihat semua opsi yang mungkin untuk driver Redshift JDBC, lihat Opsi untuk konfigurasi driver JDBC versi 2.1.

Parameter	Diperlukan	Bawaan	Deskripsi
label	Tidak	" "	<p>Pengidentifikasi untuk disertakan dalam kumpulan kueri yang disetel saat menjalankan kueri dengan konektor. Harus 100 karakter atau kurang, dan semua karakter harus valid unicode IdentifierParts .</p> <p>Jika pengenalan Anda memiliki lebih dari 100 karakter, kelebihannya akan dihapus. Saat menjalankan kueri dengan konektor, grup kueri akan ditetapkan sebagai string format JSON, seperti</p> <pre> {"spark-redshift-connector": {"svc": "5.1.0-amzn-1-spark_3.3", "op": "Read", "tbl": ""}} </pre> <p>. Opsi ini menggantikan nilai <code>tbl</code> kunci.</p>

Note

Pengakuan: Dokumentasi ini berisi kode contoh dan bahasa yang dikembangkan oleh [Yayasan Perangkat Lunak Apache](#) berlisensi di bawah [Lisensi Apache 2.0](#).

Tipe data yang didukung

Tipe data berikut di Amazon Redshift didukung dengan konektor Spark. Untuk mengetahui daftar lengkap tipe data yang didukung di Amazon Redshift, lihat [Tipe data](#). Jika tipe data tidak ada dalam tabel di bawah ini, itu tidak didukung di konektor Spark.

Tipe data	Alias
SMALLINT	INT2
BILANGAN BULAT	INT, INT4
BIGINT	INT8
DESIMAL	NUMERIK
NYATA	FLOAT4
DOUBLE PRECISION	MENGAPUNG8, MENGAPUNG
BOOLEAN	BOOL
CHAR	KARAKTER, NCHAR, BPCHAR
VARCHAR	KARAKTER BERVARIASI, NVARCHAR, TEKS
TANGGAL	
TIMESTAMP	Stempel waktu tanpa zona waktu
TIMESTAMPTZ	Stempel waktu dengan zona waktu
SUPER	

Tipe data	Alias
WAKTU	Waktu tanpa zona waktu
JADWAL	Waktu dengan zona waktu
VARBYTE	VARBINARY, BINER

Tipe data yang kompleks

Anda dapat menggunakan konektor percikan untuk membaca dan menulis tipe data kompleks Spark seperti `ArrayType`, `MapType`, dan `StructType` ke dan dari kolom tipe data Redshift SUPER. Jika Anda memberikan skema selama operasi baca, data di kolom akan dikonversi ke tipe kompleks yang sesuai di Spark, termasuk semua jenis bersarang. Selain itu, jika `autopushdown` diaktifkan, proyeksi atribut bersarang, nilai peta, dan indeks array didorong ke Redshift sehingga seluruh struktur data bersarang tidak perlu lagi dibongkar saat mengakses hanya sebagian data.

Saat Anda menulis `DataFrames` dari konektor, kolom jenis apa pun `MapType` (menggunakan `StringType`), `StructType`, atau `ArrayType` ditulis ke kolom tipe data Redshift SUPER. Saat menulis struktur data bersarang ini, `tempFormatParameter` harus dari tipe `CSV`, `CSV_GZIP`, atau `PARQUET`. Menggunakan `AVRO` akan menyebabkan pengecualian. Menulis `MapType` struktur data yang memiliki tipe kunci selain `StringType` juga akan menyebabkan pengecualian.

StructType

Contoh berikut menunjukkan cara membuat tabel dengan tipe data SUPER yang berisi struct

```
create table contains_super (a super);
```

Anda kemudian dapat menggunakan konektor untuk menanyakan `StringType` bidang `hello` dari kolom SUPER dalam tabel menggunakan skema seperti pada contoh berikut.

```
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")
```

Contoh berikut menunjukkan bagaimana untuk menulis sebuah struct ke koloma.

```
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

Jika Anda lebih suka menggunakan `MapType` untuk mewakili data Anda, maka Anda dapat menggunakan `MapType` struktur data dalam skema Anda dan mengambil nilai yang sesuai dengan kunci di peta. Perhatikan bahwa semua kunci di `MapType` struktur data harus bertipe `String`, dan semua nilai harus dari jenis yang sama, seperti `int`.

Contoh berikut menunjukkan bagaimana untuk mendapatkan nilai kunci `hello` di koloma.

```
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

Jika kolom berisi array bukan struct, Anda dapat menggunakan konektor untuk query elemen pertama dalam array.

```

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]")

```

Keterbatasan:

Menggunakan tipe data yang kompleks dengan konektor percikan memiliki batasan berikut:

- Semua nama bidang struct bersarang dan kunci peta harus huruf kecil. Jika menanyakan nama bidang kompleks dengan huruf besar, Anda dapat mencoba menghilangkan skema dan menggunakan `from_json` fungsi spark untuk mengonversi string yang dikembalikan secara lokal sebagai solusi.
- Setiap bidang peta yang digunakan dalam operasi baca atau tulis harus hanya memiliki `StringType` kunci.

- Hanya CSV, CSV GZIP, dan PARQUET didukung nilai tempformat untuk menulis tipe kompleks ke Redshift. Mencoba untuk menggunakan AVRO akan melempar pengecualian.

Mengonfigurasi koneksi untuk driver ODBC versi 2.x untuk Amazon Redshift

Anda dapat menggunakan koneksi ODBC untuk terhubung ke kluster Amazon Redshift Anda dari banyak alat dan aplikasi klien SQL pihak ketiga. Jika alat klien Anda mendukung JDBC, Anda dapat memilih untuk menggunakan jenis koneksi itu daripada ODBC karena kemudahan konfigurasi yang disediakan JDBC. Namun, jika alat klien Anda tidak mendukung JDBC, Anda dapat mengikuti langkah-langkah di bagian ini untuk mengatur koneksi ODBC di komputer klien atau instans Amazon EC2.

Amazon Redshift menyediakan driver ODBC 64-bit untuk sistem operasi Linux dan Windows; driver ODBC 32-bit dihentikan. Saat ini, macOS X tidak didukung. Pembaruan lebih lanjut untuk driver ODBC 32-bit tidak akan dirilis, kecuali untuk patch keamanan yang mendesak. Untuk mengunduh dan instal driver ODBC untuk macOS X dan sistem operasi 32-bit, [lihat Mengonfigurasi koneksi ODBC](#).

Untuk informasi terbaru tentang perubahan driver ODBC, lihat [log perubahan](#).

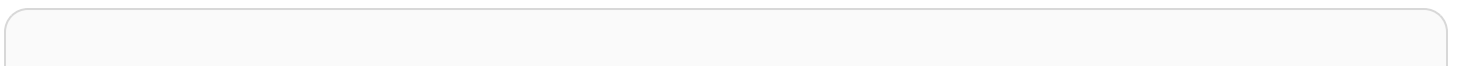
Topik

- [Mendapatkan URL ODBC](#)
- [Menginstal dan mengonfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#)
- [Menginstal dan mengonfigurasi driver Amazon Redshift ODBC di Linux](#)
- [Mengkonfigurasi otentikasi](#)
- [Mengonversi tipe data](#)
- [Mengkonfigurasi opsi driver ODBC](#)
- [Versi driver ODBC sebelumnya](#)

Mendapatkan URL ODBC

Amazon Redshift menampilkan URL ODBC untuk kluster Anda di konsol Amazon Redshift. URL ini berisi informasi yang diperlukan untuk mengatur koneksi antara komputer klien Anda dan database.

URL ODBC memiliki format berikut:



```
Driver={driver}; Server=endpoint_host; Database=database_name; UID=user_name;
PWD=password; Port=port_number
```

Bidang format sebelumnya memiliki nilai-nilai berikut:

Nilai bidang URL ODBC

Bidang	Nilai
<i>Driver</i>	Nama driver ODBC 64-bit yang akan digunakan: Amazon Redshift ODBC Driver (x64)
<i>Server</i>	Host endpoint dari cluster Amazon Redshift.
<i>Database</i>	Database yang Anda buat untuk cluster Anda.
<i>UID</i>	Nama pengguna dari akun pengguna database yang memiliki izin untuk terhubung ke database. Meskipun nilai ini adalah izin tingkat database dan bukan izin tingkat cluster, Anda dapat menggunakan akun pengguna admin Redshift yang Anda atur saat meluncurkan cluster.
<i>PWD</i>	Kata sandi untuk akun pengguna database untuk terhubung ke database.
<i>Port</i>	Nomor port yang Anda tentukan saat Anda meluncurkan cluster. Jika Anda memiliki firewall, pastikan port ini terbuka untuk Anda gunakan.

Berikut ini adalah contoh URL ODBC:

```
Driver={Amazon Redshift ODBC Driver (x64)}; Server=examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com; Database=dev; UID=adminuser;
PWD=insert_your_admin_user_password_here; Port=5439
```

Untuk informasi tentang tempat menemukan URL ODBC, lihat [Menemukan string koneksi cluster Anda](#).

Menginstal dan mengonfigurasi driver Amazon Redshift ODBC di Microsoft Windows

Persyaratan Sistem

Anda harus menginstal driver Amazon Redshift ODBC di komputer klien yang mengakses gudang data Amazon Redshift. Untuk setiap komputer tempat Anda menginstal driver, ada persyaratan minimum berikut:

- Hak administrator pada mesin.
- Mesin memenuhi persyaratan sistem berikut:
 - Salah satu sistem operasi berikut:
 - Windows 10 atau 8.1.
 - Windows Server 2019, 2016, atau 2012.
 - 100 MB ruang disk yang tersedia.
 - Visual C ++ Redistributable untuk Visual Studio 2015 untuk Windows 64-bit diinstal. Anda dapat mengunduh paket instalasi di [Download Visual C++ Redistributable for Visual Studio 2022](#) di situs web Microsoft.

Menginstal driver Amazon Redshift ODBC

Gunakan prosedur berikut untuk mengunduh dan menginstal driver Amazon Redshift ODBC untuk sistem operasi Windows. Hanya gunakan driver yang berbeda jika Anda menjalankan aplikasi pihak ketiga yang disertifikasi untuk digunakan dengan Amazon Redshift, dan aplikasi itu memerlukan driver khusus itu.

Untuk mengunduh dan menginstal driver ODBC:

1. Unduh driver berikut: [64-bit ODBC driver versi 2.1.2.0](#) driver versi 2.1.2.0

Nama driver ini adalah Amazon Redshift ODBC Driver (x64).

Note

Driver ODBC 32-bit dihentikan. Pembaruan lebih lanjut tidak akan dirilis, kecuali untuk patch keamanan yang mendesak. Untuk mengunduh dan menginstal driver ODBC untuk sistem operasi 32-bit, lihat [Menginstal dan mengkonfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#).

2. Tinjau lisensi [driver Amazon Redshift ODBC versi 2.x](#).
3. Klik dua kali file.msi, lalu ikuti langkah-langkah di wizard untuk menginstal driver.

Membuat entri DSN sistem untuk koneksi ODBC

Setelah Anda mengunduh dan menginstal driver ODBC, tambahkan entri nama sumber data (DSN) ke komputer klien atau instans Amazon EC2. Alat klien SQL dapat menggunakan sumber data ini untuk terhubung ke database Amazon Redshift.

Kami menyarankan Anda membuat sistem DSN bukan DSN pengguna. Beberapa aplikasi memuat data menggunakan akun pengguna database yang berbeda, dan mungkin tidak dapat mendeteksi DSN pengguna yang dibuat di bawah akun pengguna database lain.

Note

Untuk autentikasi menggunakan kredensial AWS Identity and Access Management (IAM) atau kredensial penyedia identitas (iDP), diperlukan langkah-langkah tambahan. Untuk informasi selengkapnya, lihat [Mengkonfigurasi koneksi JDBC atau ODBC untuk menggunakan kredensial IAM](#).

Untuk membuat entri DSN sistem untuk koneksi ODBC:

1. Di menu Mulai, ketik “Sumber Data ODBC.” Pilih Sumber Data ODBC.

Pastikan Anda memilih Administrator Sumber Data ODBC yang memiliki bitness yang sama dengan aplikasi klien yang Anda gunakan untuk terhubung ke Amazon Redshift.
2. Di Administrator Sumber Data ODBC, pilih tab Driver dan cari folder driver berikut: Amazon Redshift ODBC Driver (x64).
3. Pilih tab Sistem DSN untuk mengonfigurasi driver untuk semua pengguna di komputer, atau tab DSN Pengguna untuk mengonfigurasi driver hanya untuk akun pengguna database Anda.
4. Pilih Tambahkan. Jendela Create New Data Source terbuka.
5. Pilih driver Amazon Redshift ODBC (x64), lalu pilih Selesai. Jendela Pengaturan DSN Driver Amazon Redshift ODBC terbuka.
6. Di bawah bagian Pengaturan Koneksi, masukkan informasi berikut:
 - Nama sumber data

Masukkan sebuah nama untuk sumber data. Misalnya, jika Anda mengikuti Panduan Memulai Amazon Redshift, Anda dapat mengetik `exampleclusterdsn` agar mudah mengingat cluster yang Anda kaitkan dengan DSN ini.

- Server

Tentukan host endpoint untuk cluster Amazon Redshift Anda. Anda dapat menemukan informasi ini di konsol Amazon Redshift di halaman detail cluster. Untuk informasi selengkapnya, lihat [Mengonfigurasi koneksi di Amazon Redshift](#).

- Port

Masukkan nomor port yang digunakan database. Bergantung pada port yang Anda pilih saat membuat, memodifikasi, atau memigrasi klaster, izinkan akses ke port yang dipilih.

- Basis Data

Masukkan nama database Amazon Redshift. Jika Anda meluncurkan cluster Anda tanpa menentukan nama database, masukkan `dev`. Jika tidak, gunakan nama yang Anda pilih selama proses peluncuran. Jika Anda mengikuti Panduan Memulai Amazon Redshift, masukkan `dev`.

7. Di bawah bagian Otentikasi, tentukan opsi konfigurasi untuk mengonfigurasi otentikasi standar atau IAM.

8. Pilih Opsi SSL dan tentukan nilai untuk yang berikut ini:

- Mode autentikasi

Pilih mode untuk menangani Secure Sockets Layer (SSL). Dalam lingkungan pengujian, Anda mungkin menggunakan `prefer`. Namun, untuk lingkungan produksi dan ketika pertukaran data yang aman diperlukan, gunakan `verify-ca` atau `verify-full`.

- Min TLS

Secara opsional, pilih versi minimum TLS/SSL yang driver memungkinkan penyimpanan data untuk digunakan untuk mengenkripsi koneksi. Misalnya, jika Anda menentukan TLS 1.2, TLS 1.1 tidak dapat digunakan untuk mengenkripsi koneksi. Versi defaultnya adalah TLS 1.2.

9. Di tab Proxy, tentukan pengaturan koneksi proxy apa pun.

10 Di tab Cursor, tentukan opsi tentang cara mengembalikan hasil kueri ke alat atau aplikasi klien SQL Anda.

11 Di Opsi Lanjutan, tentukan nilai untuk `logLevel`, `logPath`, `compression`, dan opsi lainnya.

12. Pilih Uji. Jika komputer klien dapat terhubung ke database Amazon Redshift, pesan berikut akan muncul: Koneksi berhasil. Jika komputer klien gagal terhubung ke database, Anda dapat memecahkan masalah yang mungkin terjadi dengan membuat file log dan menghubungi AWS dukungan. Untuk informasi tentang membuat log, lihat (LINK).

13. Pilih OK.

Menginstal dan mengonfigurasi driver Amazon Redshift ODBC di Linux

Persyaratan Sistem

Anda harus menginstal driver Amazon Redshift ODBC di komputer klien yang mengakses gudang data Amazon Redshift. Untuk setiap komputer tempat Anda menginstal driver, ada persyaratan minimum berikut:

- Akses root pada mesin.
- Salah satu distribusi berikut:
 - Red Hat® Enterprise Linux® (RHEL) 8 atau lebih baru
 - CentOS 8 atau lebih baru.
- 150 MB ruang disk yang tersedia.
- UnixODBC 2.2.14 atau yang lebih baru.
- glibc 2.26 atau yang lebih baru.

Menginstal driver Amazon Redshift ODBC

Untuk mengunduh dan menginstal driver Amazon Redshift ODBC versi 2.x untuk Linux:

1. Unduh driver berikut: [64-bit RPM driver versi 2.1.2.0](#) driver versi 2.1.2.0

Note

Driver ODBC 32-bit dihentikan. Pembaruan lebih lanjut tidak akan dirilis, kecuali untuk patch keamanan yang mendesak.

2. Pergi ke lokasi di mana Anda mengunduh paket, dan kemudian jalankan salah satu perintah berikut. Gunakan perintah yang sesuai dengan distribusi Linux Anda.

Pada sistem operasi RHEL dan CentOS, jalankan perintah berikut:


```
yum --nogpgcheck localinstall RPMFileName
```

Ganti *RPMFileName* dengan nama file paket RPM. Misalnya, perintah berikut menunjukkan menginstal driver 64-bit:

```
yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-2.x.xx.xxxx.x86_64.rpm
```

Menggunakan manajer driver ODBC untuk mengkonfigurasi driver ODBC di Linux

Di Linux, Anda menggunakan manajer driver ODBC untuk mengonfigurasi pengaturan koneksi ODBC. Manajer driver ODBC menggunakan file konfigurasi untuk menentukan dan mengkonfigurasi sumber data dan driver ODBC. Manajer driver ODBC yang Anda gunakan bergantung pada sistem operasi yang Anda gunakan.

Mengkonfigurasi driver ODBC menggunakan pengelola driver UnixODBC

File-file berikut diperlukan untuk mengonfigurasi driver Amazon Redshift ODBC:

- `amazon.redshiftdbc.ini`
- `odbc.ini`
- `odbcinst.ini`

Jika Anda menginstal ke lokasi default, file `amazon.redshiftdbc.ini` konfigurasi terletak di `opt/amazon/redshiftdbcx64`.

Selain itu, di bawah `opt/amazon/redshiftdbcx64`, Anda dapat menemukan sampel `odbc.ini` dan `odbcinst.ini` file. Anda dapat menggunakan file-file ini sebagai contoh untuk mengonfigurasi driver Amazon Redshift ODBC dan nama sumber data (DSN).

Kami tidak menyarankan menggunakan direktori instalasi driver Amazon Redshift ODBC untuk file konfigurasi. File sampel dalam direktori yang diinstal hanya untuk tujuan contoh. Jika Anda menginstal ulang driver Amazon Redshift ODBC di lain waktu, atau meningkatkan ke versi yang lebih baru, direktori instalasi akan ditimpa. Anda akan kehilangan perubahan apa pun yang mungkin telah Anda buat pada file di direktori instalasi.

Untuk menghindari hal ini, salin `amazon.redshiftodbc.ini` file ke direktori selain direktori instalasi. Jika Anda menyalin file ini ke direktori home pengguna, tambahkan titik (.) ke awal nama file untuk menjadikannya file tersembunyi.

Untuk `odbcinst.ini` file `odbc.ini` dan, gunakan file konfigurasi di direktori home pengguna atau buat versi baru di direktori lain. Secara default, sistem operasi Linux Anda harus memiliki `odbc.ini` file dan `odbcinst.ini` file di direktori home pengguna (`/home/$USER` atau `~/.`). File default ini adalah file tersembunyi, yang ditunjukkan oleh titik (.) di depan setiap nama file. File-file ini hanya ditampilkan ketika Anda menggunakan `-a` bendera untuk daftar isi direktori.

Opsi apa pun yang Anda pilih untuk `odbcinst.ini` file `odbc.ini` dan, ubah file untuk menambahkan informasi konfigurasi driver dan DSN. Jika Anda membuat file baru, Anda juga perlu mengatur variabel lingkungan untuk menentukan di mana file konfigurasi ini berada.

Secara default, manajer driver ODBC dikonfigurasi untuk menggunakan versi tersembunyi dari file `odbc.ini` dan `odbcinst.ini` konfigurasi (bernama `.odbc.ini` dan `.odbcinst.ini`) yang terletak di direktori home. Mereka juga dikonfigurasi untuk menggunakan `amazon.redshiftodbc.ini` file di direktori instalasi driver. Jika Anda menyimpan file konfigurasi ini di tempat lain, atur variabel lingkungan yang dijelaskan berikut sehingga manajer driver dapat menemukan file.

Jika Anda menggunakan UnixODBC, lakukan hal berikut:

- Atur `ODBCINI` ke path lengkap dan nama file `odbc.ini` file.
- Setel `ODBCSYSINI` ke path lengkap direktori yang berisi `odbcinst.ini` file.
- Atur `AMAZONREDSHIFTODBCINI` ke path lengkap dan nama file `amazon.redshiftodbc.ini` file.

Berikut ini adalah contoh pengaturan nilai-nilai di atas:

```
export ODBCINI=/usr/local/odbc/odbc.ini
export ODBCSYSINI=/usr/local/odbc
export AMAZONREDSHIFTODBCINI=/etc/amazon.redshiftodbc.ini
```

Mengkonfigurasi koneksi menggunakan nama sumber data (DSN) di Linux

Saat menghubungkan ke penyimpanan data Anda menggunakan nama sumber data (DSN), konfigurasi `odbc.ini` file untuk menentukan nama sumber data (DSN). Tetapkan properti dalam

odbc.ini file untuk membuat DSN yang menentukan informasi koneksi untuk penyimpanan data Anda.

Pada sistem operasi Linux, gunakan format berikut:

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file
Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

Contoh berikut menunjukkan konfigurasi untuk odbc.ini dengan driver ODBC 64-bit pada sistem operasi Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift ODBC Driver (x64)

[Amazon_Redshift_x64]
Driver=/opt/amazon/redshiftdbcx64/librsodbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932Database=dev
locale=en-US
```

Mengkonfigurasi koneksi tanpa DSN di Linux

Untuk terhubung ke penyimpanan data Anda melalui koneksi yang tidak memiliki DSN, tentukan driver dalam odbcinst.ini file. Kemudian berikan string koneksi tanpa DSN di aplikasi Anda.

Pada sistem operasi Linux, gunakan format berikut:

```
[ODBC Drivers]
driver_name=Installed
...
```

```
[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

Contoh berikut menunjukkan konfigurasi untuk `odbcinst.ini` dengan driver ODBC 64-bit pada sistem operasi Linux.

```
[ODBC Drivers]
Amazon Redshift ODBC Driver (x64)=Installed

[Amazon Redshift ODBC Driver (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.so
```



Mengkonfigurasi otentikasi



Untuk melindungi data dari akses yang tidak sah, penyimpanan data Amazon Redshift memerlukan semua koneksi untuk diautentikasi menggunakan kredensial pengguna.


Tabel berikut mengilustrasikan opsi koneksi yang diperlukan dan opsional untuk setiap metode otentikasi yang dapat digunakan untuk menyambung ke driver Amazon Redshift ODBC versi 2.x:


Metode otentikasi ODBC diperlukan dan opsi koneksi opsional

Metode Otentikasi	Diperlukan	Opsional
Standar	<ul style="list-style-type: none"> Host Port Basis Data UID Kata sandi 	
Profil IAM	<ul style="list-style-type: none"> Host Port 	<ul style="list-style-type: none"> ClusterID Wilayah


Metode Otentikasi	Diperlukan	Opsional
	<ul style="list-style-type: none"> • Basis Data • IAM • Profil 	<ul style="list-style-type: none"> • AutoCreate • EndpointURL • StsEndpointURL • InstanceProfile <div data-bbox="1068 491 1507 806" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>ClusterID dan Region harus disetel di Host jika tidak disetel secara terpisah.</p> </div>
Kredensi IAM	<ul style="list-style-type: none"> • Host • Port • Basis Data • IAM • AccessKeyID • SecretAccessKunci 	<ul style="list-style-type: none"> • ClusterID • Wilayah • AutoCreate • EndpointURL • StsEndpointURL • SessionToken • UID <div data-bbox="1068 1297 1507 1612" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>ClusterID dan Region harus disetel di Host jika tidak disetel secara terpisah.</p> </div>

Metode Otentikasi	Diperlukan	Opsional
IKLAN FS	<ul style="list-style-type: none"> • Host • Port • Basis Data • IAM • plugin_name • UID • Kata sandi • IDP_host • IDP_port 	<ul style="list-style-type: none"> • ClusterID • Wilayah • AutoCreate • EndpointUrl • StsEndpointUrl • Diutamakan_Peran • login ToRp • SSL_tidak aman <div data-bbox="1068 737 1507 1052" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>ClusterID dan Region harus disetel di Host jika tidak disetel secara terpisah.</p> </div>
Azure AD	<ul style="list-style-type: none"> • Host • Port • Basis Data • IAM • plugin_name • UID • Kata sandi • IDP_penyewa • Client_ID • Klien_Rahasia 	<ul style="list-style-type: none"> • ClusterID • Wilayah • AutoCreate • EndpointUrl • StsEndpointUrl • Diutamakan_Peran • dbgroups_filter <div data-bbox="1068 1541 1507 1856" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>ClusterID dan Region harus disetel di Host jika tidak disetel secara terpisah.</p> </div>


Metode Otentikasi	Diperlukan	Opsional
JWT	<ul style="list-style-type: none"> • Host • Port • Basis Data • IAM • plugin_name • web_identity_token 	<ul style="list-style-type: none"> • provider_name
Okta	<ul style="list-style-type: none"> • Host • Port • Basis Data • IAM • plugin_name • UID • Kata sandi • IDP_host • App_Nama • App_ID 	<ul style="list-style-type: none"> • ClusterID • Wilayah • AutoCreate • EndpointUrl • StsEndpointUrl • Diutamakan_Peran <div data-bbox="1068 989 1508 1304" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>ClusterID dan Region harus disetel di Host jika tidak disetel secara terpisah.</p> </div>


Metode Otentikasi	Diperlukan	Opsional
Federasi Ping	<ul style="list-style-type: none">• Host• Port• Basis Data• IAM• plugin_name• UID• Kata sandi• IDP_host• IDP_port	<ul style="list-style-type: none">• ClusterID• Wilayah• AutoCreate• EndpointUrl• StsEndpointUrl• Diutamakan_Peran• SSL_tidak aman• partner_spid <div data-bbox="1068 737 1507 1052"><p> Note</p><p>ClusterID dan Region harus disetel di Host jika tidak disetel secara terpisah.</p></div>

Metode Otentikasi	Diperlukan	Opsional
Browser Azure AD	<ul style="list-style-type: none">• Host• Port• Basis Data• IAM• plugin_name• IDP_penyewa• Client_ID• UID	<ul style="list-style-type: none">• ClusterID• Wilayah• AutoCreate• EndpointUrl• StsEndpointUrl• Diutamakan_Peran• dbgroups_filter• IDP_Response_Timeout• listen_port

 **Note**

ClusterID dan Region harus disetel di Host jika tidak disetel secara terpisah.

Metode Otentikasi	Diperlukan	Opsional
Browser SAMP	<ul style="list-style-type: none"> • Host • Port • Basis Data • IAM • plugin_name • login_url • UID 	<ul style="list-style-type: none"> • ClusterID • Wilayah • AutoCreate • EndpointUrl • StsEndpointUrl • Diutamakan_Peran • dbgroups_filter • IDP_Response_Timeout • listen_port <div data-bbox="1068 793 1507 1108" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>ClusterID dan Region harus disetel di Host jika tidak disetel secara terpisah.</p> </div>
Profil Auth	<ul style="list-style-type: none"> • Host • Port • Basis Data • AccessKeyID • SecretAccessKunci 	

Metode Otentikasi	Diperlukan	Opsional
Browser Azure AD OAUTH2	<ul style="list-style-type: none"> • Host • Port • Basis Data • IAM • plugin_name • IDP_penyewa • Client_ID • UID 	<ul style="list-style-type: none"> • ClusterID • Wilayah • EndpointUrl • IDP_Response_Timeout • listen_port • cakupan • provider_name <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>ClusterID dan Region harus disetel di Host jika tidak disetel secara terpisah.</p> </div>

Menggunakan layanan kredensial eksternal

Selain dukungan bawaan untuk AD FS, Azure AD, dan Okta, versi Windows dari driver Amazon Redshift ODBC juga menyediakan dukungan untuk layanan kredensial lainnya. Driver dapat mengautentikasi koneksi menggunakan plugin penyedia kredensial berbasis SAML pilihan Anda.

Untuk mengkonfigurasi layanan kredensial eksternal pada Windows:

1. Buat profil IAM yang menentukan plugin penyedia kredensial dan parameter otentikasi lainnya sesuai kebutuhan. Profil harus dikodekan ASCII, dan harus berisi pasangan kunci-nilai berikut, di mana jalur lengkap ke aplikasi PluginPath plugin:

```
plugin_name = PluginPath
```

Sebagai contoh:

```
plugin_name = C:\Users\kjson\myapp\CredServiceApp.exe
```

Untuk informasi tentang cara membuat profil, lihat [Menggunakan Profil Konfigurasi di Panduan Manajemen Cluster Amazon Redshift](#).

2. Konfigurasi driver untuk menggunakan profil ini. Driver mendeteksi dan menggunakan pengaturan otentikasi yang ditentukan dalam profil.

Mengonversi tipe data

Driver Amazon Redshift ODBC versi 2.x mendukung banyak format data umum, mengonversi antara Amazon Redshift dan tipe data SQL.

Tabel berikut mencantumkan pemetaan tipe data yang didukung.

Jenis Amazon Redshift	Jenis SQL
BIGINT	SQL_BIGINT
BOOLEAN	SQL_BIT
CHAR	SQL_CHAR
DATE	SQL_TYPE_DATE
DECIMAL	SQL_NUMERIK
DOUBLE PRECISION	SQL_GANDA
GEOGRAPHY	SQL_LONGVARBINARY
GEOMETRY	SQL_LONGVARBINARY
INTEGER	SQL_INTEGER
REAL	SQL_REAL
SMALLINT	SQL_SMALLINT
SUPER	SQL_LONGVARCHAR
TEXT	SQL_LONGVARCHAR

Jenis Amazon Redshift	Jenis SQL
TIME	SQL_TYPE_TIME
JADWAL	SQL_TYPE_TIME
TIMESTAMP	STEMPEL WAKTU SQL_TYPE_
TIMESTAMPTZ	STEMPEL WAKTU SQL_TYPE_
VARBYTE	SQL_LONGVARIABLE
VARCHAR	SQL_VARCHAR

Mengkonfigurasi opsi driver ODBC

Anda dapat menggunakan opsi konfigurasi driver untuk mengontrol perilaku driver Amazon Redshift ODBC. Opsi driver tidak peka huruf besar/kecil.

Di Microsoft Windows, Anda biasanya mengatur opsi driver saat mengonfigurasi nama sumber data (DSN). Anda juga dapat mengatur opsi driver dalam string koneksi saat Anda terhubung secara terprogram, atau dengan menambahkan atau mengubah kunci registri. `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\your_DSN` Untuk informasi selengkapnya tentang mengonfigurasi DSN, lihat. [Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#)

Di Linux, Anda mengatur opsi konfigurasi driver di `amazon.redshiftdbc.ini` file `odbc.ini` dan Anda, seperti yang dijelaskan dalam [Gunakan pengelola driver ODBC untuk mengonfigurasi driver di sistem operasi Linux dan macOS X](#). Opsi konfigurasi yang diatur dalam `amazon.redshiftdbc.ini` file berlaku untuk semua koneksi. Sebaliknya, opsi konfigurasi yang diatur dalam `odbc.ini` file khusus untuk koneksi. Opsi konfigurasi yang disetel lebih `odbc.ini` diutamakan daripada opsi konfigurasi yang ditetapkan. `amazon.redshiftdbc.ini`

Berikut ini adalah deskripsi untuk opsi yang dapat Anda tentukan untuk driver Amazon Redshift ODBC versi 2.x:

AccessKeyID

- Nilai Default - Tidak Ada
- Tipe Data - String

Kunci akses IAM untuk pengguna atau peran. Jika Anda mengatur parameter ini, Anda juga harus menentukan SecretAccessKunci.

Parameter ini bersifat opsional.

app_id

- Nilai Default - Tidak Ada
- Tipe Data - String

ID unik yang disediakan OKTA yang terkait dengan aplikasi Amazon Redshift Anda.

Parameter ini bersifat opsional.

app_name

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama aplikasi Okta yang Anda gunakan untuk mengautentikasi koneksi ke Amazon Redshift.

Parameter ini bersifat opsional.

AuthProfile

- Nilai Default - Tidak Ada
- Tipe Data - String

Profil otentikasi yang digunakan untuk mengelola pengaturan koneksi. Jika Anda mengatur parameter ini, Anda juga harus mengatur AccessKeyID dan SecretAccessKunci.

Parameter ini bersifat opsional.

AuthType

- Nilai Default - Standar
- Tipe Data - String

Opsi ini menentukan mode otentikasi yang digunakan driver saat Anda mengonfigurasi DSN menggunakan kotak dialog Amazon Redshift ODBC Driver DSN Setup:

- Standar: Otentikasi standar menggunakan nama pengguna dan kata sandi Amazon Redshift Anda.
- AWS Profil: Autentikasi IAM menggunakan profil.
- AWS IAM Credentials: Autentikasi IAM menggunakan kredensi IAM.
- Penyedia Identitas: AD FS: Autentikasi IAM menggunakan Layanan Federasi Direktori Aktif (AD FS).
- Penyedia Identitas: Plugin Auth: Plugin otorisasi yang menerima token IAM Identity Center atau token identitas berbasis JSON (OIDC) OpenID Connect (OIDC) dari penyedia identitas web mana pun yang ditautkan ke IAM Identity Center.
- Penyedia Identitas: Azure AD: Autentikasi IAM menggunakan portal Azure AD.
- Penyedia Identitas: JWT: Autentikasi IAM menggunakan JSON Web Token (JWT).
- Penyedia Identitas: Okta: Otentikasi IAM menggunakan Okta.
- Penyedia Identitas: PingFederate: Autentikasi IAM menggunakan PingFederate

Opsi ini hanya tersedia ketika Anda mengonfigurasi DSN menggunakan kotak dialog Amazon Redshift ODBC Driver DSN Setup di driver Windows. Saat Anda mengonfigurasi koneksi menggunakan string koneksi atau mesin non-Windows, driver secara otomatis menentukan apakah akan menggunakan otentikasi Kredensial Standar, AWS Profil, atau AWS IAM berdasarkan kredensi yang Anda tentukan. Untuk menggunakan penyedia identitas, Anda harus mengatur properti `plugin_name`.

Parameter ini diperlukan.

AutoCreate

- Nilai Default - 0
- Tipe Data - Boolean

Boolean yang menentukan apakah driver membuat pengguna baru ketika pengguna yang ditentukan tidak ada.

- 1 | BENAR: Jika pengguna yang ditentukan oleh UID tidak ada, driver membuat pengguna baru.
- 0 | SALAH: Driver tidak membuat pengguna baru. Jika pengguna yang ditentukan tidak ada, otentikasi gagal.

Parameter ini bersifat opsional.

CaFile

- Nilai Default - Tidak Ada
- Tipe Data - String

Jalur file ke file sertifikat CA yang digunakan untuk beberapa bentuk otentikasi IAM.

Parameter ini hanya tersedia di Linux.

Parameter ini bersifat opsional.

client_id

- Nilai Default - Tidak Ada
- Tipe Data - String

ID klien yang terkait dengan aplikasi Amazon Redshift Anda di Azure AD.

Parameter ini diperlukan jika mengotentikasi melalui layanan Azure AD.

rahasia klien_

- Nilai Default - Tidak Ada
- Tipe Data - String

Kunci rahasia yang terkait dengan aplikasi Amazon Redshift Anda di Azure AD.

Parameter ini diperlukan jika mengotentikasi melalui layanan Azure AD.

ClusterId

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama cluster Amazon Redshift yang ingin Anda sambungkan. Ini digunakan dalam otentikasi IAM. ID Cluster tidak ditentukan dalam parameter Server.

Parameter ini bersifat opsional.

Kompresi

- Nilai Default - off
- Tipe Data - String

Metode kompresi yang digunakan untuk komunikasi protokol kawat antara server Amazon Redshift dan klien atau driver.

Anda dapat menentukan salah satu nilai berikut:

- lz4: Mengatur metode kompresi yang digunakan untuk komunikasi protokol kawat dengan Amazon Redshift ke. lz4
- zstd: Menyetel metode kompresi yang digunakan untuk komunikasi protokol kawat dengan Amazon Redshift ke. zstd
- off: Tidak menggunakan kompresi untuk komunikasi protokol kawat dengan Amazon Redshift.

Parameter ini bersifat opsional.

Basis Data

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama database Amazon Redshift yang ingin Anda akses.

Parameter ini diperlukan.

DatabaseMetadataCurrentDbHanya

- Nilai Default - 1
- Tipe Data - Boolean

Boolean yang menentukan apakah driver mengembalikan metadata dari beberapa database dan cluster.

- 1 | BENAR: Driver hanya mengembalikan metadata dari database saat ini.
- 0 | SALAH. Driver mengembalikan metadata di beberapa database dan cluster Amazon Redshift.

Parameter ini bersifat opsional.

`dbgroups_filter`

- Nilai Default - Tidak Ada
- Tipe Data - String

Ekspresi reguler yang dapat Anda tentukan untuk memfilter DbGroups yang diterima dari respons SAMP ke Amazon Redshift saat menggunakan jenis autentikasi Azure, Browser Azure, dan Browser SAMP.

Parameter ini bersifat opsional.

`Driver`

- Nilai Default - Driver Amazon Redshift ODBC (x64)
- Tipe Data - String

Nama sopirnya. Satu-satunya nilai yang didukung adalah Amazon Redshift ODBC Driver (x64).

Parameter ini diperlukan jika Anda tidak mengatur DSN.

`DSN`

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama nama sumber data driver. Aplikasi ini menentukan DSN di SQL DriverConnect API.

Parameter ini diperlukan jika Anda tidak mengatur Driver. .

`EndpointUrl`

- Nilai Default - Tidak Ada
- Tipe Data - String

Titik akhir utama yang digunakan untuk berkomunikasi dengan Amazon Redshift Coral Service untuk otentikasi IAM.

Parameter ini bersifat opsional.

ForceLowercase

- Nilai Default - 0
- Tipe Data - Boolean

Boolean yang menentukan apakah driver huruf kecil semua DbGroups dikirim dari penyedia identitas ke Amazon Redshift saat menggunakan autentikasi masuk tunggal.

- 1 | BENAR: Driver huruf kecil semua DbGroups yang dikirim dari penyedia identitas.
- 0 | SALAH: Pengemudi tidak berubah DbGroups.

Parameter ini bersifat opsional.

group_federasi

- Nilai Default - 0
- Tipe Data - Boolean

Boolean yang menentukan apakah `getClusterCredentialsWithIAM` API digunakan untuk mendapatkan kredensial kluster sementara di kluster yang disediakan. Opsi ini memungkinkan pengguna IAM berintegrasi dengan peran database Redshift dalam cluster yang disediakan. Perhatikan bahwa opsi ini tidak berlaku untuk ruang nama Redshift Tanpa Server.

- 1 | BENAR: Driver menggunakan `getClusterCredentialsWithIAM` API untuk mendapatkan kredensial cluster sementara di cluster yang disediakan.
- 0 | FALSE: Driver menggunakan `getClusterCredentials` API default untuk mendapatkan kredensial cluster sementara di cluster yang disediakan.

Parameter ini bersifat opsional.

http_proxy_host

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama host atau alamat IP server proxy tempat Anda ingin melewati proses otentikasi IAM.

Parameter ini bersifat opsional.

`http_proxy_password`

- Nilai Default - Tidak Ada
- Tipe Data - String

Kata sandi yang Anda gunakan untuk mengakses server proxy. Ini digunakan untuk otentikasi IAM.

Parameter ini bersifat opsional.

`http_proxy_port`

- Nilai Default - Tidak Ada
- Tipe Data - Integer

Jumlah port yang digunakan server proxy untuk mendengarkan koneksi klien. Ini digunakan untuk otentikasi IAM.

Parameter ini bersifat opsional.

`http_proxy_nama pengguna`

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama pengguna yang Anda gunakan untuk mengakses server proxy. Ini digunakan untuk otentikasi IAM.

Parameter ini bersifat opsional.

`IAM`

- Nilai Default - 0
- Tipe Data - Boolean

Boolean yang menentukan apakah driver menggunakan metode otentikasi IAM untuk mengautentikasi koneksi.

- 1 | BENAR: Driver menggunakan salah satu metode autentikasi IAM (menggunakan kunci akses dan secret key pair, atau profil, atau layanan kredensial).
- 0 | SALAH. Driver menggunakan otentikasi standar (menggunakan nama pengguna dan kata sandi database Anda).

Parameter ini bersifat opsional.

`identity_namespace`

- Nilai Default - Tidak Ada
- Tipe Data - String

Namespace identitas yang akan digunakan saat mengautentikasi menggunakan.

IdpTokenAuthPlugin Ini membantu Redshift menentukan instance IAM Identity Center mana yang akan digunakan.

Jika hanya ada satu instance IAM Identity Center yang ada atau jika namespace identitas default disetel, maka parameter ini opsional, jika tidak diperlukan.

`idp_host`

- Nilai Default - Tidak Ada
- Tipe Data - String

Host iDP (penyedia identitas) yang Anda gunakan untuk mengautentikasi ke Amazon Redshift.

Parameter ini bersifat opsional.

`idp_port`

- Nilai Default - Tidak Ada
- Tipe Data - Integer

Port untuk IDP (penyedia identitas) yang Anda gunakan untuk mengautentikasi ke Amazon Redshift. Bergantung pada port yang Anda pilih saat membuat, memodifikasi, atau memigrasi kluster, izinkan akses ke port yang dipilih.

Parameter ini bersifat opsional.

`idp_response_timeout`

- Nilai Default - 120
- Tipe Data - Integer

Jumlah detik driver menunggu respons SAMP dari penyedia identitas saat menggunakan layanan SAMP atau Azure AD melalui plugin browser.

Parameter ini bersifat opsional.

`idp_penyewa`

- Nilai Default - Tidak Ada
- Tipe Data - String

ID penyewa Azure AD yang terkait dengan aplikasi Amazon Redshift Anda.

Parameter ini diperlukan jika mengautentikasi melalui layanan Azure AD.

`idp_use_https_proxy`

- Nilai Default - 0
- Tipe Data - Boolean

Boolean yang menentukan apakah driver melewati proses otentikasi untuk penyedia identitas (iDP) melalui server proxy.

- 1 | BENAR: Driver melewati proses otentikasi IDP melalui server proxy.
- 0 | SALAH. Driver tidak melewati proses otentikasi IDP melalui server proxy.

Parameter ini bersifat opsional.

InstanceProfile

- Nilai Default - 0
- Tipe Data - Boolean

Boolean yang menentukan apakah driver menggunakan profil instans Amazon EC2, saat dikonfigurasi untuk menggunakan profil untuk otentikasi.

- 1 | BENAR: Driver menggunakan profil instans Amazon EC2.
- 0 | SALAH. Pengemudi menggunakan profil peran berantai yang ditentukan oleh opsi Nama Profil (Profil) sebagai gantinya.

Parameter ini bersifat opsional.

KeepAlive

- Nilai Default - 1
- Tipe Data - Boolean

Boolean yang menentukan apakah driver menggunakan TCP keepalives untuk mencegah koneksi dari timing out.

- 1 | BENAR: Driver menggunakan TCP keepalives untuk mencegah koneksi dari timing out.
- 0 | SALAH. Pengemudi tidak menggunakan keepalives TCP.

Parameter ini bersifat opsional.

KeepAliveHitung

- Nilai Default - 0
- Tipe Data - Integer

Jumlah paket TCP keepalive yang dapat hilang sebelum koneksi dianggap rusak. Ketika parameter ini diatur ke 0, driver menggunakan sistem default untuk pengaturan ini.

Parameter ini bersifat opsional.

KeepAliveInterval

- Nilai Default - 0
- Tipe Data - Integer

Jumlah detik antara setiap transmisi ulang TCP keepalive. Ketika parameter ini diatur ke 0, driver menggunakan sistem default untuk pengaturan ini.

Parameter ini bersifat opsional.

KeepAliveWaktu

- Nilai Default - 0
- Tipe Data - Integer

Jumlah detik tidak aktif sebelum driver mengirim paket TCP keepalive. Ketika parameter ini diatur ke 0, driver menggunakan sistem default untuk pengaturan ini.

Parameter ini bersifat opsional.

listen_port

- Nilai Default - 7890
- Tipe Data - Integer

Port yang digunakan driver untuk menerima respons SAMP dari penyedia identitas saat menggunakan layanan SAMP atau Azure AD melalui plugin browser.

Parameter ini bersifat opsional.

login_url

- Nilai Default - Tidak Ada
- Tipe Data - String

URL untuk sumber daya di situs web penyedia identitas saat menggunakan plugin SAML Browser generik.

Parameter ini diperlukan jika mengautentikasi dengan layanan SAMP atau Azure AD melalui plugin browser.

login ToRp

- Nilai default - urn:amazon:webservices
- Tipe Data - String

Pihak yang mengandalkan percaya bahwa Anda ingin menggunakan untuk jenis otentikasi AD FS.

String ini opsional.

LogLevel

- Nilai Default - 0
- Tipe Data - Integer

Gunakan properti ini untuk mengaktifkan atau menonaktifkan logging di driver dan untuk menentukan jumlah detail yang disertakan dalam log. file. Kami menyarankan Anda hanya mengaktifkan logging cukup lama untuk menangkap masalah, karena logging mengurangi kinerja dan dapat menghabiskan sejumlah besar ruang disk.

Atur properti ke salah satu nilai berikut:

- 0: MATI. Nonaktifkan semua logging.
- 1: KESALAHAN. Mencatat peristiwa kesalahan yang memungkinkan driver untuk terus berjalan tetapi menghasilkan kesalahan.
- 2: API_CALL. Log panggilan fungsi API ODBC dengan nilai argumen fungsi.
- 3: INFO. Log informasi umum yang menggambarkan kemajuan pengemudi.
- 4: MSG_PROTOCOL. Log informasi rinci dari pesan pengemudi protocol.
- 5: DEBUG. Mencatat semua aktivitas pengemudi
- 6: DEBUG_APPEND. Terus tambahkan log untuk semua aktivitas pengemudi.

Saat logging diaktifkan, driver menghasilkan file log berikut di lokasi yang Anda tentukan di LogPathproperti:

- `redshift_odbc.log.1` File yang mencatat aktivitas driver yang terjadi selama jabat tangan koneksi.
- `redshift_odbc.log` File untuk semua aktivitas driver setelah koneksi dibuat ke database.

Parameter ini bersifat opsional.

LogPath

- Nilai Default - Direktori TEMP khusus OS
- Tipe Data - String

Jalur lengkap ke folder tempat driver menyimpan file log saat LogLevel lebih tinggi dari 0.

Parameter ini bersifat opsional.

Min_tls

- Nilai Default - 1.2
- Tipe Data - String

Versi minimum TLS/SSL yang driver memungkinkan penyimpanan data untuk digunakan untuk mengenkripsi koneksi. Misalnya, jika TLS 1.2 ditentukan, TLS 1.1 tidak dapat digunakan untuk mengenkripsi koneksi.

Min_tls menerima nilai-nilai berikut:

- 1.0: Koneksi harus menggunakan setidaknya TLS 1.0.
- 1.1: Koneksi harus menggunakan setidaknya TLS 1.1.
- 1.2: Koneksi harus menggunakan setidaknya TLS 1.2.

Parameter ini bersifat opsional.

partner_spid

- Nilai Default - Tidak Ada
- Tipe Data - String

Nilai SPID mitra (ID penyedia layanan) yang akan digunakan saat mengautentikasi koneksi menggunakan layanan. PingFederate

Parameter ini bersifat opsional.

Kata Sandi | PWS

- Nilai Default - Tidak Ada
- Tipe Data - String

Kata sandi yang sesuai dengan nama pengguna database yang Anda berikan di bidang User (UID | User | LogonId).

Parameter ini bersifat opsional.

plugin_name

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama plugin penyedia kredensial yang ingin Anda gunakan untuk otentikasi.

Nilai berikut didukung:

- `ADFS`: Gunakan Layanan Federasi Direktori Aktif untuk otentikasi.
- `AzureAD`: Gunakan Layanan Microsoft Azure Active Directory (AD) untuk otentikasi.
- `BrowserAzureAD`: Gunakan plugin browser untuk Layanan Microsoft Azure Active Directory (AD) untuk otentikasi.
- `BrowserSAML`: Gunakan plugin browser untuk layanan SAMP seperti Okta atau Ping untuk otentikasi.
- `IdpTokenAuthPlugin`: Plugin otorisasi yang menerima token IAM Identity Center atau OpenID Connect (OIDC) JSON berbasis token identitas (JWT) dari penyedia identitas web mana pun yang ditautkan ke IAM Identity Center.
- `JWT`: Gunakan JSON Web Token (JWT) untuk otentikasi.
- `Ping`: Gunakan PingFederate layanan untuk otentikasi.
- `Okta`: Gunakan layanan Okta untuk otentikasi.

Parameter ini bersifat opsional.

Pelabuhan | PortNumber

- Nilai default - 5439
- Tipe Data - Integer

Jumlah port TCP yang digunakan server Amazon Redshift untuk mendengarkan koneksi klien.

Parameter ini bersifat opsional.

preferred_role

- Nilai Default - Tidak Ada
- Tipe Data - String

Peran yang ingin Anda asumsikan selama koneksi ke Amazon Redshift. Ini digunakan untuk otentikasi IAM.

Parameter ini bersifat opsional.

Profil

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama AWS profil pengguna yang digunakan untuk mengautentikasi ke Amazon Redshift.

- Jika parameter Use Instance Profile (InstanceProfileproperty) disetel ke 1 | TRUE, setelah tersebut akan diutamakan dan driver menggunakan profil instans Amazon EC2 sebagai gantinya.
- Lokasi default untuk file kredensyal yang berisi profil adalah. ~/.aws/Credentials Variabel AWS_SHARED_CREDENTIALS_FILE lingkungan dapat digunakan untuk menunjuk ke file kredensyal yang berbeda.

Parameter ini bersifat opsional.

provider_name

- Nilai Default - Tidak Ada

- Tipe Data - String

Penyedia otentikasi yang dibuat oleh pengguna menggunakan kueri CREATE IDENTITY PROVIDER. Ini digunakan dalam otentikasi Amazon Redshift asli.

Parameter ini bersifat opsional.

ProxyHost

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama host atau alamat IP dari server proxy yang ingin Anda sambungkan.

Parameter ini bersifat opsional.

ProxyPort

- Nilai Default - Tidak Ada
- Tipe Data - Integer

Jumlah port yang digunakan server proxy untuk mendengarkan koneksi klien.

Parameter ini bersifat opsional.

ProxyPwd

- Nilai Default - Tidak Ada
- Tipe Data - String

Kata sandi yang Anda gunakan untuk mengakses server proxy.

Parameter ini bersifat opsional.

ProxyUid

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama pengguna yang Anda gunakan untuk mengakses server proxy.

Parameter ini bersifat opsional.

ReadOnly

- Nilai Default - 0
- Tipe Data - Boolean

Boolean yang menentukan apakah driver dalam mode read-only.

- 1 | BENAR: Koneksi dalam mode hanya-baca, dan tidak dapat menulis ke penyimpanan data.
- 0 | SALAH: Koneksi tidak dalam mode read-only, dan dapat menulis ke penyimpanan data.

Parameter ini bersifat opsional.

region

- Nilai Default - Tidak Ada
- Tipe Data - String

AWS Wilayah tempat cluster Anda berada.

Parameter ini bersifat opsional.

SecretAccessKunci

- Nilai Default - Tidak Ada
- Tipe Data - String

Kunci rahasia IAM untuk pengguna atau peran. Jika Anda mengatur parameter ini, Anda juga harus mengatur AccessKeyID.

Parameter ini bersifat opsional.

SessionToken

- Nilai Default - Tidak Ada

- Tipe Data - String

Token sesi IAM sementara yang terkait dengan peran IAM yang Anda gunakan untuk mengautentikasi.

Parameter ini bersifat opsional.

Server | HostName | Tuan rumah

- Nilai Default - Tidak Ada
- Tipe Data - String

Server endpoint untuk terhubung ke.

Parameter ini diperlukan.

ssl_insecure

- Nilai Default - 0
- Tipe Data - Boolean

Boolean yang menentukan apakah driver memeriksa keaslian sertifikat server iDP.

- 1 | BENAR: Driver tidak memeriksa keaslian sertifikat server iDP.
- 0 | FALSE: Driver memeriksa keaslian sertifikat server iDP

Parameter ini bersifat opsional.

SSLMode

- Nilai Default - `verify-ca`
- Tipe Data - String

Mode verifikasi sertifikat SSL untuk digunakan saat menghubungkan ke Amazon Redshift. Nilai-nilai berikut dimungkinkan:

- `verify-full`: Connect hanya menggunakan SSL, otoritas sertifikat tepercaya, dan nama server yang cocok dengan sertifikat.

- `verify-ca`: Connect hanya menggunakan SSL dan otoritas sertifikat tepercaya.
- `require`: Connect hanya menggunakan SSL.
- `prefer`: Connect menggunakan SSL jika tersedia. Jika tidak, sambungkan tanpa menggunakan SSL.
- `allow`: Secara default, sambungkan tanpa menggunakan SSL. Jika server membutuhkan koneksi SSL, maka gunakan SSL.
- `disable`: Connect tanpa menggunakan SSL.

Parameter ini bersifat opsional.

StsConnectionBatas waktu

- Nilai Default - 0
- Tipe Data - Integer

Waktu tunggu maksimum untuk koneksi IAM, dalam hitungan detik. Jika disetel ke 0 atau tidak ditentukan, driver menunggu 60 detik untuk setiap AWS STS panggilan.

Parameter ini bersifat opsional.

StsEndpointUrl

- Nilai Default - Tidak Ada
- Tipe Data - String

Opsi ini menentukan endpoint utama yang digunakan untuk berkomunikasi dengan (). AWS Security Token Service AWS STS

Parameter ini bersifat opsional.

token

- Nilai Default - Tidak Ada
- Tipe Data - String

Pusat Identitas IAM menyediakan token akses atau OpenID Connect (OIDC) JSON Web Token (JWT) yang disediakan oleh penyedia identitas web yang terhubung dengan IAM Identity Center.

Aplikasi Anda harus menghasilkan token ini dengan mengautentikasi pengguna aplikasi Anda dengan IAM Identity Center atau penyedia identitas yang ditautkan dengan IAM Identity Center.

Parameter ini bekerja dengan `IdpTokenAuthPlugin`.

`token_type`

- Nilai Default - Tidak Ada
- Tipe Data - String

Jenis token yang digunakan di `IdpTokenAuthPlugin`.

Anda dapat menentukan salah satu nilai berikut:

`ACCESS_TOKEN`

Masukkan ini jika Anda menggunakan token akses yang disediakan Pusat Identitas IAM.

`EXT_JWT`

Masukkan ini jika Anda menggunakan OpenID Connect (OIDC) JSON Web Token (JWT) yang disediakan oleh penyedia identitas berbasis web yang terintegrasi dengan IAM Identity Center.

Parameter ini bekerja dengan `IdpTokenAuthPlugin`.

`UID | Pengguna | LogonID`

- Nilai Default - Tidak Ada
- Tipe Data - String

Nama pengguna yang Anda gunakan untuk mengakses server Amazon Redshift.

Parameter ini diperlukan jika Anda menggunakan otentikasi database.

`web_identity_token`

- Nilai Default - Tidak Ada
- Tipe Data - String

Token OAUTH yang disediakan oleh penyedia identitas. Ini digunakan dalam plugin JWT.

Parameter ini diperlukan jika Anda mengatur parameter `plugin_name` ke.

`BasicJwtCredentialsProvider`

Versi driver ODBC sebelumnya

Unduh versi driver Amazon Redshift ODBC versi 2.x sebelumnya hanya jika alat Anda memerlukan versi driver tertentu.

Menggunakan versi driver ODBC sebelumnya untuk Microsoft Windows

Berikut ini adalah versi sebelumnya dari driver Amazon Redshift ODBC versi 2.x untuk Microsoft Windows:

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.1.0/ AmazonRedshift ODBC64-2.1.1.0.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.0.0/ AmazonRedshift ODBC64-2.1.0.0.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/ AmazonRedshift ODBC64-2.0.1.0.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/ AmazonRedshift ODBC64-2.0.0.11.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/ AmazonRedshift ODBC64-2.0.0.9.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/ AmazonRedshift ODBC64-2.0.0.8.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/ AmazonRedshift ODBC64-2.0.0.7.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/ AmazonRedshift ODBC64-2.0.0.6.MSi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/ AmazonRedshift ODBC64-2.0.0.5.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/ AmazonRedshift ODBC64-2.0.0.3.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/ AmazonRedshift ODBC64-2.0.0.1.msi>

Gunakan versi driver ODBC sebelumnya untuk Linux

Berikut ini adalah versi sebelumnya dari driver Amazon Redshift ODBC versi 2.x untuk Linux:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.1.0/ AmazonRedshift ODBC-64-bit-2.1.1.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.0.0/ AmazonRedshift ODBC-64-bit-2.1.0.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/ AmazonRedshift ODBC-64-bit-2.0.1.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/ AmazonRedshift ODBC-64-bit-2.0.0.11.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/ AmazonRedshift ODBC-64-bit-2.0.0.9.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/ AmazonRedshift ODBC-64-bit-2.0.0.8.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/ AmazonRedshift ODBC-64-bit-2.0.0.7.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/ AmazonRedshift ODBC-64-bit-2.0.0.6.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/ AmazonRedshift ODBC-64-bit-2.0.0.5.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/ AmazonRedshift ODBC-64-bit-2.0.0.3.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/ AmazonRedshift ODBC-64-bit-2.0.0.1.x86_64.rpm

Mengkonfigurasi koneksi ODBC

Anda dapat menggunakan koneksi ODBC untuk terhubung ke kluster Amazon Redshift Anda dari banyak alat dan aplikasi klien SQL pihak ketiga. Untuk melakukan ini, atur koneksi di komputer klien Anda atau instans Amazon EC2. Jika alat klien Anda mendukung JDBC, Anda mungkin memilih untuk menggunakan jenis koneksi itu daripada ODBC karena kemudahan konfigurasi yang disediakan JDBC. Namun, jika alat klien Anda tidak mendukung JDBC, ikuti langkah-langkah di bagian ini untuk mengonfigurasi koneksi ODBC.

Amazon Redshift menyediakan driver ODBC 64-bit untuk sistem operasi Linux, Windows, dan macOS X. Driver ODBC 32-bit dihentikan. Pembaruan lebih lanjut tidak akan dirilis, kecuali untuk patch keamanan yang mendesak.

[Untuk informasi terbaru tentang fungsionalitas dan prasyarat driver ODBC, lihat catatan rilis driver Amazon Redshift ODBC.](#)

Untuk informasi penginstalan dan konfigurasi untuk driver Amazon Redshift ODBC, lihat panduan pemasangan dan konfigurasi konektor [Amazon Redshift ODBC](#).

Jika Anda ingin menggunakan koneksi ODBC, lakukan langkah-langkah berikut.

Topik

- [Dapatkan URL ODBC untuk klaster Anda](#)
- [Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#)
- [Instal driver Amazon Redshift ODBC di Linux](#)
- [Instal driver Amazon Redshift ODBC di macOS X](#)
- [Gunakan pengelola driver ODBC untuk mengonfigurasi driver di sistem operasi Linux dan macOS X](#)
- [Konfigurasi opsi driver ODBC](#)
- [Versi driver ODBC sebelumnya](#)

Dapatkan URL ODBC untuk klaster Anda

Amazon Redshift menampilkan URL ODBC untuk klaster Anda di konsol Amazon Redshift. URL ini berisi informasi untuk mengatur koneksi antara komputer klien Anda dan database.

URL ODBC memiliki format berikut:

```
Driver={driver};Server=endpoint;Database=database_name;UID=user_name;PWD=password
```

Bidang format yang ditunjukkan sebelumnya memiliki nilai berikut.

Bidang	Nilai
Driver	Nama driver ODBC 64-bit yang akan digunakan: Amazon Redshift (x64). Nama driver ODBC 32-bit: Amazon Redshift (x86).

Bidang	Nilai
Server	Titik akhir dari cluster Amazon Redshift.
Database	Database yang Anda buat untuk cluster Anda.
UID	Nama pengguna akun pengguna yang memiliki izin untuk terhubung ke database. Nilai ini adalah izin database, bukan izin Amazon Redshift, meskipun Anda dapat menggunakan akun pengguna admin yang Anda atur saat meluncurkan klaster.
PWD	Kata sandi untuk akun pengguna untuk terhubung ke database.
Port	Nomor port yang Anda tentukan saat Anda meluncurkan cluster. Jika Anda memiliki firewall, pastikan port ini terbuka untuk Anda gunakan.

Bidang dalam tabel sebelumnya dapat berisi karakter khusus berikut:

```
[ ] { } ( ) , ; ? * = ! @
```

Jika Anda menggunakan karakter khusus ini, Anda harus melampirkan nilainya dalam kurung kurawal. Misalnya, nilai kata sandi `Your ; password123` dalam string koneksi direpresentasikan sebagai `PWD={Your ; password123};`.

Karena `Field=value` pasangan dipisahkan oleh titik koma, kombinasi `}` dan `;` dengan sejumlah spasi di antaranya dianggap sebagai akhir dari pasangan. `Field={value};` Kami menyarankan Anda menghindari urutan `};` dalam nilai bidang Anda. Misalnya, jika Anda menetapkan nilai kata sandi Anda sebagai `PWD={This is a passwor} ;d};`, kata sandi Anda akan menjadi `This is a passwor} ;` dan URL akan error.

Berikut ini adalah contoh URL ODBC.

```
Driver={Amazon Redshift (x64)};
        Server=examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com;
        Database=dev;
        UID=adminuser;
        PWD=insert_your_admin_user_password_here;
        Port=5439
```

Untuk informasi tentang cara mendapatkan koneksi ODBC Anda, lihat [Menemukan string koneksi cluster Anda](#).

Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows

Persyaratan sistem

Anda menginstal driver Amazon Redshift ODBC di komputer klien yang mengakses gudang data Amazon Redshift. Setiap komputer tempat Anda menginstal driver harus memenuhi daftar persyaratan sistem minimum. Untuk informasi tentang persyaratan sistem minimum, lihat panduan [pemasangan dan konfigurasi konektor Amazon Redshift ODBC](#).

Menginstal driver Amazon Redshift pada sistem operasi Windows

Gunakan prosedur berikut untuk mengunduh driver Amazon Redshift ODBC untuk sistem operasi Windows. Hanya gunakan driver selain ini jika Anda menjalankan aplikasi pihak ketiga yang disertifikasi untuk digunakan dengan Amazon Redshift dan yang memerlukan driver tertentu.

Untuk menginstal driver ODBC

1. Unduh salah satu dari berikut ini, tergantung pada arsitektur sistem alat atau aplikasi klien SQL Anda:

- [64-bit ODBC driver versi 1.5.9](#) driver versi 1.5.9.

Nama driver ini adalah Amazon Redshift (x64).

- [32-bit ODBC driver versi 1.4.52](#) ODBC driver versi 1.4.52

Nama driver ini adalah Amazon Redshift (x86). Driver ODBC 32-bit dihentikan. Pembaruan lebih lanjut tidak akan dirilis, kecuali untuk patch keamanan yang mendesak.

Note

Unduh paket MSI yang sesuai dengan arsitektur sistem alat atau aplikasi klien SQL Anda. Misalnya, jika alat klien SQL Anda 64-bit, instal driver 64-bit.

Kemudian unduh dan tinjau perjanjian [SIM Amazon Redshift ODBC dan JDBC](#).

2. Klik dua kali file.msi, lalu ikuti langkah-langkah di wizard untuk menginstal driver.

Membuat entri DSN sistem untuk koneksi ODBC di Microsoft Windows

Setelah Anda mengunduh dan menginstal driver ODBC, tambahkan entri nama sumber data (DSN) ke komputer klien atau instans Amazon EC2. Alat klien SQL menggunakan sumber data ini untuk terhubung ke database Amazon Redshift.

Kami menyarankan Anda membuat sistem DSN bukan DSN pengguna. Beberapa aplikasi memuat data menggunakan akun pengguna yang berbeda. Aplikasi ini mungkin tidak dapat mendeteksi DSN pengguna yang dibuat di bawah akun pengguna lain.

Note

Untuk autentikasi menggunakan kredensial AWS Identity and Access Management (IAM) atau kredensial penyedia identitas (iDP), diperlukan langkah-langkah tambahan. Untuk informasi selengkapnya, lihat [Konfigurasi koneksi JDBC atau ODBC untuk menggunakan kredensial IAM](#).

Untuk informasi tentang cara membuat entri DSN sistem, lihat panduan [pemasangan dan konfigurasi konektor Amazon Redshift ODBC](#).

Untuk membuat entri DSN sistem untuk koneksi ODBC pada Windows

1. Di menu Start, buka ODBC Data Sources.

Pastikan Anda memilih Administrator Sumber Data ODBC yang memiliki bitness yang sama dengan aplikasi klien yang Anda gunakan untuk terhubung ke Amazon Redshift.

2. Di Administrator Sumber Data ODBC, pilih tab Driver dan cari folder driver:
 - Driver Amazon Redshift ODBC (64-bit)
 - Driver Amazon Redshift ODBC (32-bit)
3. Pilih tab DSN Sistem untuk mengonfigurasi driver untuk semua pengguna di komputer, atau tab DSN Pengguna untuk mengonfigurasi driver hanya untuk akun pengguna Anda.
4. Pilih Tambahkan. Jendela Create New Data Source terbuka.
5. Pilih driver Amazon Redshift ODBC, lalu pilih Selesai. Jendela Pengaturan DSN Driver Amazon Redshift ODBC terbuka.
6. Di bawah Pengaturan Koneksi, masukkan informasi berikut:

Nama sumber data

Masukkan sebuah nama untuk sumber data. Anda dapat menggunakan nama apa pun yang ingin Anda identifikasi sumber data nanti saat Anda membuat koneksi ke cluster. Misalnya, jika Anda mengikuti Panduan Memulai Amazon Redshift, Anda dapat mengetik `exampleclusterdsn` agar mudah mengingat cluster yang Anda kaitkan dengan DSN ini.

Server

Tentukan titik akhir untuk cluster Amazon Redshift Anda. Anda dapat menemukan informasi ini di konsol Amazon Redshift di halaman detail cluster. Untuk informasi selengkapnya, lihat [Mengonfigurasi koneksi di Amazon Redshift](#).

Port

Masukkan nomor port yang digunakan database. Gunakan port yang cluster dikonfigurasi untuk digunakan ketika diluncurkan atau dimodifikasi.

Basis Data

Masukkan nama database Amazon Redshift. Jika Anda meluncurkan cluster Anda tanpa menentukan nama database, masukkan `dev`. Jika tidak, gunakan nama yang Anda pilih selama proses peluncuran. Jika Anda mengikuti Panduan Memulai Amazon Redshift, masukkan `dev`.

7. Di bawah Otentikasi, tentukan opsi konfigurasi untuk mengonfigurasi otentikasi standar atau IAM. Untuk informasi tentang opsi otentikasi, lihat “Mengonfigurasi Otentikasi di Windows” di Panduan Pemasangan dan Konfigurasi Konektor Amazon Redshift ODBC.
8. Di bawah Pengaturan SSL, tentukan nilai untuk hal berikut:

Otentikasi SSL

Pilih mode untuk menangani Secure Sockets Layer (SSL). Dalam lingkungan pengujian, Anda mungkin menggunakan `prefer`. Namun, untuk lingkungan produksi dan ketika pertukaran data yang aman diperlukan, gunakan `verify-ca` atau `verify-full`. Untuk informasi selengkapnya tentang penggunaan SSL di Windows, lihat “Mengonfigurasi Verifikasi SSL di Windows” di Panduan Pemasangan dan Konfigurasi Konektor Amazon Redshift ODBC.

9. Di bawah Opsi Tambahan, tentukan opsi tentang cara mengembalikan hasil kueri ke alat atau aplikasi klien SQL Anda. Untuk informasi selengkapnya, lihat “Mengonfigurasi Opsi Tambahan di Windows” di Panduan Pemasangan dan Konfigurasi Konektor Amazon Redshift ODBC.

10. Di Opsi Logging, tentukan nilai untuk opsi logging. Untuk informasi selengkapnya, lihat “Mengonfigurasi Opsi Pencatatan di Windows” di Panduan Pemasangan dan Konfigurasi Konektor Amazon Redshift ODBC.

Lalu pilih OK.

11. Di bawah Opsi Tipe Data, tentukan nilai untuk tipe data. Untuk informasi selengkapnya, lihat “Mengonfigurasi Opsi Jenis Data di Windows” di Panduan Pemasangan dan Konfigurasi Konektor Amazon Redshift ODBC.

Lalu pilih OK.

12. Pilih Uji. Jika komputer klien dapat terhubung ke database Amazon Redshift, Anda melihat pesan berikut: Koneksi berhasil.

Jika komputer klien gagal terhubung ke database, Anda dapat memecahkan masalah yang mungkin terjadi. Untuk informasi selengkapnya, lihat [Memecahkan masalah koneksi di Amazon Redshift](#).

13. Konfigurasi keepalives TCP di Windows untuk mencegah koneksi dari waktu habis. Untuk informasi tentang cara mengonfigurasi keepalives TCP di Windows, lihat Panduan Instalasi dan Konfigurasi Konektor Amazon Redshift ODBC.

14. Untuk membantu pemecahan masalah, konfigurasi logging. Untuk informasi tentang cara mengonfigurasi logging di Windows, lihat Panduan Instalasi dan Konfigurasi Konektor Amazon Redshift ODBC.

Instal driver Amazon Redshift ODBC di Linux

Persyaratan sistem

Anda menginstal driver Amazon Redshift ODBC di komputer klien yang mengakses gudang data Amazon Redshift. Setiap komputer tempat Anda menginstal driver harus memenuhi daftar persyaratan sistem minimum. Untuk informasi tentang persyaratan sistem minimum, lihat panduan [pemasangan dan konfigurasi konektor Amazon Redshift ODBC](#).

Menginstal driver Amazon Redshift pada sistem operasi Linux

Gunakan langkah-langkah di bagian ini untuk mengunduh dan menginstal driver Amazon Redshift ODBC pada distribusi Linux yang didukung. Proses instalasi menginstal file driver di direktori berikut:


- /opt/amazon/redshiftdbc/lib/64(untuk driver 64-bit)

- /opt/amazon/redshiftdbc/ErrorMessage
- /opt/amazon/redshiftdbc/Setup
- /opt/amazon/redshiftdbc/lib/32(untuk driver 32-bit)

Untuk menginstal driver Amazon Redshift ODBC

1. Unduh salah satu dari berikut ini, tergantung pada arsitektur sistem alat atau aplikasi klien SQL Anda:
 - [Versi driver RPM 64-bit 1.5.9](#) 1.5.9.
 - [64-bit Debian driver versi 1.5.9](#) versi 1.5.9.
 - [Driver RPM 32-bit versi 1.4.52](#) versi 1.4.52
 - [Debian driver 32-bit versi 1.4.52](#) versi 1.4.52

Nama untuk masing-masing driver ini adalah driver Amazon Redshift ODBC. Driver ODBC 32-bit dihentikan. Pembaruan lebih lanjut tidak akan dirilis, kecuali untuk patch keamanan yang mendesak.

 Note

Unduh paket yang sesuai dengan arsitektur sistem alat atau aplikasi klien SQL Anda. Misalnya, jika alat klien Anda 64-bit, instal driver 64-bit.

Kemudian unduh dan tinjau perjanjian [SIM Amazon Redshift ODBC dan JDBC](#).

2. Pergi ke lokasi di mana Anda mengunduh paket, dan kemudian jalankan salah satu perintah berikut. Gunakan perintah yang sesuai dengan distribusi Linux Anda.
 - Pada sistem operasi RHEL dan CentOS, jalankan perintah berikut.

```
yum --nogpgcheck localinstall RPMFileName
```

Ganti *RPMFileName* dengan nama file paket RPM. Misalnya, perintah berikut menunjukkan menginstal driver 64-bit.

```
yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-1.x.xx.xxxx-x.x86_64.rpm
```

- Pada SLES, jalankan perintah berikut.

```
zypper install RPMFileName
```

Ganti *RPMFileName* dengan nama file paket RPM. Misalnya, perintah berikut menunjukkan menginstal driver 64-bit.

```
zypper install AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.rpm
```

- Pada Debian, jalankan perintah berikut.

```
sudo apt install DEBFileName.deb
```

Ganti *DEBFileName.deb* dengan nama file paket Debian. Misalnya, perintah berikut menunjukkan menginstal driver 64-bit.

```
sudo apt install ./AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.deb
```

Important

Setelah Anda selesai menginstal driver, konfigurasi untuk digunakan pada sistem Anda. Untuk informasi selengkapnya tentang konfigurasi driver, lihat [Gunakan pengelola driver ODBC untuk mengonfigurasi driver di sistem operasi Linux dan macOS X](#).

Instal driver Amazon Redshift ODBC di macOS X

Persyaratan sistem

Anda menginstal driver di komputer klien yang mengakses gudang data Amazon Redshift. Setiap komputer tempat Anda menginstal driver harus memenuhi daftar persyaratan sistem minimum. Untuk informasi tentang persyaratan sistem minimum, lihat panduan [pemasangan dan konfigurasi konektor Amazon Redshift ODBC](#).

Menginstal driver Amazon Redshift ODBC di macOS X

Gunakan langkah-langkah di bagian ini untuk mengunduh dan menginstal driver Amazon Redshift ODBC pada versi macOS X yang didukung. Proses instalasi menginstal file driver di direktori berikut:

- /opt/amazon/redshift/lib/universal
- /opt/amazon/redshift/ErrorMessage
- /opt/amazon/redshift/Setup

Untuk menginstal driver Amazon Redshift ODBC di macOS X

1. Jika sistem macOS X Anda menggunakan arsitektur Intel, unduh driver [macOS X Intel](#) versi 1.5.9. Jika sistem Anda menggunakan arsitektur ARM, unduh [driver macOS X ARM versi](#) 1.5.9. Dalam kedua kasus, nama untuk driver ini adalah driver Amazon Redshift ODBC.

Kemudian unduh dan tinjau perjanjian [SIM Amazon Redshift ODBC dan JDBC](#).

2. Klik dua kali AmazonRedshiftODBC.dmg untuk me-mount image disk.
3. Klik dua kali AmazonRedshiftODBC.pkg untuk menjalankan installer.
4. Ikuti langkah-langkah di installer untuk menyelesaikan proses instalasi driver. Untuk melakukan instalasi, setuju ketentuan perjanjian lisensi.

Important

Setelah Anda selesai menginstal driver, konfigurasi untuk digunakan pada sistem Anda. Untuk informasi selengkapnya tentang konfigurasi driver, lihat [Gunakan pengelola driver ODBC untuk mengonfigurasi driver di sistem operasi Linux dan macOS X](#).

Gunakan pengelola driver ODBC untuk mengonfigurasi driver di sistem operasi Linux dan macOS X

Di sistem operasi Linux dan macOS X, Anda menggunakan pengelola driver ODBC untuk mengonfigurasi pengaturan koneksi ODBC. Manajer driver ODBC menggunakan file konfigurasi untuk menentukan dan mengkonfigurasi sumber data dan driver ODBC. Manajer driver ODBC yang Anda gunakan bergantung pada sistem operasi yang Anda gunakan:

- Manajer driver UnixODBC (untuk sistem operasi Linux)
- Manajer driver iODBC (untuk sistem operasi macOS X)

Untuk informasi selengkapnya tentang pengelola driver ODBC yang didukung untuk mengonfigurasi driver Amazon Redshift ODBC, [Persyaratan sistem](#) lihat sistem operasi Linux dan [Persyaratan sistem](#)

sistem operasi macOS X. Juga, lihat “Menentukan Manajer Driver ODBC di Mesin Non-Windows” di panduan pemasangan dan [konfigurasi konektor Amazon Redshift ODBC](#).

Tiga file diperlukan untuk mengonfigurasi driver Amazon Redshift ODBC: `amazon.redshiftdbc.ini`, `odbc.ini`, dan `odbcinst.ini`.

Jika Anda menginstal ke lokasi default, file `amazon.redshiftdbc.ini` konfigurasi terletak di salah satu direktori berikut:

- `/opt/amazon/redshiftdbc/lib/64` (untuk driver 64-bit pada sistem operasi Linux)
- `/opt/amazon/redshiftdbc/lib/32` (untuk driver 32-bit pada sistem operasi Linux)
- `/opt/amazon/redshift/lib` (untuk driver di macOS X)

Selain itu, `/opt/amazon/redshiftdbc/Setup` di Linux atau `/opt/Amazon/RedShift/Setup` di macOS X, ada contoh dan file `odbc.ini` dan `odbcinst.ini`. Anda dapat menggunakan file-file ini sebagai contoh untuk mengonfigurasi driver Amazon Redshift ODBC dan nama sumber data (DSN).

Kami tidak menyarankan menggunakan direktori instalasi driver Amazon Redshift ODBC untuk file konfigurasi. File sampel dalam `Setup` direktori hanya untuk tujuan contoh. Jika Anda menginstal ulang driver Amazon Redshift ODBC di lain waktu, atau meningkatkan ke versi yang lebih baru, direktori instalasi akan ditimpa. Anda kemudian kehilangan perubahan apa pun yang mungkin telah Anda buat pada file-file itu.

Untuk menghindari hal ini, salin `amazon.redshiftdbc.ini` file ke direktori selain direktori instalasi. Jika Anda menyalin file ini ke direktori home pengguna, tambahkan titik (.) ke awal nama file untuk menjadikannya file tersembunyi.

Untuk `odbcinst.ini` file `odbc.ini` dan, gunakan file konfigurasi di direktori home pengguna atau buat versi baru di direktori lain. Secara default, sistem operasi Linux atau macOS X Anda harus memiliki `odbc.ini` file dan `odbcinst.ini` file di direktori home pengguna (`/home/$USER` atau `~/.`). File default ini adalah file tersembunyi, yang ditunjukkan oleh titik (.) di depan setiap nama file. File-file ini hanya ditampilkan ketika Anda menggunakan `-a` bendera untuk daftar isi direktori.

Opsi apa pun yang Anda pilih untuk `odbcinst.ini` file `odbc.ini` dan, ubah file untuk menambahkan informasi konfigurasi driver dan DSN. Jika Anda membuat file baru, Anda juga perlu mengatur variabel lingkungan untuk menentukan di mana file konfigurasi ini berada.

Secara default, manajer driver ODBC dikonfigurasi untuk menggunakan versi tersembunyi dari file `odbc.ini` dan `odbcinst.ini` konfigurasi (bernama `odbc.in` dan `odbcinst.in`) terletak di

direktori home. Mereka juga dikonfigurasi untuk menggunakan `amazon.redshiftdbc.ini` file di `/lib` subfolder direktori instalasi driver. Jika Anda menyimpan file konfigurasi ini di tempat lain, atur variabel lingkungan yang dijelaskan berikut ini sehingga manajer driver dapat menemukan file. Untuk informasi selengkapnya, lihat “Menentukan Lokasi File Konfigurasi Driver” di panduan [pemasangan dan konfigurasi konektor Amazon Redshift ODBC](#).

Membuat nama sumber data di sistem operasi Linux dan macOS X

Saat menghubungkan ke penyimpanan data Anda menggunakan nama sumber data (DSN), konfigurasi `odbc.ini` file untuk menentukan DSN. Tetapkan properti dalam `odbc.ini` file untuk membuat DSN yang menentukan informasi koneksi untuk penyimpanan data Anda.

Untuk informasi tentang cara mengonfigurasi `odbc.ini` file, lihat “Membuat Nama Sumber Data pada Mesin Non-Windows” di panduan [pemasangan dan konfigurasi konektor Amazon Redshift ODBC](#) ODBC

Gunakan format berikut pada sistem operasi Linux.

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file

Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

Contoh berikut menunjukkan konfigurasi untuk `odbc.ini` dengan driver ODBC 64-bit pada sistem operasi Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift (x64)

[Amazon Redshift (x64)]
Driver=/opt/amazon/redshiftdbc/lib/64/libamazonredshiftdbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

Contoh berikut menunjukkan konfigurasi untuk `odbc.ini` dengan driver ODBC 32-bit pada sistem operasi Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x32=Amazon Redshift (x86)

[Amazon Redshift (x86)]
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

Gunakan format berikut pada sistem operasi macOS X.

```
[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
```

Contoh berikut menunjukkan konfigurasi untuk `odbc.ini` pada sistem operasi macOS X.

```
[ODBC Data Sources]
Amazon_Redshift_dylib=Amazon Redshift DSN for macOS X

[Amazon Redshift DSN for macOS X]
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

Mengonfigurasi koneksi tanpa DSN di sistem operasi Linux dan macOS X

Untuk terhubung ke penyimpanan data Anda melalui koneksi yang tidak memiliki DSN, tentukan driver dalam `odbcinst.ini` file. Kemudian berikan string koneksi tanpa DSN di aplikasi Anda.

Untuk informasi tentang cara mengonfigurasi `odbcinst.ini` file dalam kasus ini, lihat “Mengonfigurasi Koneksi Tanpa DSN pada Mesin Non-Windows” di panduan pemasangan dan konfigurasi konektor Amazon Redshift [ODBC](#).

Gunakan format berikut pada sistem operasi Linux.

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file
...
```

Contoh berikut menunjukkan `odbcinst.ini` konfigurasi untuk driver 64-bit yang diinstal di direktori default pada sistem operasi Linux.

```
[ODBC Drivers]
Amazon Redshift (x64)=Installed

[Amazon Redshift (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
```

Contoh berikut menunjukkan `odbcinst.ini` konfigurasi untuk driver 32-bit yang diinstal di direktori default pada sistem operasi Linux.

```
[ODBC Drivers]
Amazon Redshift (x86)=Installed

[Amazon Redshift (x86)]
Description=Amazon Redshift ODBC Driver (32-bit)
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so
```


Gunakan format berikut pada sistem operasi macOS X.

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/lib/amazonredshiftodbc.dylib
...
```

Contoh berikut menunjukkan `odbcinst.ini` konfigurasi untuk driver yang diinstal di direktori default pada sistem operasi macOS X.

```
[ODBC Drivers]
Amazon RedshiftODBC DSN=Installed

[Amazon RedshiftODBC DSN]
Description=Amazon Redshift ODBC Driver for macOS X
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
```

Mengonfigurasi variabel lingkungan

Gunakan manajer driver ODBC yang benar untuk memuat driver yang benar. Untuk melakukan ini, atur variabel lingkungan jalur perpustakaan. Untuk informasi selengkapnya, lihat “Menentukan Manajer Driver ODBC di Mesin Non-Windows” di panduan pemasangan dan konfigurasi [konektor Amazon Redshift ODBC](#).

Secara default, manajer driver ODBC dikonfigurasi untuk menggunakan versi tersembunyi dari file `odbc.ini` dan `odbcinst.ini` konfigurasi (bernama `odbc.inidan.odbcinst.ini`) terletak di direktori home. Mereka juga dikonfigurasi untuk menggunakan `amazon.redshiftodbc.ini` file di `/lib` subfolder direktori instalasi driver. Jika Anda menyimpan file konfigurasi ini di tempat lain, variabel lingkungan sehingga manajer driver dapat menemukan file. Untuk informasi selengkapnya, lihat “Menentukan Lokasi File Konfigurasi Driver” di Panduan Pemasangan dan Konfigurasi Konektor Amazon Redshift ODBC.

Mengkonfigurasi fitur koneksi

Anda dapat mengonfigurasi fitur koneksi berikut untuk pengaturan ODBC Anda:

- Konfigurasi driver ODBC untuk memberikan kredensi dan mengautentikasi koneksi ke database Amazon Redshift.
- Konfigurasi driver ODBC untuk menyambung ke soket yang diaktifkan dengan Secure Sockets Layer (SSL), jika Anda terhubung ke server Amazon Redshift yang mengaktifkan SSL.
- Konfigurasi driver ODBC untuk terhubung ke Amazon Redshift melalui server proxy.
- Konfigurasi driver ODBC untuk menggunakan mode pemrosesan kueri untuk mencegah kueri menghabiskan terlalu banyak memori.
- Konfigurasi driver ODBC untuk meneruskan proses otentikasi IAM melalui server proxy.
- Konfigurasi driver ODBC untuk menggunakan keepalives TCP untuk mencegah koneksi dari waktu habis.

Untuk informasi tentang fitur koneksi ini, lihat panduan [pemasangan dan konfigurasi konektor Amazon Redshift ODBC](#).

Konfigurasi opsi driver ODBC

Anda dapat menggunakan opsi konfigurasi untuk mengontrol perilaku driver Amazon Redshift ODBC.

Di Microsoft Windows, Anda biasanya mengatur opsi driver saat mengonfigurasi nama sumber data (DSN). Anda juga dapat mengatur opsi driver dalam string koneksi saat Anda terhubung secara terprogram, atau dengan menambahkan atau mengubah kunci registri. `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\your_DSN` Untuk informasi selengkapnya tentang mengonfigurasi DSN, lihat. [Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#)

Di Linux dan macOS X, Anda mengatur opsi konfigurasi driver di `amazon.redshiftdbc.ini` file `odbc.ini` dan file Anda, seperti yang dijelaskan dalam. [Gunakan pengelola driver ODBC untuk mengonfigurasi driver di sistem operasi Linux dan macOS X](#) Opsi konfigurasi yang diatur dalam `amazon.redshiftdbc.ini` file berlaku untuk semua koneksi. Sebaliknya, opsi konfigurasi yang diatur dalam `odbc.ini` file khusus untuk koneksi. Opsi konfigurasi yang disetel lebih `odbc.ini` diutamakan daripada opsi konfigurasi yang ditetapkan. `amazon.redshiftdbc.ini`

Untuk informasi tentang cara mengatur opsi konfigurasi driver ODBC, lihat panduan [pemasangan dan konfigurasi konektor Amazon Redshift ODBC](#).

Versi driver ODBC sebelumnya

Unduh versi driver Amazon Redshift ODBC sebelumnya hanya jika alat Anda memerlukan versi driver tertentu.

Gunakan versi driver ODBC sebelumnya untuk Windows

Berikut ini adalah driver 64-bit:

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/ AmazonRedshift ODBC64-1.5.7.1007.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/ AmazonRedshift ODBC64-1.4.65.1000.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/ AmazonRedshift ODBC64-1.4.62.1000.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift ODBC64-1.4.59.1000.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC64-1.4.56.1000.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.53.1000/ AmazonRedshift ODBC64-1.4.53.1000.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC64-1.4.52.1000.msi>

Driver 32-bit dihentikan dan versi sebelumnya tidak didukung.

Gunakan versi driver ODBC sebelumnya untuk Linux

Berikut ini adalah versi driver 64-bit:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/ AmazonRedshift ODBC-64-bit-1.5.7.1007-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/ AmazonRedshift ODBC-64-bit-1.4.65.1000-1.x86_64.rpm Di Wilayah China
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/ AmazonRedshift ODBC-64-bit-1.4.62.1000-1.x86_64.rpm Di Wilayah China
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift ODBC-64-bit-1.4.59.1000-1.x86_64.rpm Di Wilayah China
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift ODBC-64-bit-1.4.59.1000-1.x86_64.deb

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC-64-bit-1.4.56.1000-1.x86_64.rpm Di Wilayah China
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC-64-bit-1.4.56.1000-1.x86_64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC-64-bit-1.4.52.1000-1.x86_64.rpm Di Wilayah China
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC-64-bit-1.4.52.1000-1.x86_64.deb

Driver 32-bit dihentikan dan versi sebelumnya tidak didukung.

Menggunakan versi driver ODBC sebelumnya untuk macOS X

Berikut ini adalah versi driver Amazon Redshift ODBC untuk macOS X:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/ AmazonRedshift ODBC-1.5.7.1007.x86_64.dmg
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/ AmazonRedshift ODBC-1.4.65.1000.dmg>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/ AmazonRedshift ODBC-1.4.62.1000.dmg>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift ODBC-1.4.59.1000.dmg>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC-1.4.56.1000.dmg>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC-1.4.52.1000.dmg>

Mengkonfigurasi opsi keamanan untuk koneksi

Amazon Redshift mendukung koneksi Secure Sockets Layer (SSL) untuk mengenkripsi data dan sertifikat server untuk memvalidasi sertifikat server yang terhubung dengan klien.

Connect menggunakan SSL

Untuk mendukung koneksi SSL, Amazon Redshift membuat dan menginstal sertifikat SSL ([ACM](#))AWS Certificate Manager yang dikeluarkan pada setiap cluster. Sertifikat ACM dipercaya publik oleh sebagian besar sistem operasi, browser web, dan klien. Anda mungkin perlu mengunduh bundel sertifikat jika klien atau aplikasi SQL Anda terhubung ke Amazon Redshift menggunakan SSL dengan `sslmode` opsi koneksi disetel `require` `verify-ca`, atau `verify-full`. Jika klien Anda memerlukan sertifikat, Amazon Redshift menyediakan sertifikat bundel sebagai berikut:

- Unduh bundel dari <https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt>.
 - Nomor checksum MD5 yang diharapkan adalah `418dea9b6d5d5de7a8f1ac42e164cdf`.
 - Nomor checksum sha256 adalah `36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550`.

Jangan gunakan bundel sertifikat sebelumnya yang berada di `https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt`.

- Di China Wilayah AWS, unduh bundel dari <https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt>.
 - Nomor checksum MD5 yang diharapkan adalah `418dea9b6d5d5de7a8f1ac42e164cdf`.
 - Nomor checksum sha256 adalah `36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550`.

Jangan gunakan bundel sertifikat sebelumnya yang berada di `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` dan `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem`

Important

Amazon Redshift telah mengubah cara sertifikat SSL dikelola. Anda mungkin perlu memperbarui sertifikat CA root kepercayaan Anda saat ini untuk terus terhubung ke cluster Anda menggunakan SSL. Untuk informasi selengkapnya, lihat [Transisi ke sertifikat ACM untuk koneksi SSL](#).

Secara default, database cluster menerima koneksi apakah menggunakan SSL atau tidak. Untuk mengonfigurasi klaster Anda agar memerlukan koneksi SSL, atur `require_ssl` parameter ke `true` dalam grup parameter yang terkait dengan cluster.

Amazon Redshift mendukung mode SSL yang sesuai dengan Federal Information Processing Standard (FIPS) 140-2. Mode SSL yang sesuai dengan FIPS dinonaktifkan secara default.

Important

Aktifkan mode SSL yang sesuai dengan FIPS hanya jika sistem Anda harus sesuai dengan FIPS.

Untuk mengaktifkan mode SSL yang sesuai dengan FIPS, setel `use_fips_ssl` parameter dan parameter ke `true` dalam grup `require_ssl` parameter yang terkait dengan cluster Amazon Redshift atau grup kerja Redshift Serverless. Untuk informasi tentang memodifikasi grup parameter pada klaster, lihat [Grup parameter Amazon Redshift](#). Untuk informasi tentang memodifikasi grup parameter pada workgroup, lihat [Mengonfigurasi koneksi SSL yang sesuai dengan FIPS ke Amazon Redshift Tanpa Server](#)

Amazon Redshift mendukung protokol perjanjian kunci Elliptic Curve Diffie—Hellman Ephemeral (ECDHE). Dengan ECDHE, klien dan server masing-masing memiliki elliptic curve public-private key pair yang digunakan untuk membangun rahasia bersama melalui saluran yang tidak aman. Anda tidak perlu mengonfigurasi apa pun di Amazon Redshift untuk mengaktifkan ECDHE. Jika Anda terhubung dari alat klien SQL yang menggunakan ECDHE untuk mengenkripsi komunikasi antara klien dan server, Amazon Redshift menggunakan daftar sandi yang disediakan untuk membuat koneksi yang sesuai. [Untuk informasi lebih lanjut, lihat Elliptic curve diffie—hellman di Wikipedia dan Ciphers di situs web OpenSSL.](#)

Menggunakan SSL dan mempercayai sertifikat CA di ODBC

Jika Anda terhubung menggunakan driver Amazon Redshift ODBC terbaru (versi 1.3.7.1000 atau yang lebih baru), Anda dapat melewati bagian ini. Untuk mengunduh driver terbaru, lihat [Mengkonfigurasi koneksi ODBC](#).

Anda mungkin perlu memperbarui sertifikat CA root kepercayaan Anda saat ini untuk terus terhubung ke cluster Anda menggunakan SSL. Untuk informasi selengkapnya, lihat [Connect menggunakan SSL](#).

Anda dapat memverifikasi bahwa sertifikat yang Anda unduh cocok dengan nomor checksum MD5 yang diharapkan. Untuk melakukan ini, Anda dapat menggunakan program MD5sum pada sistem operasi Linux, atau alat lain pada sistem operasi Windows dan macOS X.

ODBC DSN berisi `sslmode` pengaturan yang menentukan cara menangani enkripsi untuk koneksi klien dan verifikasi sertifikat server. Amazon Redshift mendukung `sslmode` nilai-nilai berikut dari koneksi klien:

- `disable`

SSL dinonaktifkan dan koneksi tidak dienkripsi.

- `allow`

SSL digunakan jika server membutuhkannya.

- `prefer`

SSL digunakan jika server mendukungnya. Amazon Redshift mendukung SSL, jadi SSL digunakan saat Anda menyetelnya. `sslmode prefer`

- `require`

SSL diperlukan.

- `verify-ca`

SSL harus digunakan dan sertifikat server harus diverifikasi.

- `verify-full`

SSL harus digunakan. Sertifikat server harus diverifikasi dan nama host server harus cocok dengan atribut `hostname` pada sertifikat.

Anda dapat menentukan apakah SSL digunakan dan sertifikat server diverifikasi dalam koneksi antara klien dan server. Untuk melakukan ini, Anda perlu meninjau `sslmode` pengaturan untuk ODBC DSN Anda pada klien dan `require_ssl` pengaturan untuk cluster Amazon Redshift di server. Tabel berikut menjelaskan hasil enkripsi untuk berbagai kombinasi pengaturan klien dan server:

sslmode (klien)	Require_SSL (server)	Hasil
disable	false	Koneksi tidak dienkripsi.
disable	true	Koneksi tidak dapat dibuat karena server memerlukan SSL dan klien memiliki SSL dinonaktifkan untuk koneksi.
allow	true	Koneksi dienkripsi.
allow	false	Koneksi tidak dienkripsi.
prefer atau require	true	Koneksi dienkripsi.
prefer atau require	false	Koneksi dienkripsi.
verify-ca	true	Koneksi dienkripsi dan sertifikat server diverifikasi.
verify-ca	false	Koneksi dienkripsi dan sertifikat server diverifikasi.
verify-full	true	Koneksi dienkripsi dan sertifikat server dan nama host diverifikasi.
verify-full	false	Koneksi dienkripsi dan sertifikat server dan nama host diverifikasi.

Connect menggunakan sertifikat server dengan ODBC di Microsoft Windows

Jika Anda ingin terhubung ke kluster menggunakan SSL dan sertifikat server, unduh sertifikat terlebih dahulu ke komputer klien Anda atau instans Amazon EC2. Kemudian konfigurasi ODBC DSN.

1. Unduh bundel otoritas sertifikat Amazon Redshift ke komputer klien Anda di `lib` folder di direktori instalasi driver Anda, dan simpan file sebagai `root.crt` Untuk informasi unduhan, lihat [Connect menggunakan SSL](#).

2. Buka Administrator Sumber Data ODBC, dan tambahkan atau edit entri DSN sistem untuk koneksi ODBC Anda. Untuk Mode SSL, pilih `verify-full` kecuali Anda menggunakan alias DNS. Jika Anda menggunakan alias DNS, pilih `verify-ca` Lalu, pilih Simpan.

Untuk informasi selengkapnya tentang mengonfigurasi ODBC DSN, lihat. [Mengkonfigurasi koneksi ODBC](#)

Menggunakan sertifikat SSL dan server di Java

SSL menyediakan satu lapisan keamanan dengan mengenkripsi data yang bergerak antara klien dan cluster Anda. Menggunakan sertifikat server memberikan lapisan keamanan tambahan dengan memvalidasi bahwa klaster tersebut adalah klaster Amazon Redshift. Ia melakukannya dengan memeriksa sertifikat server yang secara otomatis diinstal pada semua cluster yang Anda sediakan. Untuk informasi lebih lanjut tentang menggunakan sertifikat server dengan JDBC, buka [Mengkonfigurasi klien dalam](#) dokumentasi PostgreSQL.

Connect menggunakan sertifikat CA trust di Java

Important

Amazon Redshift telah mengubah cara sertifikat SSL dikelola. Anda mungkin perlu memperbarui sertifikat CA root kepercayaan Anda saat ini untuk terus terhubung ke cluster Anda menggunakan SSL. Untuk informasi selengkapnya, lihat [Connect menggunakan SSL](#).

Untuk terhubung menggunakan sertifikat CA trust

Anda dapat menggunakan `redshift-keytool.jar` file tersebut untuk mengimpor sertifikat CA di bundel Amazon Redshift Certificate Authority ke Java TrustStore atau private Anda. TrustStore

1. Jika Anda menggunakan `-Djavax.net.ssl.trustStore` opsi baris perintah Java, hapus dari baris perintah, jika memungkinkan.
2. Unduh [redshift-keytool.jar](#).
3. Lakukan salah satu hal berikut ini:
 - Untuk mengimpor bundel Amazon Redshift Certificate Authority ke Java TrustStore, jalankan perintah berikut.

```
java -jar redshift-keytool.jar -s
```

- Untuk mengimpor bundel Amazon Redshift Certificate Authority ke private Anda TrustStore, jalankan perintah berikut:

```
java -jar redshift-keytool.jar -k <your_private_trust_store> -  
p <keystore_password>
```

Transisi ke sertifikat ACM untuk koneksi SSL

Amazon Redshift mengganti sertifikat SSL di klaster Anda dengan sertifikat yang dikeluarkan [AWS Certificate Manager \(ACM\)](#). ACM adalah otoritas sertifikat publik terpercaya (CA) yang dipercaya oleh sebagian besar sistem saat ini. Anda mungkin perlu memperbarui sertifikat CA root kepercayaan Anda saat ini untuk terus terhubung ke cluster Anda menggunakan SSL.

Perubahan ini hanya memengaruhi Anda jika semua hal berikut berlaku:

- Klien atau aplikasi SQL Anda terhubung ke klaster Amazon Redshift menggunakan SSL dengan `sslMode` opsi koneksi disetel `require` `keverify-ca`, atau opsi konfigurasi `verify-full`
- Anda tidak menggunakan driver Amazon Redshift ODBC atau JDBC, atau Anda menggunakan driver Amazon Redshift sebelum ODBC versi 1.3.7.1000 atau JDBC versi 1.2.8.1005.

Jika perubahan ini memengaruhi Anda di Wilayah Amazon Redshift komersial, maka Anda harus memperbarui sertifikat CA root kepercayaan Anda saat ini sebelum 23 Oktober 2017. Amazon Redshift akan mentransisikan cluster Anda untuk menggunakan sertifikat ACM antara sekarang dan 23 Oktober 2017. Perubahan seharusnya sangat sedikit atau tidak berpengaruh pada kinerja atau ketersediaan cluster Anda.

Jika perubahan ini memengaruhi Anda di Wilayah AWS GovCloud (US) (AS), maka Anda harus memperbarui sertifikat CA root kepercayaan Anda saat ini sebelum 1 April 2020 untuk menghindari gangguan layanan. Mulai tanggal ini, klien yang terhubung ke klaster Amazon Redshift menggunakan koneksi terenkripsi SSL memerlukan otoritas sertifikat terpercaya (CA) tambahan. Klien menggunakan otoritas sertifikat terpercaya untuk mengonfirmasi identitas klaster Amazon Redshift saat mereka terhubung dengannya. Tindakan Anda diperlukan untuk memperbarui klien dan aplikasi SQL Anda untuk menggunakan bundel sertifikat yang diperbarui yang menyertakan CA terpercaya baru.

⚠ Important

Di Wilayah China pada 5 Januari 2021, Amazon Redshift mengganti sertifikat SSL di kluster Anda dengan sertifikat yang dikeluarkan AWS Certificate Manager (ACM). Jika perubahan ini memengaruhi Anda di Wilayah China (Beijing) atau Wilayah China (Ningxia), maka Anda harus memperbarui sertifikat CA root kepercayaan Anda saat ini sebelum 5 Januari 2021 untuk menghindari gangguan layanan. Mulai tanggal ini, klien yang terhubung ke kluster Amazon Redshift menggunakan koneksi terenkripsi SSL memerlukan otoritas sertifikat tepercaya (CA) tambahan. Klien menggunakan otoritas sertifikat tepercaya untuk mengonfirmasi identitas kluster Amazon Redshift saat mereka terhubung dengannya. Tindakan Anda diperlukan untuk memperbarui klien dan aplikasi SQL Anda untuk menggunakan bundel sertifikat yang diperbarui yang menyertakan CA tepercaya baru.

- [Menggunakan driver Amazon Redshift ODBC atau JDBC terbaru](#)
- [Menggunakan driver Amazon Redshift ODBC atau JDBC sebelumnya](#)
- [Menggunakan jenis koneksi SSL lainnya](#)

Menggunakan driver Amazon Redshift ODBC atau JDBC terbaru

Metode yang disukai adalah menggunakan driver Amazon Redshift ODBC atau JDBC terbaru. Driver Amazon Redshift dimulai dengan ODBC versi 1.3.7.1000 dan JDBC versi 1.2.8.1005 secara otomatis mengelola transisi dari sertifikat yang ditandatangani sendiri Amazon Redshift ke sertifikat ACM. Untuk mengunduh driver terbaru, lihat [Mengkonfigurasi koneksi ODBC](#) atau [Mengkonfigurasi koneksi untuk driver JDBC versi 2.1 untuk Amazon Redshift](#).

Jika Anda menggunakan driver Amazon Redshift JDBC terbaru, sebaiknya jangan gunakan `-Djavax.net.ssl.trustStore` dalam opsi JVM. Jika Anda harus menggunakan `-Djavax.net.ssl.trustStore`, impor bundel otoritas sertifikat Redshift ke truststore yang ditunjuknya. Untuk informasi unduhan, lihat [Connect menggunakan SSL](#). Untuk informasi selengkapnya, lihat [Mengimpor bundel otoritas sertifikat Amazon Redshift ke dalam TrustStore](#).

Menggunakan driver Amazon Redshift ODBC atau JDBC sebelumnya

- Jika ODBC DSN Anda dikonfigurasi `SSLCertPath`, timpa file sertifikat di jalur yang ditentukan.
- Jika tidak `SSLCertPath` disetel, maka timpa file sertifikat yang dinamai `root.crt` di lokasi DLL driver.

Jika Anda harus menggunakan driver Amazon Redshift JDBC sebelum versi 1.2.8.1005, lakukan salah satu hal berikut:

- Jika string koneksi JDBC Anda menggunakan `sslCert` opsi, hapus opsi. `sslCert` Kemudian impor bundel otoritas sertifikat Redshift ke Java Anda. TrustStore Untuk informasi unduhan, lihat [Connect menggunakan SSL](#). Untuk informasi selengkapnya, lihat [Mengimpor bundel otoritas sertifikat Amazon Redshift ke dalam TrustStore](#).
- Jika Anda menggunakan `-Djavax.net.ssl.trustStore` opsi baris perintah Java, hapus dari baris perintah, jika memungkinkan. Kemudian impor bundel otoritas sertifikat Redshift ke Java Anda. TrustStore Untuk informasi unduhan, lihat [Connect menggunakan SSL](#). Untuk informasi selengkapnya, lihat [Mengimpor bundel otoritas sertifikat Amazon Redshift ke dalam TrustStore](#).

Mengimpor bundel otoritas sertifikat Amazon Redshift ke dalam TrustStore

Anda dapat menggunakan `redshift-keytool.jar` untuk mengimpor sertifikat CA di bundel Amazon Redshift Certificate Authority ke Java TrustStore atau truststore pribadi Anda.

Untuk mengimpor bundel otoritas sertifikat Amazon Redshift ke dalam TrustStore

1. Unduh [redshift-keytool.jar](#).
2. Lakukan salah satu hal berikut ini:
 - Untuk mengimpor bundel Amazon Redshift Certificate Authority ke Java TrustStore, jalankan perintah berikut.

```
java -jar redshift-keytool.jar -s
```

- Untuk mengimpor bundel Amazon Redshift Certificate Authority ke private Anda TrustStore, jalankan perintah berikut:

```
java -jar redshift-keytool.jar -k <your_private_trust_store> -  
p <keystore_password>
```

Menggunakan jenis koneksi SSL lainnya

Ikuti langkah-langkah di bagian ini jika Anda terhubung menggunakan salah satu dari berikut ini:

- Driver ODBC sumber terbuka

- Driver JDBC sumber terbuka
- Antarmuka [baris perintah Amazon Redshift RSQL](#)
- Binding bahasa apa pun berdasarkan libpq, seperti psycopg2 (Python) dan ruby-pg (Ruby)

Untuk menggunakan sertifikat ACM dengan jenis koneksi SSL lainnya:

1. Unduh bundel otoritas sertifikat Amazon Redshift. Untuk informasi unduhan, lihat [Connect menggunakan SSL](#).
2. Tempatkan sertifikat dari bundel di `root.crt` file Anda.
 - Pada sistem operasi Linux dan macOS X, file tersebut adalah `~/.postgresql/root.crt`
 - Di Microsoft Windows, file tersebut adalah `%APPDATA%\postgresql\root.crt`.

Menghubungkan dari alat dan kode klien

Amazon Redshift menyediakan editor kueri Amazon Redshift v2 untuk terhubung ke cluster dan grup kerja Anda. Untuk informasi selengkapnya, lihat [Mengkueri database menggunakan editor kueri Amazon Redshift v2](#).

Bagian ini menyediakan beberapa opsi untuk alat pihak ketiga untuk terhubung. Selain itu, ini menjelaskan cara terhubung ke cluster Anda secara terprogram.

Topik

- [Menghubungkan dengan Amazon Redshift RSQL](#)
- [Connect ke cluster dengan Amazon Redshift RSQL](#)
- [Perintah meta Amazon Redshift RSQL](#)
- [Variabel Amazon Redshift RSQL](#)
- [Kode kesalahan Amazon Redshift RSQL](#)
- [Variabel lingkungan Amazon Redshift RSQL](#)

Menghubungkan dengan Amazon Redshift RSQL

Amazon Redshift RSQL adalah klien baris perintah untuk berinteraksi dengan cluster dan database Amazon Redshift. Anda dapat terhubung ke kluster Amazon Redshift, menjelaskan objek database, data kueri, dan melihat hasil kueri dalam berbagai format keluaran.

Amazon Redshift RSQL mendukung kemampuan alat baris perintah PostgreSQL psql dengan serangkaian kemampuan tambahan khusus untuk Amazon Redshift. Sumber daya yang dimaksud meliputi:

- Anda dapat menggunakan otentikasi masuk tunggal menggunakan ADFS, Okta PingIdentity, Azure AdM atau penyedia identitas berbasis SAML/JWT lainnya. Anda juga dapat menggunakan penyedia identitas SAMP berbasis browser untuk otentikasi multi-faktor (MFA).
- Anda dapat menjelaskan properti atau atribut objek Amazon Redshift seperti kunci distribusi tabel, kunci pengurutan tabel, tampilan pengikatan akhir (LBV), dan tampilan terwujud. Anda juga dapat menjelaskan properti atau atribut tabel eksternal dalam AWS Glue katalog atau Apache Hive Metastore, database eksternal di Amazon RDS untuk PostgreSQL, Amazon Aurora PostgreSQL Edisi yang kompatibel dengan PostgreSQL, RDS untuk MySQL (pratinjau) dan Amazon Aurora Edisi yang kompatibel dengan MySQL (pratinjau), dan tabel yang dibagikan menggunakan Amazon Redshift Berbagi data.
- Anda juga dapat menggunakan perintah aliran kontrol yang disempurnakan seperti IF (\ELSEIF, \ELSE, \ENDIF), \GOTO dan \LABEL.

Dengan mode batch Amazon Redshift RSQL, yang menjalankan skrip yang diteruskan sebagai parameter input, Anda dapat menjalankan skrip yang menyertakan SQL dan logika bisnis yang kompleks. Jika Anda memiliki gudang data lokal yang dikelola sendiri, Anda dapat menggunakan Amazon Redshift RSQL untuk mengganti skrip ekstrak, transformasi, pemuatan (ETL), dan otomatisasi yang ada, seperti skrip Teradata BTEQ. Menggunakan RSQL membantu Anda menghindari penerapan ulang skrip secara manual dalam bahasa prosedural.

Amazon Redshift RSQL tersedia untuk sistem operasi Linux, Windows, dan macOS X.

<Untuk melaporkan masalah Amazon Redshift RSQL, tulis ke redshift-rsql-support@amazon.com

Topik

- [Memulai dengan Amazon Redshift RSQL](#)
- [Log perubahan Amazon Redshift RSQL](#)

Memulai dengan Amazon Redshift RSQL

Instal Amazon Redshift RSQL di komputer dengan sistem operasi Linux, macOS, atau Microsoft Windows.

Unduh RSQL

-
-
-

Lihat log perubahan dan unduhan untuk versi sebelumnya di [Log perubahan Amazon Redshift RSQL](#).

Instal RSQL untuk Linux

Ikuti langkah-langkah di bawah ini untuk menginstal RSQL untuk Linux.

1. Instal manajer driver dengan perintah berikut:

```
sudo yum install unixODBC openssl
```

OpenSSL diperlukan untuk distribusi Linux. Library OpenSSL terletak di repositori [Linux OpenSSL](#) Github. [Untuk informasi selengkapnya tentang OpenSSL, lihat OpenSSL](#).

2. Instal driver ODBC: [Menginstal driver Amazon Redshift pada sistem operasi Linux](#).
3. Salin file ini ke direktori home Anda:

```
cp /opt/amazon/redshiftodbc/Setup/odbc.ini ~/.odbc.ini
```

4. Atur variabel lingkungan untuk menunjuk ke lokasi file:

```
export ODBCINI=~/.odbc.ini
export ODBCSYSINI=/opt/amazon/redshiftodbc/Setup
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshiftodbc/lib/64/
amazon.redshiftodbc.ini
```

Untuk informasi selengkapnya tentang mengonfigurasi variabel lingkungan ODBC, lihat [Mengonfigurasi variabel lingkungan](#)

5. Anda sekarang dapat menginstal RSQL dengan menjalankan perintah berikut.

```
sudo rpm -i AmazonRedshiftRsql-<version>-1.x86_64.rpm
```

Instal RSQL untuk Mac

Ikuti langkah-langkah di bawah ini untuk menginstal RQL for Mac OSX.

1. Instal manajer driver dengan perintah berikut:

```
brew install unixodbc openssl@1.1 --build-from-source
```

2. Instal driver ODBC: [Instal driver Amazon Redshift ODBC di macOS X](#).
3. Salin file ini ke direktori home Anda:

```
cp /opt/amazon/redshift/Setup/odbc.ini ~/.odbc.ini
```

4. Atur variabel lingkungan untuk menunjuk ke lokasi file:

```
export ODBCINI=~/.odbc.ini
export ODBCSYSINI=/opt/amazon/redshift/Setup
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshift/lib/amazon.redshiftoDBC.ini
```

Untuk informasi selengkapnya tentang mengonfigurasi variabel lingkungan ODBC, lihat.

[Mengonfigurasi variabel lingkungan](#)

5. Setel DYLD_LIBRARY_PATH ke lokasi libodbc.dylib Anda jika tidak masuk. /usr/local/lib

```
export DYLD_LIBRARY_PATH=$DYLD_LIBRARY_PATH:/usr/local/lib
```

6. Klik dua kali file dmg untuk memasang gambar disk.
7. Klik dua kali file pkg untuk menjalankan installer.
8. Ikuti langkah-langkah di installer untuk menyelesaikan instalasi. Setuju dengan ketentuan perjanjian lisensi.

Instal RSQL untuk Windows

Ikuti instruksi di [Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#) untuk menginstal driver. Windows tidak memerlukan manajer driver.

OpenSSL diperlukan untuk Amazon Redshift RSQL di Windows. Perpustakaan OpenSSL Windows terletak di repositori [Windows OpenSSL](#). GitHub [Untuk informasi selengkapnya tentang OpenSSL, lihat OpenSSL](#).

Klik dua kali file unduhan RSQL untuk menjalankan penginstal, lalu ikuti petunjuk untuk menyelesaikan instalasi.

Log perubahan Amazon Redshift RSQL

1.0.8 (2023-06-19)

Perbaikan Bug

- Memperbaiki masalah saat output terpotong dengan perintah SHOW.
- Menambahkan dukungan ke\ de untuk menjelaskan aliran Kinesis eksternal dan topik Kafka.

1.0.7 (2023-03-22)

Perbaikan Bug

- Memperbaiki masalah di mana RSQL tidak dapat menggambarkan tampilan terwujud.
- Memperbaiki kesalahan penolakan izin pada stl_connection_log saat menggunakan Amazon Redshift Serverless.
- Memperbaiki masalah di mana RSQL dapat memproses label\ GOTO secara tidak benar.
- Memperbaiki masalah saat pesan SSL dicetak dalam mode senyap.
- Memperbaiki masalah dengan karakter acak yang ditampilkan saat menjelaskan prosedur yang disimpan.
- Memperbaiki masalah dengan mencetak pesan ERROR/INFO duplikat.

Baru

- RSQL sekarang mendapatkan informasi SSL langsung dari driver ODBC.

1.0.6 (2023-02-21)

Perbaikan Bug

- Memperbaiki masalah di mana\ d melempar kesalahan - sintaks input tidak valid untuk integer: "xid" - pada patch Redshift 1.0.46086 (P173).

Baru

- Berganti nama menjadi file instalasi untuk mencerminkan arsitektur yang didukung.

1.0.5 (2022-06-27)

Perbaiki Bug

- Kirim pesan kesalahan SQL ke kesalahan standar (stderr).
- Memperbaiki masalah dengan kode keluar saat menggunakan ON_ERROR_STOP. Skrip sekarang berakhir setelah mengalami kesalahan dan mengembalikan kode keluar yang benar.
- Maxerror sekarang tidak peka huruf besar/kecil.

Baru

- Menambahkan dukungan untuk driver ODBC 2.x.

1.0.4 (2022-03-19)

- Tambahkan dukungan untuk variabel lingkungan RSPASSWORD. Tetapkan kata sandi untuk terhubung ke Amazon Redshift. Misalnya, `export RSPASSWORD=TestPassw0rd`.

1.0.3 (2021-12-08)

Perbaiki Bug

- Dialog tetap muncul saat menggunakan `\c` atau `\l`ogon beralih antar database di OS Windows.
- Memperbaiki kerusakan saat memeriksa informasi ssl.

Amazon Redshift RSQL versi sebelumnya

Pilih salah satu tautan untuk mengunduh versi Amazon Redshift RSQL yang Anda butuhkan, berdasarkan sistem operasi Anda.

Linux 64-bit RPM

- [RSQL Versi](#)

- [RSQL Versi](#)
- [RSQL Versi 1.0.5](#)
- [RSQL Versi](#)
- [RSQL Versi 1.0.3](#) RSQL Versi 1.0.3
- [RSQL Versi 1.0.1](#) RSQL Versi 1.0.1

Mac OS 64-bit DMG

- [RSQL Versi](#)
- [RSQL Versi](#)
- [RSQL Versi 1.0.5](#) RSQL Versi 1.0.5
- [RSQL Versi 1.0.4](#) [64-bit RSQL Versi 1.0.4](#)
- [RSQL Versi 1.0.3](#) RSQL Versi 1.0.3
- [RSQL Versi 1.0.1](#) RSQL Versi 1.0.1

Windows 64-bit MSI

- [RSQL Versi](#)
- [RSQL Versi](#)
- [RSQL Versi 1.0.5](#)
- [RSQL Versi](#)
- [RSQL Versi 1.0.3](#) RSQL Versi 1.0.3
- [RSQL Versi 1.0.1](#) RSQL Versi 1.0.1

Connect ke cluster dengan Amazon Redshift RSQL

Menghubungkan tanpa DSN

1. Di konsol Amazon Redshift, pilih cluster yang ingin Anda sambungkan dan catat titik akhir, database, dan port.
2. Pada prompt perintah, tentukan informasi koneksi dengan menggunakan parameter baris perintah.

```
rsql -h <endpoint> -U <username> -d <databasename> -p <port>
```

Di sini, berikut ini berlaku:

- <endpoint> adalah Endpoint yang Anda rekam pada langkah sebelumnya.
- <username> adalah nama pengguna dengan izin untuk terhubung ke cluster.
- <databasename> adalah Nama Database yang Anda rekam pada langkah sebelumnya.
- <port> adalah Port yang Anda rekam pada langkah sebelumnya. <port> adalah parameter opsional.

Berikut contohnya.

```
rsql -h testcluster.example.amazonaws.com -U user1 -d dev -p 5439
```

3. Pada prompt kata sandi, masukkan kata sandi untuk <username> pengguna.

Respons koneksi yang berhasil terlihat seperti berikut ini.

```
% 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=#
```

Perintah untuk menghubungkan memiliki parameter yang sama di Linux, Mac OS, dan Windows.

Menghubungkan menggunakan DSN

Anda dapat menghubungkan RSQL ke Amazon Redshift dengan menggunakan nama sumber data (DSN) untuk menyederhanakan organisasi properti koneksi. Untuk informasi selengkapnya, lihat [Mengkonfigurasi fitur koneksi](#). Topik ini mencakup instruksi untuk instalasi ODBC-driver dan deskripsi

untuk properti DSN. Misalnya, bagian berikut, [Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#), menunjukkan cara terhubung dengan DSN menggunakan Windows.

Menggunakan koneksi DSN dengan kata sandi

Berikut ini menunjukkan contoh konfigurasi koneksi DSN yang menggunakan kata sandi.

Default <path to driver> untuk Mac OSX adalah /opt/amazon/redshift/lib/libamazonredshiftodbc.dylib dan untuk Linux adalah /opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so.

```
[testuser]
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
Port=<database port>
Database=<dbname>
UID=<username>
PWD=<password>
sslmode=prefer
```

Hasil output berikut dari koneksi yang berhasil.

```
% 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=#
```

Menggunakan DSN masuk tunggal

Anda dapat mengonfigurasi DSN untuk otentikasi masuk tunggal. Berikut ini menunjukkan contoh konfigurasi koneksi DSN yang menggunakan tanda tunggal Okta.

```
[testokta]
Driver=<path to driver>
```

```
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
clusterid=<cluster id>
region=<region name>
Database=<dbname>
locale=en-US
iam=1
plugin_name=<plugin name>
uid=<okta username>
pwd=<okta password>
idp_host=<idp endpoint>
app_id=<app id>
app_name=<app name>
preferred_role=<role arn>
```

Contoh output dari koneksi yang berhasil.

```
% 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=#
```

Contoh berikut menunjukkan contoh konfigurasi koneksi DSN yang menggunakan tanda tunggal Azure.

```
[testazure]
Driver=<path to driver>
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
Port=<cluster port>
clusterid=<cluster id>
region=<region name>
Database=<dbname>
```

```

locale=en-us
iam=1
plugin_name=<plugin name>
uid=<azure username>
pwd=<azure password>
idp_tenant=<Azure idp tenant uuid>
client_id=<Azure idp client uuid>
client_secret=<Azure idp client secret>

```

Menggunakan koneksi DSN dengan profil IAM

Anda dapat terhubung ke Amazon Redshift menggunakan profil IAM yang telah dikonfigurasi. Profil IAM harus memiliki hak istimewa untuk menelepon. `GetClusterCredentials` Contoh berikut menunjukkan properti DSN untuk digunakan. `RegionParameter ClusterID` dan diperlukan hanya jika Host bukan titik akhir yang disediakan Amazon seperti `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`.

```

[testiam]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Profile=default

```

Nilai untuk `Profile` kunci adalah profil bernama yang Anda pilih dari kredensial AWS CLI Anda. Contoh ini menunjukkan kredensial untuk profil bernama. `default`

```

$ cat .aws/credentials
[default]
aws_access_key_id = ASIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY

```

Berikut ini menunjukkan respons koneksi.

```

$ 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=>
```

Menggunakan koneksi DSN dengan profil Instance

Anda dapat terhubung ke Amazon Redshift menggunakan profil instans Amazon EC2. Profil instance harus memiliki hak istimewa untuk menelepon `GetClusterCredentials`. Lihat contoh di bawah ini untuk properti DSN yang akan digunakan. `RegionParameter ClusterID` dan diperlukan hanya jika Host bukan titik akhir yang disediakan Amazon seperti `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`.

```
[testinstanceprofile]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Instanceprofile=1
```

Berikut ini menunjukkan respons koneksi.

```
$ 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=>
```

Menggunakan koneksi DSN dengan rantai penyedia kredensi default

Untuk menyambung menggunakan rantai penyedia kredensi default, tentukan hanya properti IAM, dan Amazon Redshift RSQL akan mencoba memperoleh kredensial dalam urutan yang dijelaskan dalam Bekerja dengan Kredensial di SDK for [Java](#). AWS AWS Setidaknya salah satu penyedia dalam

rantai harus memiliki `GetClusterCredentials` izin. Ini berguna untuk menghubungkan dari wadah ECS, misalnya.

```
[iamcredentials]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
```

Perintah meta Amazon Redshift RSQL

Perintah meta Amazon Redshift RSQL mengembalikan catatan informasi tentang database atau objek database tertentu. Hasil dapat mencakup berbagai kolom dan metadata. Perintah lain melakukan tindakan tertentu. Perintah ini didahului dengan garis miring terbalik.

`\d [S +]`

Daftar tabel buatan pengguna lokal, tampilan reguler, tampilan yang mengikat akhir, dan tampilan terwujud. `\dS` juga mencantumkan tabel dan tampilan `\d`, seperti, tetapi objek sistem disertakan dalam catatan yang dikembalikan. +Hasil di kolom metadata tambahan `description` untuk semua objek yang terdaftar. Berikut ini menunjukkan catatan sampel dikembalikan sebagai hasil dari perintah.

```
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+] NAMA`

Menjelaskan tabel, tampilan, atau indeks. Termasuk nama kolom dan jenis. Ini juga menyediakan `diststyle`, konfigurasi cadangan, membuat tanggal (tabel dibuat setelah Oktober 2018), dan kendala.

Misalnya, `\dS+` sample mengembalikan properti objek. Menambahkan S+ hasil di kolom tambahan termasuk dalam catatan yang dikembalikan.

```
Table "public.sample"
Column |          Type          | Collation | Nullable | Default Value |
Encoding | DistKey | SortKey
-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+
col1   | smallint                |           | NO       |               |
none   | t                       |           |          |               |
col2   | character(100)          | case_sensitive | YES     |               |
none   | f                       |           |          |               |
col3   | character varying(100) | case_sensitive | YES     |               |
text32k | f                       |           |          |               |
col4   | timestamp without time zone |           | YES     |               |
runlength | f                       |           |          |               |
col5   | super                   |           | YES     |               |
zstd   | f                       |           |          |               |
col6   | bigint                  |           | YES     |               |
az64   | f                       |           |          |               |

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)
```

Gaya distribusi, atau Diststyle, dari tabel bisa KEY, AUTO, EVEN atau ALL.

Backup menunjukkan apakah tabel dicadangkan saat snapshot diambil. Nilai-nilai yang valid adalah YES atau NO.

Dibuat adalah stempel waktu untuk saat tabel dibuat. Tanggal pembuatan tidak tersedia untuk tabel Amazon Redshift yang dibuat sebelum November 2018. Tabel yang dibuat sebelum tanggal ini menampilkan n/a (Tidak Tersedia).

Kendala Unik mencantumkan kendala kunci unik dan primer di atas meja.

Kendala kunci asing mencantumkan kendala kunci asing di atas meja.

\dC [+] [POLA]

Daftar gips. Termasuk jenis sumber, tipe target, dan apakah pemeran itu implisit.

Berikut ini menunjukkan subset hasil dari\dC+.

```
List of casts
      source type      |      target type      |      function      |
implicit? | description
-----+-----+-----+
+-----+-----+-----+
"char"      | character              | bpchar             | in
assignment |
"char"      | character varying     | text               | in
assignment |
"char"      | integer                | int4               | no
      |
"char"      | text                   | text               | yes
      |
"path"      | point                  | point              | no
      |
"path"      | polygon                | polygon            | in
assignment |
abstime    | date                   | date               | in
assignment |
abstime    | integer                | (binary coercible) | no
      |
abstime    | time without time zone | time               | in
assignment |
abstime    | timestamp with time zone | timestamptz      | yes
      |
abstime    | timestamp without time zone | timestamp         | yes
      |
bigint     | bit                    | bit                | no
      |
bigint     | boolean                | bool               | yes
      |
bigint     | character               | bpchar             | in
assignment |
bigint     | character varying     | text               | in
assignment |
bigint     | double precision       | float8             | yes
      |
```

```

bigint          | integer          | int4           | in
assignment |
bigint          | numeric          | numeric        | yes
|
bigint          | oid              | oid            | yes
|
bigint          | real             | float4         | yes
|
bigint          | regclass         | oid            | yes
|
bigint          | regoper          | oid            | yes
|
bigint          | regoperator      | oid            | yes
|
bigint          | regproc          | oid            | yes
|
bigint          | regprocedure     | oid            | yes
|
bigint          | regtype          | oid            | yes
|
bigint          | smallint         | int2           | in
assignment |
bigint          | super            | int8_partiql  | in
assignment |

```

`\dd [S] [POLA]`

Menampilkan deskripsi objek yang tidak ditampilkan di tempat lain.

`\de`

Daftar tabel eksternal. Ini termasuk tabel dalam katalog AWS Glue data, Hive Metastore dan tabel federasi dari Amazon RDS/Aurora MySQL, Amazon RDS/Aurora PostgreSQL dan tabel Amazon Redshift datashare.

`\NAMA`

Menjelaskan tabel eksternal.

Contoh berikut menunjukkan tabel AWS Glue eksternal.

```
# \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"}

Meja Hive Metastore.

```
# \de emr.lineitem
```

Hive Metastore External Table "emr.lineitem"

Column	External Type	Redshift Type	Position	Partition Key	Nullable
l_orderkey	bigint	bigint	1	0	
l_partkey	bigint	bigint	2	0	
l_suppkey	int	int	3	0	
l_linenumber	int	int	4	0	
l_quantity	decimal(12,2)	decimal(12,2)	5	0	
l_extendedprice	decimal(12,2)	decimal(12,2)	6	0	
l_discount	decimal(12,2)	decimal(12,2)	7	0	
l_tax	decimal(12,2)	decimal(12,2)	8	0	

l_returnflag	char(1)	char(1)	9	0	
l_linestatus	char(1)	char(1)	10	0	
l_commitdate	date	date	11	0	
l_receiptdate	date	date	12	0	
l_shipinstruct	char(25)	char(25)	13	0	
l_shipmode	char(10)	char(10)	14	0	
l_comment	varchar(44)	varchar(44)	15	0	
l_shipdate	date	date	16	1	

Location: s3://redshiftbucket/cetas

Input_format: org.apache.hadoop.hive.q1.io.parquet.MapredParquetInputFormat

Output_format: org.apache.hadoop.hive.q1.io.parquet.MapredParquetOutputFormat

Serialization_lib: org.apache.hadoop.hive.q1.io.parquet.serde.ParquetHiveSerDe

Serde_parameters: {"serialization.format":"1"}

Parameters: {"EXTERNAL":"TRUE", "numRows":"4307207",
"transient_lastDdlTime":"1626990007"}

PostgreSQL tabel eksternal.

```
# \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

col134	text	varchar(65535)	31	0
col135	time without time zone	varchar(65535)	32	0
col136	time with time zone	varchar(65535)	33	0
col137	timestamp without time zone	timestamp without time zone	34	0
col138	timestamp with time zone	timestamp with time zone	35	0
col139	tsquery	varchar(65535)	36	0
col140	tsvector	varchar(65535)	37	0
col141	txid_snapshot	varchar(65535)	38	0
col142	uuid	varchar(65535)	39	0
col143	xml	varchar(65535)	40	0

`\df [anptw] [S+] [POLA]`

Daftar fungsi dari berbagai jenis. Perintah `\df`, misalnya, mengembalikan daftar fungsi. Hasil mencakup properti seperti nama, tipe data yang dikembalikan, hak akses, dan metadata tambahan. Jenis fungsi dapat mencakup pemicu, prosedur tersimpan, fungsi jendela dan jenis lainnya. Ketika Anda menambahkan `S+` ke perintah, misalnya `\dfantS+`, kolom metadata tambahan disertakan, seperti `owner`, dan `security access privileges`

`\dL [S+] [POLA]`

Daftar data tentang bahasa prosedural yang terkait dengan database. Informasi mencakup nama, seperti `plpgsql`, dan metadata tambahan, yang mencakup apakah itu tepercaya, hak akses, dan deskripsi. Contoh panggilan, misalnya `\dLS+`, yang mencantumkan bahasa dan propertinya. Ketika Anda menambahkan `S+` ke perintah, kolom metadata tambahan disertakan, seperti `call handler access privileges`

Hasil sampel:

```
List of languages
```


name	trusted	internal language	call handler	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+] [POLA]

Daftar tampilan terwujud. Misalnya, \ dmS+ daftar tampilan terwujud dan propertinya. Saat Anda menambahkan S+ perintah, kolom metadata tambahan disertakan.

\ dn [S+] [POLA]

Daftar skema. Ketika Anda menambahkan S+ ke perintah, misalnya \ dnS+, kolom metadata tambahan disertakan, seperti dan. description access privileges

\ dp [POLA]

Daftar hak akses tabel, tampilan, dan urutan.

`\ dt [S+] [POLA]`

Daftar tabel. Ketika Anda menambahkan S+ ke perintah, misalnya `\ dt S+`, kolom metadata tambahan disertakan, seperti `description` dalam kasus ini.

`\ du`

Daftar pengguna untuk database. Termasuk nama mereka dan peran mereka, seperti Superuser, dan atribut.

`\ dv [S+] [POLA]`

Daftar tampilan. Termasuk skema, jenis, dan data pemilik. Ketika Anda menambahkan S+ ke perintah, misalnya `\ dv S+`, kolom metadata tambahan disertakan.

`\ H`

Menghidupkan output HTML. Ini berguna untuk mengembalikan hasil yang diformat dengan cepat. Misalnya, `select * from sales;` `\ H` mengembalikan hasil dari tabel penjualan, dalam HTML. Untuk beralih kembali ke hasil tabular, gunakan `\ q`, atau diam.

`\ saya`

Menjalankan perintah dari file. Misalnya, dengan asumsi Anda memiliki `rsql_steps.sql` di direktori kerja Anda, berikut ini menjalankan perintah dalam file: `\ i rsql_steps.sql`.

`\ I [+] [POLA]`

Daftar database. Termasuk pemilik, pengkodean, dan informasi tambahan.

`\ q`

Keluar, atau `\ q` perintah, log off sesi database dan keluar dari RSQL.

`\ sv [+] NAMA TAMPILAN`

Menunjukkan definisi tampilan.

`\ waktu`

Menunjukkan waktu berjalan, untuk kueri, misalnya.

`\ z [POLA]`

Output yang sama dengan `\ dp`.

\?

Menampilkan informasi bantuan. Parameter opsional menentukan item untuk menjelaskan.

\KELUAR

Log off semua sesi database dan keluar dari Amazon Redshift RSQL. Selain itu, Anda dapat menentukan kode keluar opsional. Misalnya, \EXIT 15 akan keluar dari terminal Amazon Redshift RSQL dan mengembalikan kode keluar 15.

Contoh berikut menunjukkan output dari koneksi dan keluar dari 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
```

\EKSPOR

Menentukan nama file ekspor yang RSQL gunakan untuk menyimpan informasi database yang dikembalikan oleh pernyataan SQL SELECT berikutnya.

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
```

Keluaran konsol

```
Rformat is off.  
Target width is 1500.  
Heading is set to: General Title  
Titledashes is on.  
(exported 40 rows)
```

\MASUK

Terhubung ke database. Anda dapat menentukan parameter koneksi menggunakan sintaks posisi atau sebagai string koneksi.

Sintaks perintah adalah sebagai berikut: `\logon {[DBNAME]- USERNAME|- HOST|- PORT|- [PASSWORD]] | conninfo}`

`DBNAME` ini adalah nama database untuk terhubung ke. `USERNAME` itu adalah nama pengguna untuk terhubung sebagai. `HOST` defaultnya adalah `localhost`. `PORT` defaultnya adalah `5439`.

Ketika nama host ditentukan dalam `\LOGON` perintah, itu menjadi nama host default untuk `\LOGON` perintah tambahan. Untuk mengubah nama host default, tentukan yang baru `HOST` dalam `\LOGON` perintah tambahan.

Contoh output dari `\LOGON` perintah untuk `user1` berikut.

```
(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=#
```

Output sampel untuk `pengguna2`.

```
(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=#
```

\ KOMENTAR

Perpanjangan `\echo` perintah. `\REMARK` mencetak string yang ditentukan ke aliran output. `\REMARK` meluas `\echo` dengan menambahkan kemampuan untuk memecah output melalui jalur terpisah.

Contoh berikut menunjukkan output dari perintah.

```
(testcluster) user1@dev=# \remark 'hello//world'
hello
world
```

\ RSET

Perintah `\rset` menetapkan parameter perintah dan variabel. `\rset` memiliki mode interaktif dan batch. `<arg>` itu tidak mendukung opsi sebagai opsi bash, seperti `-x`, atau argumen, misalnya `--`.

Ini menetapkan variabel, seperti berikut:

- TINGKAT KESALAHAN
- HEADING dan RTITLE
- RFORMAT
- MAXERROR
- TITLEDASHES
- LEBAR

Contoh berikut menentukan judul.

```
\rset heading "Winter Sales Report"
```

Untuk lebih banyak contoh cara menggunakan `\rset`, Anda dapat menemukan beberapa [Variabel Amazon Redshift RSQL](#) topik.

\ LARI

Menjalankan skrip Amazon Redshift RSQL yang terdapat dalam file yang ditentukan.

`\RUN` memperluas `\i` perintah dengan menambahkan opsi untuk melewati baris header dalam file.

Jika nama file menyertakan koma, titik koma, atau spasi, lampirkan dalam tanda kutip tunggal. Selain itu, jika teks mengikuti nama file, lampirkan dalam tanda kutip. Di UNIX, nama file peka huruf besar/kecil. Di Windows, nama file tidak peka huruf besar/kecil.

Contoh berikut menunjukkan output dari perintah.

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) as lineitem_cnt from lineitem;
select count(*) as customer_cnt from customer;
select count(*) as orders_cnt from orders;

(testcluster) user1@dev=# \run file=test.sql
  lineitem_cnt
-----
          4307207
(1 row)

  customer_cnt
-----
          37796166
(1 row)

  orders_cnt
-----
           0
(1 row)

(testcluster) user1@dev=# \run file=test.sql skip=2
2 records skipped in RUN file.
  orders_cnt
-----
           0
(1 row)
```

\OS

Sebuah alias untuk \! perintah. \OS menjalankan perintah sistem operasi yang diteruskan sebagai parameter. Kontrol kembali ke Amazon Redshift RSQL setelah perintah dijalankan. Misalnya, Anda dapat menjalankan perintah berikut untuk mencetak waktu tanggal sistem saat ini dan kembali ke terminal RSQL: `\os date`

```
(testcluster) user1@dev=# \os date
Tue Sep 7 20:47:54 UTC 2021
```

\GOTO

Perintah baru untuk Amazon Redshift RSQL. \GOTO melewati semua perintah intervensi dan melanjutkan pemrosesan pada yang ditentukan. \LABEL \LABEL harus menjadi referensi ke depan. Anda tidak dapat melompat ke \LABEL yang secara leksikal mendahului. \GOTO

Berikut menampilkan contoh output.

```
(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

Perintah baru untuk Amazon Redshift RSQL. \LABEL menetapkan titik masuk untuk menjalankan program, sebagai target untuk \GOTO perintah.

Berikut ini menunjukkan contoh output dari perintah.

```
(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 dan perintah terkait menjalankan bagian dari skrip input secara kondisional. Perpanjangan dari perintah PSQL `\if` (`\elif`, `\else`, `\endif`). \IF dan \ELSEIF mendukung ekspresi boolean termasuk AND, OR dan NOT kondisi.

Berikut ini menunjukkan contoh output dari perintah.

```

(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

```


Gunakan `ERRORCODE` dalam logika percabangan Anda.

```
\if :'ERRORCODE' = '00000'
  \remark 'The statement was executed without error'
\else
  \remark :LAST_ERROR_MESSAGE
\endif
```

Gunakan `\GOTO` dalam `\IF` blok untuk mengontrol bagaimana kode dijalankan.

Variabel Amazon Redshift RSQL

Beberapa kata kunci bertindak sebagai variabel dalam RSQL. Anda dapat mengatur masing-masing ke nilai tertentu, atau mengatur ulang nilainya. Sebagian besar diatur dengan `\rset`, yang memiliki mode interaktif dan mode batch. Perintah dapat didefinisikan dalam huruf kecil atau huruf besar.

ACTIVITYCOUNT

Menunjukkan jumlah baris yang dipengaruhi oleh permintaan terakhir yang dikirimkan. Untuk permintaan pengembalian data, ini adalah jumlah baris yang dikembalikan ke RSQL dari database. Nilai adalah 0 atau bilangan bulat positif. Nilai maksimum adalah 18.446.744.073.709.551.615.

Variabel `ACTIVITYCOUNT` yang diperlakukan secara khusus mirip dengan variabel `ROW_COUNT`. Namun, `ROW_COUNT` tidak melaporkan jumlah baris yang terpengaruh ke aplikasi klien pada penyelesaian perintah untuk `SELECT`, `COPY` atau `UNLOAD`. Tapi `ACTIVITYCOUNT` tidak.

activitycount_01.sql:

```
select viewname, schemaname
from pg_views
where schemaname = 'not_existing_schema';
\if :ACTIVITYCOUNT = 0
\remark 'views do not exist'
\endif
```

Keluaran konsol:

```
viewname | schemaname
-----+-----
(0 rows)
```

```
views do not exist
```

TINGKAT KESALAHAN

Menugaskan tingkat keparahan untuk kesalahan. Gunakan tingkat keparahan untuk menentukan tindakan. Jika `ERRORLEVEL` perintah belum digunakan, nilainya secara default `ON`.

`errorlevel_01.sql`:

```
\rset errorlevel 42P01 severity 0

select * from tbl;

select 1 as col;

\echo exit
\quit
```

Keluaran konsol:

```
Errorlevel is on.
rsql: ERROR: relation "tbl" does not exist
(1 row)

col
1

exit
```

HEADING dan RTITLE

Memungkinkan pengguna untuk menentukan header yang muncul di bagian atas laporan. Header yang ditentukan oleh `RSET RTITLE` perintah secara otomatis menyertakan tanggal sistem saat ini dari komputer klien.

konten `rset_heading_rtitle_02.rsq`:

```
\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...
```

Keluaran konsol:

```
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

Menentukan tingkat keparahan kesalahan maksimum di luar mana RSQL menghentikan pemrosesan pekerjaan. Kode pengembalian adalah nilai integer yang RSQL kembali ke sistem operasi klien setelah menyelesaikan setiap pekerjaan atau tugas. Nilai kode pengembalian menunjukkan status penyelesaian pekerjaan atau tugas. Jika skrip berisi pernyataan yang menghasilkan tingkat keparahan kesalahan lebih besar dari `maxerror` nilai yang ditentukan, RSQL segera keluar. Oleh karena itu, untuk memiliki RSQL keluar pada tingkat keparahan kesalahan 8, gunakan `RSET MAXERROR 7`

konten `maxerror_01.sql`:

```
\rset maxerror 0

select 1 as col;

\quit
```

Keluaran konsol:

```
Maxerror is default.
(1 row)

col
1
```

RFORMAT

Memungkinkan pengguna untuk menentukan apakah akan menerapkan pengaturan untuk perintah pemformatan.

konten rset_rformat.rsq:

```
\remark Starting...
\pset border 2
\pset format wrapped
\pset expanded on
\pset title 'Great Title'
select * from rsq_test.tbl_long where id = 500;
\rset rformat
select * from rsq_test.tbl_long where id = 500;
\rset rformat off
select * from rsq_test.tbl_long where id = 500;
\rset rformat on
select * from rsq_test.tbl_long where id = 500;
\exit
\remark Finishing...
```

Keluaran konsol:

```
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

Mendapat jumlah catatan yang dipengaruhi oleh kueri sebelumnya. Ini biasanya digunakan untuk memeriksa hasil, seperti dalam fragmen kode berikut:

```

SET result = ROW_COUNT;

IF result = 0

```

...

TITLEDASHES

Kontrol ini memungkinkan pengguna untuk menentukan apakah garis karakter dasbor akan dicetak di atas data kolom yang dikembalikan untuk pernyataan SQL.

Contoh:

```
\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;
```

Keluaran konsol:

```
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
```

LEBAR

Menetapkan format output untuk dibungkus dan menentukan lebar target untuk setiap baris dalam laporan. Tanpa parameter, ia mengembalikan pengaturan saat ini untuk format dan lebar target.

konten rset_width_01.rsq1:

```
\echo Starting...
\rset width
\rset width 50
\rset width
\quit
\echo Finishing...
```

Keluaran konsol:

```
Starting...
Target width is 75.
Target width is 50.
Target width is 50.
Press any key to continue . . .
```

Contoh dengan 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...
```

Keluaran konsol:

```
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 . . .
```

Kode kesalahan Amazon Redshift RSQL**Pesan sukses, peringatan, dan pengecualian:**

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
00000	Kelas 00 — Penyelesaian Berhasil	successful_completion
01000	Kelas 01 - Peringatan	memperingati
0100C	Kelas 01 - Peringatan	dynamic_result_sets_returned
01008	Kelas 01 - Peringatan	implicit_zero_bit_padding
01003	Kelas 01 - Peringatan	null_value_eliminated_in_set_function
01007	Kelas 01 - Peringatan	privilege_not_granted
01006	Kelas 01 - Peringatan	privilege_not_revoked
01004	Kelas 01 - Peringatan	string_data_right_truncation
01P01	Kelas 01 - Peringatan	deprecated_feature
02000	Kelas 02 - Tidak Ada Data	tidak data_data
02001	Kelas 02 - Tidak Ada Data	no_additional_dynamic_result_sets_returned
03000	Kelas 03 - Pernyataan SQL Belum Lengkap	sql_statement_not_yet_complete
08000	Kelas 08 - Pengecualian Koneksi	connection_exception
08003	Kelas 08 - Pengecualian Koneksi	connection_does_not_exist
08006	Kelas 08 - Pengecualian Koneksi	connection_failure
08001	Kelas 08 - Pengecualian Koneksi	sqlclient_unable_to_establish_sqlconnection

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
08004	Kelas 08 - Pengecualian Koneksi	sqlserver_rejected_establishment_of_sqlconnection
08007	Kelas 08 - Pengecualian Koneksi	transaction_resolution_unknown
08P01	Kelas 08 - Pengecualian Koneksi	protocol_violation
09000	Kelas 09 - Pengecualian Tindakan yang Dipicu	triggered_action_exception
0A000	Kelas 0A - Fitur Tidak Didukung	feature_not_supported
0A000	Kelas 0A - Fitur Tidak Didukung	feature_not_supported
0B000	Kelas 0B — Inisiasi Transaksi Tidak Valid	invalid_transaction_initiation
0F000	Kelas 0F - Pengecualian Pencari Lokasi	locator_exception
0F001	Kelas 0F - Pengecualian Pencari Lokasi	invalid_locator_specification
0L000	Kelas 0L - Pemberi Tidak Valid	invalid_grantor
0LP01	Kelas 0L - Pemberi Tidak Valid	invalid_grant_operation
0P000	Kelas 0P - Spesifikasi Peran Tidak Valid	invalid_role_specification

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
0Z000	Kelas 0Z - Pengecualian Diagnostik	diagnostics_exception
0Z002	Kelas 0Z - Pengecualian Diagnostik	stacked_diagnostics_accessed_without_active_handler
20000	Kelas 20 — Kasus Tidak Ditemukan	kasus_not_found
21000	Kelas 21 — Pelanggaran Kardinalitas	kardinalitas_pelanggaran

Pengecualian data:

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
22000	Kelas 22 - Pengecualian Data	data_exception
2202E	Kelas 22 - Pengecualian Data	array_subscript_error
22021	Kelas 22 - Pengecualian Data	character_not_in_repertoar
22008	Kelas 22 - Pengecualian Data	datetime_field_overflow
22012	Kelas 22 - Pengecualian Data	division_by_zero
22005	Kelas 01 - Peringatan	error_in_assignment
2200B	Kelas 01 - Peringatan	escape_character_conflict
22022	Kelas 01 - Peringatan	indicator_overflow
22015	Kelas 01 - Peringatan	interval_field_overflow
2201E	Kelas 01 - Peringatan	invalid_argument_for_logaritma

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
2201F	Kelas 01 - Peringatan	invalid_argument_for_power_function
2201G	Kelas 01 - Peringatan	invalid_argument_for_width_bucket_function
22018	Kelas 01 - Peringatan	invalid_character_value_for_cast
22007	Kelas 01 - Peringatan	format_invalid_datetime_
22019	Kelas 01 - Peringatan	invalid_escape_character
2200D	Kelas 01 - Peringatan	invalid_escape_octet
22025	Kelas 01 - Peringatan	invalid_escape_sequence
22P06	Kelas 01 - Peringatan	nonstandard_use_of_escape_character
22010	Kelas 01 - Peringatan	invalid_indicator_parameter_value
22023	Kelas 01 - Peringatan	invalid_parameter_value
2201B	Kelas 01 - Peringatan	invalid_regular_expression
22009	Kelas 01 - Peringatan	invalid_time_zone_displacement_value
2200C	Kelas 01 - Peringatan	invalid_use_of_escape_character
2200G	Kelas 01 - Peringatan	most_specific_type_mismatch
22004	Kelas 01 - Peringatan	null_value_not_allowed
22002	Kelas 01 - Peringatan	null_value_no_indicator_parameter
22003	Kelas 01 - Peringatan	numeric_value_out_of_range
22026	Kelas 01 - Peringatan	string_data_length_mismatch
22001	Kelas 01 - Peringatan	string_data_right_truncation
22011	Kelas 01 - Peringatan	substring_error

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
22027	Kelas 01 - Peringatan	trim_error
22024	Kelas 01 - Peringatan	unterminated_c_string
2200F	Kelas 01 - Peringatan	zero_length_character_string
22P01	Kelas 01 - Peringatan	floating_point_exception
22P02	Kelas 01 - Peringatan	invalid_text_representation
22P03	Kelas 01 - Peringatan	invalid_binary_representasi
22P04	Kelas 01 - Peringatan	bad_copy_file_format
22P05	Kelas 01 - Peringatan	untranslatable_character

Pelanggaran kendala integritas:

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
23000	Kelas 23 — Pelanggaran Kendala Integritas	integrity_constraint_violation
23001	Kelas 23 — Pelanggaran Kendala Integritas	restrict_violation
23502	Kelas 23 — Pelanggaran Kendala Integritas	not_null_violation
23503	Kelas 23 — Pelanggaran Kendala Integritas	foreign_key_violation
23505	Kelas 23 — Pelanggaran Kendala Integritas	unik_pelanggaran

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
23514	Kelas 23 — Pelanggaran Kendala Integritas	check_violation
24000	Kelas 24 - Status Kursor Tidak Valid	invalid_cursor_state
01004	Kelas 01 - Peringatan	string_data_right_truncation
25000	Kelas 25 - Status Transaksi Tidak Valid	invalid_transaction_state
25001	Kelas 25 - Status Transaksi Tidak Valid	active_sql_transaction
25002	Kelas 25 - Status Transaksi Tidak Valid	invalid_transaction_state
25008	Kelas 25 - Status Transaksi Tidak Valid	held_cursor_requires_same_isolation_level
25003	Kelas 25 - Status Transaksi Tidak Valid	tidak sesuai_access_mode_for_branch_transaction
25004	Kelas 25 - Status Transaksi Tidak Valid	tidak sesuai_isolation_level_for_branch_transaction
25005	Kelas 25 - Status Transaksi Tidak Valid	no_active_sql_transaction_for_branch_transaction
25006	Kelas 25 - Status Transaksi Tidak Valid	read_only_sql_transaction
25007	Kelas 25 - Status Transaksi Tidak Valid	no_active_sql_transaction_for_branch_transaction
25P01	Kelas 25 - Status Transaksi Tidak Valid	no_active_sql_transaction

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
25P02	Kelas 25 - Status Transaksi Tidak Valid	dalam_failed_sql_transaction
26000	Kelas 26 - Nama Pernyataan SQL Tidak Valid	invalid_sql_statement_name
28000	Kelas 28 - Spesifikasi Otorisasi Tidak Valid	invalid_authorization_specification
2B000	Kelas 2B - Deskriptor Hak Istimewa Dependen Masih Ada	dependent_privilege_descriptors_still_exist
2BP01	Kelas 2B - Deskriptor Hak Istimewa Dependen Masih Ada	dependent_objects_still_exist
2D000	Kelas 2D — Pengakhiran Transaksi Tidak Valid	invalid_transaction_termination
2F000	Kelas 2F - Pengecualian Rutin SQL	sql_routine_exception
2F005	Kelas 2F - Pengecualian Rutin SQL	function_executed_no_return_statement
2F002	Kelas 2F - Pengecualian Rutin SQL	modifying_sql_data_not_authorized
2F003	Kelas 2F - Pengecualian Rutin SQL	prohibited_sql_statement_trial
2F004	Kelas 2F - Pengecualian Rutin SQL	reading_sql_data_not_permitted

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
34000	Kelas 34 - Nama Kursor Tidak Valid	invalid_cursor_name
38000	Kelas 38 - Pengecualian Rutin Eksternal	external_routine_exception
38001	Kelas 38 - Pengecualian Rutin Eksternal	containing_sql_not_permitted
38002	Kelas 38 - Pengecualian Rutin Eksternal	modifying_sql_data_not_authorized
38003	Kelas 38 - Pengecualian Rutin Eksternal	prohibited_sql_statement_trial
38004	Kelas 38 - Pengecualian Rutin Eksternal	reading_sql_data_not_permitted
39000	Kelas 39 - Pengecualian Doa Rutin Eksternal	external_routine_invocation_exception
39001	Kelas 39 - Pengecualian Doa Rutin Eksternal	invalid_sqlstate_returned
39004	Kelas 39 - Pengecualian Doa Rutin Eksternal	null_value_not_allowed
39P01	Kelas 39 - Pengecualian Doa Rutin Eksternal	trigger_protocol_dilanggar
39P02	Kelas 39 - Pengecualian Doa Rutin Eksternal	srf_protocol_dilanggar
3D000	Kelas 3D - Nama Katalog Tidak Valid	invalid_catalog_name

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
3F000	Kelas 3F - Nama Skema Tidak Valid	invalid_schema_name
42000	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	syntax_error_or_access_rule_violation
42601	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	syntax_error
42501	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	insufficient_privilege
42846	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	cannot_coerce
42803	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	grouping_error
42830	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	invalid_foreign_key
42602	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	invalid_name
42622	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	name_too_long

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
42939	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	reserved_name
42804	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	datatype_mismatch
42P18	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	indeterminate_datatype
42809	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	wrong_object_type
42703	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	undefined_column
42883	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	undefined_function
42P01	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	undefined_table
42P02	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	undefined_parameter
42704	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	undefined_object

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
42701	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	duplikat_kolom
42P03	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	duplikat_kursor
42P04	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	duplikate_database
42723	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	duplikate_function
42P05	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	duplikate_prepared_statement
42P06	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	duplikate_skema
42P07	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	duplikate_table
42712	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	duplikate_alias
42710	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	duplikate_objek

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
42702	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	<code>ambiguous_column</code>
42725	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	<code>ambiguous_function</code>
42P08	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	<code>ambigu_parameter</code>
42P09	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	<code>ambigu_alias</code>
42P10	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	<code>invalid_column_reference</code>
42611	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	<code>invalid_column_definition</code>
42P11	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	<code>invalid_cursor_definition</code>
42P12	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	<code>invalid_database_definition</code>
42P13	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	<code>invalid_function_definition</code>

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
42P14	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	invalid_prepared_statement_definition
42P15	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	invalid_schema_definition
42P16	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	invalid_table_definition
42P17	Kelas 42 — Kesalahan Sintaks atau Pelanggaran Aturan Akses	invalid_object_definition
44000	Kelas 44 — DENGAN CEK OPTION Pelanggaran	dengan_check_option_violation
53000	Kelas 53 - Sumber Daya Tidak Cukup	insufficient_resources
53100	Kelas 53 - Sumber Daya Tidak Cukup	disk_penuh
53200	Kelas 53 - Sumber Daya Tidak Cukup	keluar_of_memori
53300	Kelas 53 - Sumber Daya Tidak Cukup	too_many_connections
54000	Kelas 54 — Batas Program Terlampaui	program_limit_exceeded
54001	Kelas 54 — Batas Program Terlampaui	statement_too_complex

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
54011	Kelas 54 — Batas Program Terlampaui	too_many_columns
54023	Kelas 54 — Batas Program Terlampaui	too_many_argument
55000	Kelas 55 — Objek Tidak Dalam Keadaan Prasyarat	object_not_in_prerequisite_state
55006	Kelas 55 — Objek Tidak Dalam Keadaan Prasyarat	object_in_use
55P02	Kelas 55 — Objek Tidak Dalam Keadaan Prasyarat	cant_change_runtime_param
55P03	Kelas 55 — Objek Tidak Dalam Keadaan Prasyarat	lock_not_available
57000	Kelas 57 — Intervensi Operator	operator_intervensi
57014	Kelas 57 — Intervensi Operator	query_canceled
57P01	Kelas 57 — Intervensi Operator	admin_shutdown
57P02	Kelas 57 — Intervensi Operator	crash_shutdown
57P03	Kelas 57 — Intervensi Operator	cannot_connect_now
58000	Kelas 58 - Kesalahan Sistem (kesalahan eksternal ke PostgreSQL)	system_error

Kode Kesalahan	Kelas Kesalahan	Nama Kondisi
58030	Kelas 58 - Kesalahan Sistem (kesalahan eksternal ke PostgreSQL)	io_error
58P01	Kelas 58 - Kesalahan Sistem (kesalahan eksternal ke PostgreSQL)	undefined_file
58P02	Kelas 58 - Kesalahan Sistem (kesalahan eksternal ke PostgreSQL)	duplikat_file
F0000	Kelas F0 - Kesalahan File Konfigurasi	duplikat_file
F0001	Kelas F0 - Kesalahan File Konfigurasi	lock_file_exists
P0000	Kelas P0 - Kesalahan PL/PGSQL	plpgsql_error
P0001	Kelas P0 - Kesalahan PL/PGSQL	raise_exception
P0002	Kelas P0 - Kesalahan PL/PGSQL	no_data_found
P0003	Kelas P0 - Kesalahan PL/PGSQL	too_many_rows
XX000	Kelas XX - Kesalahan Internal	internal_error
XX001	Kelas XX - Kesalahan Internal	data_rusak
XX002	Kelas XX - Kesalahan Internal	index_rusak

Variabel lingkungan Amazon Redshift RSQL

Amazon Redshift RSQL dapat menggunakan variabel lingkungan untuk memilih nilai parameter default.

RSPASSWORD

Important

Kami tidak menyarankan menggunakan variabel lingkungan ini untuk alasan keamanan, karena beberapa sistem operasi memungkinkan pengguna non-administratif untuk melihat variabel lingkungan proses.

Menetapkan kata sandi untuk Amazon Redshift RSQL untuk digunakan saat menghubungkan ke Amazon Redshift. Variabel lingkungan ini memerlukan Amazon Redshift RSQL 1.0.4 ke atas.

RSQL memprioritaskan RSPASSWORD jika satu diatur. Jika RSPASSWORD tidak disetel dan Anda terhubung menggunakan DSN, RSQL mengambil kata sandi dari parameter file DSN. Akhirnya, jika RSPASSWORD tidak diatur dan Anda tidak menggunakan DSN, RSQL menyediakan prompt kata sandi setelah mencoba untuk terhubung.

Berikut ini adalah contoh pengaturan RSPASSWORD:

```
export RSPASSWORD=TestPassw0rd
```

Menghubungkan dengan SQL Workbench/J

Anda dapat terhubung ke database menggunakan SQL Workbench/J, alat kueri SQL lintas platform bebas DBMS gratis.

Amazon Redshift tidak menyediakan atau menginstal alat atau pustaka klien SQL pihak ketiga apa pun, jadi Anda harus menginstal apa pun yang ingin Anda gunakan dengan database Anda. [Untuk menginstal SQL Workbench/J, ikuti petunjuk dalam dokumentasi SQL Workbench/J \(SQL Workbench/J\)](#). Secara umum, untuk menggunakan SQL Workbench/J, Anda melakukan hal berikut:

- Tinjau Lisensi perangkat lunak SQL Workbench/J.
- Unduh paket SQL Workbench/J yang sesuai untuk sistem operasi Anda di komputer klien atau instans Amazon EC2.
- Instal SQL Workbench/J pada sistem Anda.

Memiliki Java Runtime Environment (JRE) diinstal pada sistem Anda. Pastikan Anda menggunakan versi JRE yang benar yang dibutuhkan oleh klien SQL Workbench/J.

- Connect ke database Anda melalui koneksi JDBC di SQL Workbench/J.

Pastikan komputer klien atau instans Amazon EC2 Anda memiliki driver Amazon Redshift JDBC yang direkomendasikan. Untuk tautan untuk mengunduh driver terbaru, lihat [Unduh driver Amazon Redshift JDBC, versi 2.1](#). Juga, pastikan Anda telah mengkonfigurasi pengaturan firewall untuk memungkinkan akses ke database Anda. Untuk informasi selengkapnya, lihat [Langkah 4: Mengotorisasi akses ke cluster di Panduan Memulai Amazon Redshift](#).

- Buat profil koneksi baru di SQL Workbench/J yang menggunakan driver Amazon Redshift.

Connect ke gudang data Anda secara terprogram

Untuk informasi tentang alat untuk membangun aplikasi agar tersambung ke gudang data Anda, lihat [Alat untuk Dibangun AWS](#).

Menggunakan profil otentikasi untuk terhubung ke Amazon Redshift

Jika Anda memiliki banyak koneksi ke Amazon Redshift, mungkin sulit untuk mengelola pengaturan untuk semuanya. Seringkali, setiap koneksi JDBC atau ODBC menggunakan opsi konfigurasi tertentu. Dengan menggunakan profil otentikasi, Anda dapat menyimpan opsi koneksi bersama-sama. Dengan cara ini, pengguna Anda dapat memilih profil untuk terhubung dan menghindari pengaturan pengaturan untuk opsi individual. Profil dapat diterapkan ke berbagai skenario dan jenis pengguna.

Setelah Anda membuat profil otentikasi, pengguna dapat menambahkan ready-to-use profil ke string koneksi. Dengan melakukan ini, mereka dapat terhubung ke Amazon Redshift dengan pengaturan yang tepat untuk setiap peran dan kasus penggunaan.

[Untuk informasi Amazon Redshift API, lihat CreateAuthentication Profil.](#)

Membuat profil otentikasi

Menggunakan AWS CLI, Anda membuat profil otentikasi dengan `create-authentication-profile` perintah. Ini mengasumsikan bahwa Anda memiliki cluster Amazon Redshift yang ada dan database yang ada. Kredensial Anda harus memiliki izin untuk terhubung ke database Amazon Redshift dan hak untuk mengambil profil otentikasi. Anda memberikan opsi konfigurasi sebagai string JSON, atau referensi file yang berisi string JSON Anda.


```
create-authentication-profile --authentication-profile-name<value: String> --
authentication-profile-content<value: String>
```

Contoh berikut membuat profil yang disebut `ExampleProfileName`. Di sini, Anda dapat menambahkan kunci dan nilai yang menentukan nama cluster Anda dan pengaturan opsi lainnya, sebagai string JSON.

```
create-authentication-profile --authentication-profile-name "ExampleProfileName"
--authentication-profile-content "{\"AllowDBUserOverride\": \"1\", \"Client_ID\
\": \"ExampleClientID\", \"App_ID\": \"ExampleAppID\", \"AutoCreate\": false,
\"enableFetchRingBuffer\": true, \"databaseMetadataCurrentDbOnly\": true}"
}
```

Perintah ini membuat profil dengan pengaturan JSON yang ditentukan. Berikut ini dikembalikan, yang menunjukkan bahwa profil dibuat.

```
{"AuthenticationProfileName": "ExampleProfileName",
"AuthenticationProfileContent": "{\"AllowDBUserOverride\": \"1\",
\"Client_ID\": \"ExampleClientID\", \"App_ID\": \"ExampleAppID\",
\"AutoCreate\": false, \"enableFetchRingBuffer\": true,
\"databaseMetadataCurrentDbOnly\": true}" }
```

Batasan dan kuota untuk membuat profil otentikasi

Setiap pelanggan memiliki kuota sepuluh (10) profil otentikasi.

Kesalahan tertentu dapat terjadi dengan profil otentikasi. Contohnya adalah jika Anda membuat profil baru dengan nama yang sudah ada, atau jika Anda melebihi kuota profil Anda. Untuk informasi selengkapnya, lihat [CreateAuthenticationProfil](#).

Anda tidak dapat menyimpan kunci dan nilai opsi tertentu untuk string koneksi JDBC, ODBC, dan Python di toko profil otentikasi:

- AccessKeyID
- access_key_id
- SecretAccessKey
- secret_access_key_id
- PWD
- Password

- password

Anda tidak dapat menyimpan kunci atau nilai AuthProfile di toko profil, untuk string koneksi JDBC atau ODBC. Untuk koneksi Python, Anda tidak dapat menyimpan. auth_profile

Profil otentikasi disimpan di Amazon DynamoDB dan dikelola oleh. AWS

Bekerja dengan profil otentikasi

Setelah Anda membuat profil otentikasi, Anda dapat menyertakan nama profil sebagai opsi koneksi untuk JDBC versi 2.0. AuthProfile Menggunakan opsi koneksi ini mengambil pengaturan yang disimpan.

```
jdbc:redshift:iam://endpoint:port/database?AuthProfile=<Profile-Name>&AccessKeyId=<Caller-Access-Key>&SecretAccessKey=<Caller-Secret-Key>
```

Berikut ini adalah contoh string URL JDBC.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?AuthProfile="ExampleProfile"&AccessKeyId="AKIAIOSFODNN7EXAMPLE"&SecretAccessKey="wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY"
```

Tentukan AccessKeyId dan SecretAccessKey di URL JDBC, bersama dengan nama profil otentikasi.

Anda juga dapat memisahkan opsi konfigurasi dengan pembatas titik koma, seperti pada contoh berikut, yang mencakup opsi untuk logging.

```
jdbc:redshift:iam://my_redshift_end_point:5439/dev?LogLevel=6;LogPath=/tmp;AuthProfile=my_profile;AccessKeyId="AKIAIOSFODNN7EXAMPLE";SecretAccessKey="wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY"
```

Note

Jangan menambahkan informasi rahasia ke profil otentikasi. Misalnya, jangan menyimpan SecretAccessKey nilai AccessKeyId atau dalam profil otentikasi. Toko profil otentikasi memiliki aturan untuk melarang penyimpanan kunci rahasia. Anda mendapatkan kesalahan jika Anda mencoba menyimpan kunci dan nilai yang terkait dengan informasi sensitif.

Mendapatkan profil otentikasi

Untuk membuat daftar profil otentikasi yang ada, hubungi perintah berikut.

```
describe-authentication-profiles --authentication-profile-name <value: String>
```

Contoh berikut menunjukkan dua profil diambil. Semua profil dikembalikan jika Anda tidak menentukan nama profil.

```
{ "AuthenticationProfiles": [ { "AuthenticationProfileName":  
"testProfile1", "AuthenticationProfileContent": "{\\"AllowDBUserOverride  
\":\\"1\\",\\"Client_ID\\":\\"ExampleClientID\\",\\"App_ID\\":\\"ExampleAppID  
\",\\"AutoCreate\\":false,\\"enableFetchRingBuffer\\":true,  
\\"databaseMetadataCurrentDbOnly\\":true}" }, { "AuthenticationProfileName":  
"testProfile2", "AuthenticationProfileContent": "{\\"AllowDBUserOverride  
\":\\"1\\",\\"Client_ID\\":\\"ExampleClientID\\",\\"App_ID\\":\\"ExampleAppID  
\",\\"AutoCreate\\":false,\\"enableFetchRingBuffer\\":true,  
\\"databaseMetadataCurrentDbOnly\\":true}" } ] }
```

Memecahkan masalah koneksi di Amazon Redshift

Jika Anda memiliki masalah dengan menghubungkan ke cluster Anda dari alat klien SQL, ada beberapa hal yang dapat Anda periksa untuk mempersempit masalah. Jika Anda menggunakan sertifikat SSL atau server, pertama-tama hapus kompleksitas ini saat Anda memecahkan masalah koneksi. Kemudian tambahkan ini kembali ketika Anda telah menemukan solusi. Untuk informasi selengkapnya, lihat [Mengkonfigurasi opsi keamanan untuk koneksi](#).

Important

Amazon Redshift telah mengubah cara sertifikat SSL dikelola. Jika Anda mengalami masalah saat menghubungkan menggunakan SSL, Anda mungkin perlu memperbarui sertifikat CA root kepercayaan Anda saat ini. Untuk informasi selengkapnya, lihat [Transisi ke sertifikat ACM untuk koneksi SSL](#).

Bagian berikut memiliki beberapa contoh pesan kesalahan dan kemungkinan solusi untuk masalah koneksi. Karena alat klien SQL yang berbeda menyediakan pesan kesalahan yang berbeda, ini bukan daftar lengkap, tetapi harus menjadi titik awal yang baik untuk memecahkan masalah.

Topik

- [Menghubungkan dari luar Amazon EC2—masalah batas waktu Firewall](#)
- [Koneksi ditolak atau gagal](#)
- [Klien dan driver tidak kompatibel](#)
- [Kueri tampaknya hang dan terkadang gagal mencapai cluster](#)
- [Mengatur parameter ukuran pengambilan JDBC](#)

Menghubungkan dari luar Amazon EC2—masalah batas waktu Firewall

Contoh masalah

Koneksi klien Anda ke database tampak hang atau batas waktu saat menjalankan kueri panjang, seperti perintah COPY. Dalam kasus ini, Anda mungkin mengamati bahwa konsol Amazon Redshift menampilkan bahwa kueri telah selesai, tetapi alat klien itu sendiri tampaknya masih menjalankan kueri. Hasil kueri mungkin hilang atau tidak lengkap tergantung kapan koneksi berhenti.

Solusi yang mungkin

Masalah ini terjadi saat Anda terhubung ke Amazon Redshift dari mesin selain instans Amazon EC2. Dalam hal ini, koneksi idle diakhiri oleh komponen jaringan perantara, seperti firewall, setelah periode tidak aktif. Perilaku ini khas ketika Anda masuk dari jaringan pribadi virtual (VPN) atau jaringan lokal Anda.

Untuk menghindari batas waktu ini, kami merekomendasikan perubahan berikut:

- Tingkatkan nilai sistem klien yang berhubungan dengan batas waktu TCP/IP. Buat perubahan ini di komputer yang Anda gunakan untuk terhubung ke cluster Anda. Periode batas waktu harus disesuaikan untuk klien dan jaringan Anda. Untuk informasi selengkapnya, lihat [Ubah pengaturan batas waktu TCP/IP](#).
- Secara opsional, atur perilaku keepalive di tingkat DSN. Untuk informasi selengkapnya, lihat [Ubah pengaturan batas waktu DSN](#).

Ubah pengaturan batas waktu TCP/IP

Untuk mengubah pengaturan batas waktu TCP/IP, konfigurasi pengaturan batas waktu sesuai dengan sistem operasi yang Anda gunakan untuk terhubung ke cluster Anda.

- Linux — Jika klien Anda berjalan di Linux, jalankan perintah berikut sebagai pengguna root untuk mengubah pengaturan batas waktu untuk sesi saat ini:

```
/sbin/sysctl -w net.ipv4.tcp_keepalive_time=200 net.ipv4.tcp_keepalive_intvl=200
net.ipv4.tcp_keepalive_probes=5
```

Untuk mempertahankan pengaturan, membuat atau memodifikasi file `/etc/sysctl.conf` dengan nilai-nilai berikut kemudian reboot sistem Anda.

```
net.ipv4.tcp_keepalive_time=200
net.ipv4.tcp_keepalive_intvl=200
net.ipv4.tcp_keepalive_probes=5
```

- Windows — Jika klien Anda berjalan pada Windows, edit nilai untuk pengaturan registri berikut di bawah `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\Tcpip\Parameters\`:
 - KeepAliveWaktu: 30000
 - KeepAliveInterval: 1000
 - TcpMaxDataRetransmissions: 10

Pengaturan ini menggunakan tipe data `DWORD`. Jika tidak ada di bawah jalur registri, Anda dapat membuat pengaturan dan menentukan nilai yang disarankan ini. Untuk informasi lebih lanjut tentang mengedit registri Windows, lihat dokumentasi Windows.

Setelah Anda menetapkan nilai-nilai ini, restart komputer Anda agar perubahan diterapkan.

- Mac - Jika klien Anda berjalan di Mac, jalankan perintah berikut untuk mengubah pengaturan batas waktu untuk sesi saat ini:

```
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
```

Untuk mempertahankan pengaturan, membuat atau memodifikasi file `/etc/sysctl.conf` dengan nilai-nilai berikut:

```
net.inet.tcp.keepidle=200000
net.inet.tcp.keepintvl=200000
net.inet.tcp.keepinit=200000
net.inet.tcp.always_keepalive=1
```

Nyalakan kembali komputer Anda, lalu jalankan perintah berikut untuk memverifikasi bahwa nilainya ditetapkan.

```
sysctl net.inet.tcp.keepidle
sysctl net.inet.tcp.keepintvl
sysctl net.inet.tcp.keepinit
sysctl net.inet.tcp.always_keepalive
```

Ubah pengaturan batas waktu DSN

Anda dapat mengatur perilaku keepalive di tingkat DSN jika Anda mau. Anda melakukan ini dengan menambahkan atau memodifikasi parameter berikut dalam file `odbc.ini`:

KeepAlivesHitung

Jumlah paket TCP keepalive yang dapat hilang sebelum koneksi dianggap rusak.

KeepAlivesMenganggur

Jumlah detik tidak aktif sebelum driver mengirim paket TCP keepalive.

KeepAlivesInterval

Jumlah detik antara setiap transmisi ulang TCP keepalive.

Pada Windows, Anda memodifikasi parameter ini di registri dengan menambahkan atau mengubah kunci di `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\Your_DSN`. Di Linux dan macOS, Anda menambahkan atau memodifikasi parameter ini di entri DSN target langsung di file `odbc.ini`. Untuk informasi selengkapnya tentang memodifikasi file `odbc.ini` di komputer Linux dan macOS, lihat [Gunakan pengelola driver ODBC untuk mengonfigurasi driver di sistem operasi Linux dan macOS X](#)

Jika parameter ini tidak ada, atau jika mereka memiliki nilai 0, sistem menggunakan parameter keepalive yang ditentukan untuk TCP/IP untuk menentukan perilaku DSN keepalive. Di Windows,

Anda dapat menemukan parameter TCP/IP di registri di. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ Di Linux dan macOS, Anda dapat menemukan parameter TCP/IP dapat ditemukan di file sysctl.conf.

Koneksi ditolak atau gagal

Contoh kesalahan

- “Gagal membuat koneksi ke<endpoint>.”
- “Tidak dapat terhubung ke server: Waktu koneksi habis. *Apakah server berjalan pada host '' dan menerima koneksi TCP/IP pada port ''?* <endpoint><port>
- “Koneksi ditolak. Periksa apakah nama host dan port sudah benar dan bahwa postmaster menerima koneksi TCP/IP.

Solusi yang mungkin

Umumnya, ketika Anda menerima pesan kesalahan yang menunjukkan bahwa ada kegagalan untuk membuat koneksi, itu adalah masalah dengan izin untuk mengakses cluster atau dengan lalu lintas jaringan yang mencapai cluster.

Untuk terhubung ke klaster dari alat klien di luar jaringan tempat klaster berada, Anda menambahkan aturan masuk ke grup keamanan klaster. Konfigurasi aturan tergantung pada apakah cluster Amazon Redshift dibuat di cloud pribadi virtual (VPC):

- Jika Anda membuat klaster Amazon Redshift di cloud pribadi virtual (VPC) berdasarkan Amazon VPC, tambahkan aturan masuk ke grup keamanan VPC yang menentukan alamat CIDR/IP klien, di Amazon VPC. Untuk informasi selengkapnya tentang mengonfigurasi grup keamanan VPC untuk klaster dan opsi yang dapat diakses publik, lihat. [Mengelola cluster dalam VPC](#)
- Jika Anda membuat klaster Amazon Redshift di luar VPC, tambahkan alamat CIDR/IP klien Anda ke grup keamanan klaster di Amazon Redshift. Untuk informasi selengkapnya tentang mengonfigurasi grup keamanan klaster, lihat [Grup keamanan klaster Amazon Redshift](#).

Jika Anda mencoba menyambung ke klaster dari alat klien yang berjalan pada instans Amazon EC2, Anda juga menambahkan aturan masuk. Dalam hal ini, tambahkan aturan ke grup keamanan cluster. Aturan harus menentukan grup keamanan Amazon EC2 yang terkait dengan instans Amazon EC2 alat klien.

Dalam beberapa kasus, Anda mungkin memiliki lapisan antara klien dan server Anda, seperti firewall. Dalam kasus ini, pastikan firewall menerima koneksi masuk melalui port yang Anda konfigurasi untuk cluster Anda.

Klien dan driver tidak kompatibel

Contoh kesalahan

“DSN yang ditentukan berisi ketidakcocokan arsitektur antara Driver dan Aplikasi.”

Solusi yang mungkin

Ketika Anda mencoba untuk menghubungkan dan mendapatkan kesalahan tentang ketidakcocokan arsitektur, ini berarti bahwa alat klien dan driver tidak kompatibel. Ini terjadi karena arsitektur sistem mereka tidak cocok. Misalnya, ini dapat terjadi jika Anda memiliki alat klien 32-bit tetapi telah menginstal versi 64-bit driver. Terkadang alat klien 64-bit dapat menggunakan driver 32-bit, tetapi Anda tidak dapat menggunakan aplikasi 32-bit dengan driver 64-bit. Pastikan driver dan alat klien menggunakan versi arsitektur sistem yang sama.

Kueri tampaknya hang dan terkadang gagal mencapai cluster

Contoh masalah

Anda mengalami masalah dengan penyelesaian kueri, di mana kueri tampaknya berjalan tetapi hang di alat klien SQL. Terkadang kueri gagal muncul di cluster, seperti di tabel sistem atau konsol Amazon Redshift.

Solusi yang mungkin

Masalah ini dapat terjadi karena paket drop. Dalam hal ini, ada perbedaan ukuran unit transmisi maksimum (MTU) di jalur jaringan antara dua host Internet Protocol (IP). Ukuran MTU menentukan ukuran maksimum, dalam byte, dari paket yang dapat ditransfer dalam satu bingkai Ethernet melalui koneksi jaringan. Pada tahun AWS, beberapa jenis instans Amazon EC2 mendukung MTU 1500 (frame Ethernet v2) dan jenis instans lainnya mendukung MTU 9001 (bingkai jumbo TCP/IP).

Untuk menghindari masalah yang dapat terjadi dengan perbedaan ukuran MTU, sebaiknya lakukan salah satu hal berikut:

- Jika klaster Anda menggunakan platform EC2-VPC, konfigurasi grup keamanan Amazon VPC dengan aturan Internet Control Message Protocol (ICMP) kustom masuk yang muncul. `Destination Unreachable` Aturan dengan demikian menginstruksikan host asal untuk menggunakan ukuran MTU terendah di sepanjang jalur jaringan. Untuk detail tentang pendekatan

ini, lihat [Mengkonfigurasi grup keamanan untuk memungkinkan ICMP “tujuan tidak dapat dijangkau”](#).

- Jika cluster Anda menggunakan platform EC2-Classic, atau Anda tidak dapat mengizinkan aturan masuk ICMP, nonaktifkan bingkai jumbo TCP/IP sehingga frame Ethernet v2 digunakan. Untuk detail tentang pendekatan ini, lihat [Mengkonfigurasi MTU dari sebuah instans](#).

Mengkonfigurasi grup keamanan untuk memungkinkan ICMP “tujuan tidak dapat dijangkau”

Ketika ada perbedaan ukuran MTU di jaringan antara dua host, pertama-tama pastikan bahwa pengaturan jaringan Anda tidak memblokir jalur penemuan MTU (PMTUD). PMTUD memungkinkan host penerima untuk menanggapi host asal dengan pesan ICMP berikut: Destination Unreachable: fragmentation needed and DF set (ICMP Type 3, Code 4) Pesan ini menginstruksikan host asal untuk menggunakan ukuran MTU terendah di sepanjang jalur jaringan untuk mengirim ulang permintaan. Tanpa negosiasi ini, paket drop dapat terjadi karena permintaan terlalu besar untuk diterima oleh host penerima. Untuk informasi lebih lanjut tentang pesan ICMP ini, kunjungi [RFC792](#) di situs web Internet Engineering Task Force (IETF).

Jika Anda tidak secara eksplisit mengonfigurasi aturan masuk ICMP ini untuk grup keamanan VPC Amazon Anda, PMTUD diblokir. Dalam AWS, grup keamanan adalah firewall virtual yang menentukan aturan untuk lalu lintas masuk dan keluar ke suatu instans. Untuk informasi tentang grup keamanan klaster Amazon Redshift, lihat [Grup keamanan klaster Amazon Redshift](#) Untuk cluster yang menggunakan platform EC2-VPC, Amazon Redshift menggunakan grup keamanan VPC untuk mengizinkan atau menolak lalu lintas ke cluster. Secara default, grup keamanan dikunci dan menolak semua lalu lintas masuk. Untuk informasi tentang cara menyetel aturan masuk dan keluar untuk instans EC2-Classic atau EC2-VPC, lihat Perbedaan [antara instans di EC2-Classic dan VPC di Panduan Pengguna Amazon EC2](#).

Untuk informasi selengkapnya tentang cara menambahkan aturan ke grup keamanan VPC, lihat [Mengelola grup keamanan VPC untuk sebuah cluster](#) Untuk informasi selengkapnya tentang setelan PMTUD tertentu yang diperlukan dalam aturan ini, lihat [Penemuan Path MTU di Panduan Pengguna Amazon EC2](#).

Mengkonfigurasi MTU dari sebuah instans

Dalam beberapa kasus, klaster Anda mungkin menggunakan platform EC2-Classic atau Anda tidak dapat mengizinkan aturan ICMP khusus untuk lalu lintas masuk. Dalam kasus ini, kami menyarankan Anda menyesuaikan MTU ke 1500 pada antarmuka jaringan (NIC) dari instans EC2 yang Anda sambungkan ke cluster Amazon Redshift Anda. Penyesuaian ini menonaktifkan bingkai jumbo TCP/

IP untuk memastikan bahwa koneksi secara konsisten menggunakan ukuran paket yang sama. Namun, opsi ini mengurangi throughput jaringan maksimum untuk instans sepenuhnya, tidak hanya untuk koneksi ke Amazon Redshift. Untuk informasi selengkapnya, lihat prosedur berikut ini.

Untuk mengatur MTU pada sistem operasi Microsoft Windows

Jika klien Anda berjalan di sistem operasi Microsoft Windows, Anda dapat meninjau dan mengatur nilai MTU untuk adaptor Ethernet dengan menggunakan perintah `netsh`

1. Jalankan perintah berikut untuk menentukan nilai MTU saat ini:

```
netsh interface ipv4 show subinterfaces
```

2. Tinjau MTU nilai Ethernet adaptor dalam output.
3. Jika nilainya tidak 1500, jalankan perintah berikut untuk mengaturnya:

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500 store=persistent
```

Setelah Anda menetapkan nilai ini, restart komputer Anda agar perubahan diterapkan.

Untuk mengatur MTU pada sistem operasi Linux

Jika klien Anda berjalan di sistem operasi Linux, Anda dapat meninjau dan mengatur nilai MTU dengan menggunakan `ip` perintah.

1. Jalankan perintah berikut untuk menentukan nilai MTU saat ini:

```
$ ip link show eth0
```

2. Tinjau nilai berikut mtu dalam output.
3. Jika nilainya tidak 1500, jalankan perintah berikut untuk mengaturnya:

```
$ sudo ip link set dev eth0 mtu 1500
```

Untuk mengatur MTU pada sistem operasi Mac

- Ikuti petunjuk tentang situs dukungan macOS. [How to change the MTU for troubleshooting purposes](#) Untuk informasi lebih lanjut, cari [situs dukungan](#).

Mengatur parameter ukuran pengambilan JDBC

Secara default, driver JDBC mengumpulkan semua hasil untuk kueri pada satu waktu. Akibatnya, ketika Anda mencoba untuk mengambil hasil besar yang disetel melalui koneksi JDBC, Anda mungkin mengalami kesalahan sisi klien. out-of-memory Untuk memungkinkan klien Anda mengambil set hasil dalam batch, bukan dalam satu all-or-nothing pengambilan, setel parameter ukuran pengambilan JDBC di aplikasi klien Anda.

Note

Ukuran pengambilan tidak didukung untuk ODBC.

Untuk kinerja terbaik, atur ukuran pengambilan ke nilai tertinggi yang tidak menyebabkan kesalahan memori. Nilai ukuran pengambilan yang lebih rendah menghasilkan lebih banyak perjalanan server, yang memperpanjang waktu eksekusi. Server menyimpan sumber daya, termasuk slot kueri WLM dan memori terkait, hingga klien mengambil seluruh kumpulan hasil atau kueri dibatalkan. Saat Anda menyetel ukuran pengambilan dengan tepat, sumber daya tersebut dirilis lebih cepat, membuatnya tersedia untuk kueri lain.

Note

Jika Anda perlu mengekstrak kumpulan data besar, sebaiknya gunakan pernyataan [UNLOAD](#) untuk mentransfer data ke Amazon S3. Saat Anda menggunakan UNLOAD, node komputasi bekerja secara paralel untuk mempercepat transfer data.

Untuk informasi selengkapnya tentang pengaturan parameter ukuran pengambilan JDBC, buka [Mendapatkan hasil berdasarkan kursor dalam dokumentasi PostgreSQL](#).

Menggunakan API Data Amazon Redshift

Anda dapat mengakses database Amazon Redshift menggunakan API Data Amazon Redshift bawaan. Dengan menggunakan API ini, Anda dapat mengakses data Amazon Redshift dengan aplikasi berbasis layanan web, termasuk, notebook AWS Lambda Amazon, dan SageMaker AWS Cloud9 Untuk informasi lebih lanjut tentang aplikasi ini, lihat [AWS Lambda](#), [Amazon SageMaker](#), dan [AWS Cloud9](#).

Data API tidak memerlukan koneksi persisten ke database Anda. Sebagai gantinya, ia menyediakan titik akhir HTTP yang aman dan integrasi dengan AWS SDK. Anda dapat menggunakan titik akhir untuk menjalankan pernyataan SQL tanpa mengelola koneksi. Panggilan ke API Data bersifat asinkron.

Data API menggunakan kredensial yang disimpan dalam AWS Secrets Manager atau kredensial database sementara. Anda tidak perlu meneruskan kata sandi dalam panggilan API dengan salah satu metode otorisasi. Untuk informasi lebih lanjut tentang AWS Secrets Manager, lihat [Apa itu AWS Secrets Manager?](#) dalam AWS Secrets Manager User Guide.

Untuk informasi selengkapnya tentang operasi Data API, lihat Referensi [API Data Amazon Redshift](#).

Bekerja dengan Amazon Redshift Data API

Sebelum Anda menggunakan Amazon Redshift Data API, tinjau langkah-langkah berikut:

1. Tentukan apakah Anda, sebagai pemanggil API Data, diotorisasi. Untuk informasi selengkapnya tentang otorisasi, lihat [Mengotorisasi akses ke API Data Amazon Redshift](#).
2. Tentukan apakah Anda berencana untuk memanggil Data API dengan kredensial otentikasi dari Secrets Manager atau kredensial sementara. Untuk informasi selengkapnya, lihat [Memilih kredensial otentikasi database saat memanggil Amazon Redshift Data API](#).
3. Siapkan rahasia jika Anda menggunakan Secrets Manager untuk kredensial otentikasi. Untuk informasi selengkapnya, lihat [Menyimpan kredensial basis data di AWS Secrets Manager](#).
4. Tinjau pertimbangan dan batasan saat memanggil Data API. Untuk informasi selengkapnya, lihat [Pertimbangan saat memanggil Amazon Redshift Data API](#).
5. Panggil API Data dari AWS Command Line Interface (AWS CLI), dari kode Anda sendiri, atau menggunakan editor kueri di konsol Amazon Redshift. Untuk contoh panggilan dari AWS CLI, lihat [Memanggil API Data](#).

Pertimbangan saat memanggil Amazon Redshift Data API

Pertimbangkan hal berikut saat memanggil Data API:

- Amazon Redshift Data API dapat mengakses database di kluster yang disediakan Amazon Redshift dan grup kerja Tanpa Server Redshift. Untuk daftar Wilayah AWS tempat API Data Redshift tersedia, lihat titik akhir yang tercantum untuk [Redshift Data API](#) di Referensi Umum Amazon Web Services

- Durasi maksimum kueri adalah 24 jam.
- Jumlah maksimum kueri aktif (STARTED dan SUBMITTED kueri) per cluster Amazon Redshift adalah 200.
- Ukuran hasil kueri maksimum adalah 100 MB (setelah kompresi gzip). Jika panggilan mengembalikan lebih dari 100 MB data respons, panggilan akan berakhir.
- Waktu retensi maksimum untuk hasil kueri adalah 24 jam.
- Ukuran pernyataan kueri maksimum adalah 100 KB.
- Data API tersedia untuk kueri cluster single-node dan multiple-node dari tipe node berikut:
 - dc2.large
 - dc2.8xlarge
 - ra3.xlplus
 - ra3.4xlarge
 - ra3.16xlarge
- Cluster harus berada di cloud pribadi virtual (VPC) berdasarkan layanan Amazon VPC.
- Secara default, pengguna dengan peran IAM atau izin IAM yang sama dengan pelari operasi ExecuteStatement atau BatchExecuteStatement API dapat bertindak berdasarkan pernyataan yang sama dengan CancelStatement,, DescribeStatementGetStatementResult, dan operasi API. ListStatements Untuk bertindak pada pernyataan SQL yang sama dari pengguna lain, pengguna harus dapat mengambil peran IAM dari pengguna yang menjalankan pernyataan SQL. Untuk informasi selengkapnya tentang cara mengambil peran, lihat [Mengotorisasi akses ke API Data Amazon Redshift](#).
- Pernyataan SQL dalam Sqls parameter operasi BatchExecuteStatement API dijalankan sebagai satu transaksi. Mereka berjalan secara serial dalam urutan array. Pernyataan SQL berikutnya tidak dimulai sampai pernyataan sebelumnya dalam array selesai. Jika pernyataan SQL gagal, maka karena mereka dijalankan sebagai satu transaksi, semua pekerjaan digulirkan kembali.
- Waktu retensi maksimum untuk token klien yang digunakan dalam ExecuteStatement atau operasi BatchExecuteStatement API adalah 8 jam.
- Setiap API di Redshift Data API memiliki kuota transaksi per detik sebelum membatasi permintaan. Untuk kuota, lihat [Kuota untuk Amazon Redshift Data API](#). Jika tingkat permintaan melebihi kuota, a ThrottlingException dengan Kode Status HTTP: 400 dikembalikan. Untuk merespons pembatasan, gunakan strategi coba lagi seperti yang dijelaskan dalam [Perilaku Coba lagi di](#)

[AWS SDK and Tools Reference](#) Guide. Strategi ini diterapkan secara otomatis untuk membatasi kesalahan di beberapa AWS SDK.

Note

Secara default di AWS Step Functions, percobaan ulang tidak diaktifkan. Jika Anda perlu memanggil Redshift Data API di mesin status Step Functions, sertakan parameter `ClientToken` idempotency dalam panggilan Redshift Data API Anda. Nilai `ClientToken` kebutuhan untuk bertahan di antara percobaan ulang. Dalam contoh cuplikan permintaan `ExecuteStatement` API berikut, ekspresi `States.ArrayGetItem(States.StringSplit($$.Execution.Id, ':'), 7)` menggunakan fungsi intrinsik untuk mengekstrak bagian `UUID$$$.Execution.Id`, yang unik untuk setiap eksekusi mesin status. Untuk informasi selengkapnya, lihat [Fungsi intrinsik](#) di Panduan AWS Step Functions Pengembang.

```
{
  "Database": "dev",
  "Sql": "select 1;",
  "ClusterIdentifier": "MyCluster",
  "ClientToken.$": "States.ArrayGetItem(States.StringSplit($$.Execution.Id,
  ':'), 7)"
}
```

Memilih kredensi otentikasi database saat memanggil Amazon Redshift Data API

Saat memanggil Data API, Anda menggunakan salah satu metode otentikasi berikut untuk beberapa operasi API. Setiap metode membutuhkan kombinasi parameter yang berbeda.

AWS Secrets Manager

Dengan metode ini, berikan rahasia `secret-arn` yang disimpan di AWS Secrets Manager mana memiliki `username` dan `password`. Rahasia yang ditentukan berisi kredensial untuk terhubung ke yang database Anda tentukan. Ketika Anda menghubungkan ke cluster, Anda juga menyediakan nama database, Jika Anda memberikan identifier cluster (`dbClusterIdentifier`), itu harus cocok dengan identifier cluster yang disimpan dalam rahasia. Saat Anda menghubungkan ke workgroup tanpa server, Anda juga menyediakan nama database. Untuk informasi selengkapnya, lihat [Menyimpan kredensi basis data di AWS Secrets Manager](#).

Kredensial sementara

Dengan metode ini, pilih salah satu opsi berikut:

- Saat menghubungkan ke workgroup tanpa server, tentukan nama workgroup dan nama database. Nama pengguna database berasal dari identitas IAM. Misalnya, `arn:iam::123456789012:user:foo` memiliki nama pengguna database `IAM:foo`. Juga, izin untuk memanggil `redshift-serverless:GetCredentials` operasi diperlukan.
- Saat menghubungkan ke cluster sebagai identitas IAM, tentukan pengidentifikasi cluster dan nama database. Nama pengguna database berasal dari identitas IAM. Misalnya, `arn:iam::123456789012:user:foo` memiliki nama pengguna database `IAM:foo`. Juga, izin untuk memanggil `redshift:GetClusterCredentialsWithIAM` operasi diperlukan.
- Saat menghubungkan ke cluster sebagai pengguna database, tentukan pengidentifikasi cluster, nama database, dan nama pengguna database. Juga, izin untuk memanggil `redshift:GetClusterCredentials` operasi diperlukan. Untuk informasi tentang cara bergabung dengan grup database saat menghubungkan dengan metode ini, lihat [Bergabung dengan grup basis data saat menghubungkan ke klaster](#).

Dengan metode ini, Anda juga dapat memberikan `region` nilai yang menentukan di Wilayah AWS mana data Anda berada.

Memetakan tipe data JDBC saat memanggil Amazon Redshift Data API

Tabel berikut memetakan tipe data Java Database Connectivity (JDBC) ke jenis data yang Anda tentukan dalam panggilan API Data.

Jenis data JDBC	Jenis data API Data
INTEGER, SMALLINT, BIGINT	LONG
FLOAT, REAL, DOUBLE	DOUBLE
DECIMAL	STRING
BOOLEAN, BIT	BOOLEAN
BLOB, BINARY, LONGVARBINARY	BLOB
VARBINARY	STRING

Jenis data JDBC	Jenis data API Data
CLOB	STRING
Jenis lainnya (termasuk jenis yang terkait dengan tanggal dan waktu)	STRING

Nilai string diteruskan ke database Amazon Redshift dan secara implisit diubah menjadi tipe data database.

Note

Saat ini, Data API tidak mendukung array pengidentifikasi unik universal (UUID).

Menjalankan pernyataan SQL dengan parameter saat memanggil Amazon Redshift Data API

Anda dapat mengontrol teks SQL yang dikirimkan ke mesin database dengan memanggil operasi Data API menggunakan parameter untuk bagian dari pernyataan SQL. Parameter bernama menyediakan cara yang fleksibel untuk meneruskan parameter tanpa hardcoding mereka dalam teks SQL. Mereka membantu Anda menggunakan kembali teks SQL dan menghindari masalah injeksi SQL.

Contoh berikut menunjukkan parameter bernama dari `parameters` bidang `execute-statement` AWS CLI perintah.

```
--parameters "[{"name": "id", "value": "1"}, {"name": "address", "value": "Seattle"}]"
```

Pertimbangkan hal berikut saat menggunakan parameter bernama:

- Parameter bernama hanya dapat digunakan untuk mengganti nilai dalam pernyataan SQL.
 - Anda dapat mengganti nilai dalam pernyataan INSERT, seperti `INSERT INTO mytable VALUES (:val1)`.

Parameter bernama dapat dalam urutan apa pun dan parameter dapat digunakan lebih dari satu kali dalam teks SQL. Opsi parameter yang ditunjukkan dalam contoh sebelumnya, nilai-

nilai 1 dan Seattle dimasukkan ke dalam kolom tabel `id` dan `address`. Dalam teks SQL, Anda menentukan parameter bernama sebagai berikut:

```
--sql "insert into mytable values (:id, :address)"
```

- Anda dapat mengganti nilai dalam klausa kondisi, seperti `WHERE attr >= :val1`, `WHERE attr BETWEEN :val1 AND :val2`, dan `HAVING COUNT(attr) > :val`.
- Anda tidak dapat mengganti nama kolom dalam pernyataan SQL, seperti `SELECT column-name`, `ORDER BY column-name`, atau `GROUP BY column-name`.

Misalnya, pernyataan `SELECT` berikut gagal dengan sintaks yang tidak valid.

```
--sql "SELECT :colname, FROM event" --parameters "[{"name": "colname", "value": "eventname"}]"
```

Jika Anda menjelaskan (`describe-statement` operasi) pernyataan dengan kesalahan sintaks, yang `QueryString` dikembalikan tidak menggantikan nama kolom untuk parameter ("`QueryString`": "`SELECT :colname, FROM event`"), dan kesalahan dilaporkan (`ERROR: kesalahan sintaks di atau dekat "FROM"`\nPosisi: 12).

- Anda tidak dapat mengganti nama kolom dalam fungsi agregat, seperti `COUNT(column-name)`, `AVG(column-name)`, atau `SUM(column-name)`.
- Anda tidak dapat mengganti nama kolom dalam klausa `JOIN`.
- Ketika SQL berjalan, data secara implisit dilemparkan ke tipe data. Untuk informasi selengkapnya tentang casting tipe data, lihat Tipe [data](#) di Panduan Pengembang Database Amazon Redshift.
- Anda tidak dapat menetapkan nilai ke `NULL`. Data API menafsirkannya sebagai string `NULL` literal. Contoh berikut menggantikan `id` dengan string `null` literal. Bukan nilai SQL `NULL`.

```
--parameters [{"name": "id", "value": "null"}]"
```

- Anda tidak dapat menetapkan nilai panjang nol. Pernyataan Data API SQL gagal. Contoh berikut mencoba untuk mengatur `id` dengan nilai panjang nol dan menghasilkan kegagalan pernyataan SQL.

```
--parameters [{"name": "id", "value": ""}]"
```

- Anda tidak dapat mengatur nama tabel dalam pernyataan SQL dengan parameter. Data API mengikuti aturan `JDBCPreparedStatement`.

- Output dari `describe-statement` operasi mengembalikan parameter query dari pernyataan SQL.
- Hanya `execute-statement` operasi yang mendukung pernyataan SQL dengan parameter.

Menjalankan pernyataan SQL dengan token idempotensi saat memanggil Amazon Redshift Data API

Saat Anda membuat permintaan API yang bermutasi, permintaan biasanya menampilkan hasil sebelum alur kerja asinkron operasi selesai. Operasi mungkin juga habis waktu atau mengalami masalah server lain sebelum selesai, meskipun permintaan telah mengembalikan hasilnya. Hal ini dapat membuat sulit untuk menentukan apakah permintaan berhasil atau tidak, dan dapat menyebabkan beberapa percobaan ulang untuk memastikan bahwa operasi selesai dengan sukses. Namun, jika permintaan asli dan percobaan ulang berikutnya berhasil, operasi selesai beberapa kali. Ini berarti Anda dapat memperbarui lebih banyak sumber daya daripada yang Anda inginkan.

Idempotency memastikan bahwa permintaan API selesai tidak lebih dari satu kali. Dengan permintaan idempoten, jika permintaan asli berhasil diselesaikan, percobaan ulang berikutnya berhasil diselesaikan tanpa melakukan tindakan lebih lanjut. Data API `ExecuteStatement` dan `BatchExecuteStatement` operasi memiliki parameter `ClientToken` idempoten opsional. `ClientTokenKedaluwarsa` setelah 8 jam.

Important

Jika Anda memanggil `ExecuteStatement` dan `BatchExecuteStatement` mengoperasikannya dari AWS SDK, secara otomatis akan menghasilkan token klien untuk digunakan saat mencoba lagi. Dalam hal ini, kami tidak menyarankan menggunakan `client-token` parameter dengan `ExecuteStatement` dan `BatchExecuteStatement` operasi. Lihat CloudTrail log untuk melihat `ClientToken`. Untuk contoh CloudTrail log, lihat [Contoh API Data Amazon Redshift](#).

`execute-statement` AWS CLI Perintah berikut mengilustrasikan `client-token` parameter opsional untuk idempotensi.

```
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
```

Tabel berikut menunjukkan beberapa tanggapan umum yang mungkin Anda dapatkan untuk permintaan API idempoten, dan memberikan rekomendasi coba ulang.

Respons	Rekomendasi	Komentar
200 (OK)	Jangan coba lagi	Permintaan asli berhasil diselesaikan. Setiap percobaan ulang berikutnya berhasil kembali.
Kode respons 400 seri	Jangan coba lagi	<p>Ada masalah dengan permintaan, dari antara yang berikut:</p> <ul style="list-style-type: none"> • Ini termasuk parameter atau kombinasi parameter yang tidak valid. • Ini menggunakan tindakan atau sumber daya yang Anda tidak memiliki izin. • Ini menggunakan sumber daya yang sedang dalam proses mengubah keadaan. <p>Jika permintaan melibatkan sumber daya yang sedang dalam proses mengubah status, mencoba kembali permintaan mungkin berhasil.</p>
Kode respons 500 seri	Coba lagi	<p>Kesalahan ini disebabkan oleh masalah AWS sisi server dan umumnya bersifat sementara . Ulangi permintaan dengan strategi backoff yang sesuai.</p>

Untuk informasi tentang kode respons Amazon Redshift, lihat [Kesalahan Umum](#) di Referensi API Amazon Redshift.

Mengotorisasi akses ke API Data Amazon Redshift

Untuk mengakses Data API, pengguna harus diberi wewenang. Anda dapat mengotorisasi pengguna untuk mengakses Data API dengan menambahkan kebijakan terkelola, yang merupakan kebijakan standar AWS Identity and Access Management (IAM), ke pengguna tersebut. Sebagai praktik terbaik, kami merekomendasikan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#). Untuk melihat izin yang diizinkan dan ditolak oleh kebijakan terkelola, lihat konsol IAM (<https://console.aws.amazon.com/iam/>).

Amazon Redshift menyediakan kebijakan `AmazonRedshiftDataFullAccess` terkelola. Kebijakan ini menyediakan akses penuh ke operasi Amazon Redshift Data API. Kebijakan ini juga memungkinkan akses tercakup ke Amazon Redshift tertentu AWS Secrets Manager, dan operasi IAM API yang diperlukan untuk mengautentikasi dan mengakses kluster Amazon Redshift atau grup kerja Tanpa Server Redshift.

Anda juga dapat membuat kebijakan IAM Anda sendiri yang memungkinkan akses ke sumber daya tertentu. Untuk membuat kebijakan Anda, gunakan `AmazonRedshiftDataFullAccess` kebijakan sebagai templat awal Anda. Setelah membuat kebijakan, tambahkan ke setiap pengguna yang memerlukan akses ke API Data.

Pertimbangkan persyaratan berikut dari kebijakan IAM yang terkait dengan pengguna:

- Jika Anda menggunakan AWS Secrets Manager untuk mengautentikasi, konfirmasi kebijakan mengizinkan penggunaan `secretsmanager:GetSecretValue` tindakan untuk mengambil rahasia yang ditandai dengan kunci. `RedshiftDataFullAccess`
- Jika Anda menggunakan kredensi sementara untuk mengautentikasi ke kluster, konfirmasi kebijakan tersebut mengizinkan penggunaan `redshift:GetClusterCredentials` tindakan ke nama pengguna database `redshift_data_api_user` untuk database apa pun di kluster. Nama pengguna ini harus sudah dibuat di database Anda.
- Jika Anda menggunakan kredensi sementara untuk mengautentikasi ke grup kerja tanpa server, konfirmasi kebijakan tersebut mengizinkan penggunaan `redshift-serverless:GetCredentials` tindakan untuk mengambil grup kerja yang diberi tag dengan kunci tersebut. `RedshiftDataFullAccess` Pengguna database dipetakan 1:1 ke identitas sumber AWS Identity and Access Management (IAM). Misalnya, pengguna `sample_user` dipetakan ke pengguna database `IAM:sample_user`, dan peran IAM `sample_role` dipetakan ke `IAM:sample_role` Untuk informasi selengkapnya tentang identitas IAM, lihat [Identitas IAM \(pengguna, grup pengguna, dan peran\)](#) di Panduan Pengguna IAM.

Untuk menjalankan kueri pada kluster yang dimiliki oleh akun lain, akun pemilik harus menyediakan peran IAM yang dapat diasumsikan oleh API Data di akun panggilan. Misalnya, Akun B memiliki kluster yang perlu diakses oleh Akun A. Akun B dapat melampirkan kebijakan AWS yang dikelola `AmazonRedshiftDataFullAccess` ke peran IAM Akun B. Kemudian Akun B mempercayai Akun A menggunakan kebijakan kepercayaan seperti berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::accountID-of-account-A:role/someRoleA"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Akhirnya, peran Account A IAM harus dapat mengambil peran Account B IAM.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::accountID-of-account-B:role/someRoleB"
  }
}
```

Tautan berikut memberikan informasi lebih lanjut tentang AWS Identity and Access Management Panduan Pengguna IAM.

- Untuk informasi tentang membuat peran IAM, lihat [Membuat peran IAM](#).
- Untuk informasi tentang membuat kebijakan IAM, lihat [Membuat kebijakan IAM](#).
- Untuk informasi tentang menambahkan kebijakan IAM ke pengguna, lihat [Menambahkan dan menghapus izin identitas IAM](#).

Menyimpan kredensi basis data di AWS Secrets Manager

Saat memanggil Data API, Anda dapat meneruskan kredensial untuk klaster atau grup kerja tanpa server dengan menggunakan secret in. AWS Secrets Manager Untuk memberikan kredensial dengan cara ini, Anda menentukan nama rahasia atau Amazon Resource Name (ARN) rahasia tersebut.

Untuk menyimpan kredensial dengan Secrets Manager, Anda memerlukan izin kebijakan `SecretManagerReadWrite` terkelola. Untuk informasi selengkapnya tentang izin minimum, lihat [Membuat dan Mengelola Rahasia dengan AWS Secrets Manager](#) di Panduan AWS Secrets Manager Pengguna.

Untuk menyimpan kredensial Anda secara rahasia untuk cluster Amazon Redshift

1. Gunakan AWS Secrets Manager konsol untuk membuat rahasia yang berisi kredensial untuk klaster Anda:
 - Saat Anda memilih Simpan rahasia baru, pilih `Credentials for Redshift cluster`.
 - Simpan nilai Anda untuk nama Pengguna (pengguna basis data), Kata Sandi, dan cluster DB (pengidentifikasi cluster) dalam rahasia Anda.
 - Tandai rahasia dengan kuncinya `RedshiftDataFullAccess`. Kebijakan `AWS-managed AmazonRedshiftDataFullAccess` hanya mengizinkan tindakan `secretsmanager:GetSecretValue` untuk rahasia yang ditandai dengan kunci `RedshiftDataFullAccess`

Untuk instruksi, lihat [Membuat Rahasia Basic](#) di Panduan Pengguna AWS Secrets Manager .

2. Gunakan AWS Secrets Manager konsol untuk melihat detail rahasia yang Anda buat, atau jalankan `aws secretsmanager describe-secret` AWS CLI perintah.

Catat nama dan ARN rahasia. Anda dapat menggunakan ini dalam panggilan ke Data API.

Untuk menyimpan kredensial Anda secara rahasia untuk grup kerja tanpa server

1. Gunakan AWS Secrets Manager AWS CLI perintah untuk menyimpan rahasia yang berisi kredensial untuk workgroup tanpa server Anda:
 - Buat rahasia Anda dalam sebuah file, misalnya file JSON bernama `mycreds.json`. Berikan nilai untuk nama Pengguna (pengguna basis data) dan Kata Sandi dalam file.

```
{
  "username": "myusername",
  "password": "mypassword"
}
```

- Simpan nilai-nilai Anda dalam rahasia Anda dan tandai rahasia dengan `kunciRedshiftDataFullAccess`.

```
aws secretsmanager create-secret --name MyRedshiftSecret --tags
Key="RedshiftDataFullAccess",Value="serverless" --secret-string file://
mycreds.json
```

Berikut ini menunjukkan output.

```
{
  "ARN":
  "arn:aws:secretsmanager:region:accountId:secret:MyRedshiftSecret-mvLHxf",
  "Name": "MyRedshiftSecret",
  "VersionId": "a1603925-e8ea-4739-9ae9-e509eEXAMPLE"
}
```

Untuk informasi selengkapnya, lihat [Membuat Rahasia Dasar dengan AWS CLI](#) di Panduan AWS Secrets Manager Pengguna.

2. Gunakan AWS Secrets Manager konsol untuk melihat detail rahasia yang Anda buat, atau jalankan `aws secretsmanager describe-secret` AWS CLI perintah.

Catat nama dan ARN rahasia. Anda dapat menggunakan ini dalam panggilan ke Data API.

Membuat endpoint (AWS PrivateLink) Amazon VPC untuk API Data

Amazon Virtual Private Cloud (Amazon VPC) memungkinkan Anda meluncurkan AWS sumber daya, seperti kluster dan aplikasi Amazon Redshift, ke cloud pribadi virtual (VPC). AWS PrivateLink menyediakan konektivitas pribadi antara virtual private cloud (VPC) dan AWS layanan dengan aman di jaringan Amazon. Dengan menggunakan AWS PrivateLink, Anda dapat membuat titik akhir VPC, yang dapat Anda gunakan sambungkan ke layanan di berbagai akun dan VPC berdasarkan Amazon VPC. Untuk informasi selengkapnya AWS PrivateLink, lihat [Layanan Titik Akhir VPC \(AWS PrivateLink\)](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Anda dapat memanggil titik akhir API Data dengan titik akhir Amazon VPC. Menggunakan titik akhir VPC Amazon menjaga lalu lintas antar aplikasi di VPC Amazon Anda dan API Data di AWS jaringan, tanpa menggunakan alamat IP publik. Titik akhir Amazon VPC dapat membantu Anda memenuhi persyaratan kepatuhan dan peraturan yang berkaitan dengan membatasi konektivitas internet publik. Misalnya, jika Anda menggunakan titik akhir Amazon VPC, Anda dapat mempertahankan lalu lintas antara aplikasi yang berjalan pada instans Amazon EC2 dan API Data di VPC yang memuatnya.

Setelah membuat titik akhir Amazon VPC, Anda dapat mulai menggunakannya tanpa membuat kode atau perubahan konfigurasi apa pun di aplikasi Anda.

Membuat titik akhir Amazon VPC untuk API Data

1. [Masuk ke AWS Management Console dan buka konsol VPC Amazon di https://console.aws.amazon.com/vpc/.](https://console.aws.amazon.com/vpc/)
2. Pilih Titik Akhir, lalu pilih Buat Titik Akhir.
3. Di halaman Buat Titik Akhir, untuk Kategori layanan, pilih Layanan AWS . Untuk Nama Layanan, pilih redshift-data (). `com.amazonaws.region.redshift-data`
4. Untuk VPC, pilih VPC tempat membuat titik akhir.

Pilih VPC yang berisi aplikasi yang membuat panggilan API Data.

5. Untuk Subnet, pilih subnet untuk setiap Availability Zone (AZ) yang digunakan oleh AWS layanan yang menjalankan aplikasi Anda.

Untuk membuat titik akhir VPC Amazon, tentukan rentang alamat IP pribadi tempat titik akhir dapat diakses. Untuk melakukannya, pilih subnet untuk setiap Zona Ketersediaan. Hal tersebut membatasi titik akhir VPC ke rentang alamat IP pribadi khusus untuk setiap Zona Ketersediaan dan membuat titik akhir Amazon VPC di setiap Zona Ketersediaan.

6. Untuk Aktifkan nama DNS, pilih Aktifkan untuk titik akhir ini.

DNS Pribadi menyelesaikan nama host DNS API Data standar (`https://redshift-data.region.amazonaws.com`) ke alamat IP pribadi yang dikaitkan dengan nama host DNS khusus untuk titik akhir Amazon VPC Anda. Akibatnya, Anda dapat mengakses titik akhir VPC Data API menggunakan AWS CLI atau AWS SDK tanpa membuat perubahan kode atau konfigurasi apa pun untuk memperbarui URL titik akhir API Data.

7. Untuk Grup keamanan, pilih satu grup keamanan untuk dikaitkan dengan titik akhir Amazon VPC.

Pilih grup keamanan yang memungkinkan akses ke AWS layanan yang menjalankan aplikasi Anda. Misalnya, jika instans Amazon EC2 menjalankan aplikasi Anda, pilih grup keamanan yang mengizinkan akses ke instans Amazon EC2. Grup keamanan memungkinkan Anda mengontrol lalu lintas ke titik akhir Amazon VPC dari sumber daya di VPC Anda.

8. Pilih Buat Titik Akhir.

Setelah titik akhir dibuat, pilih tautan di AWS Management Console untuk melihat detail titik akhir.

Tab Detail titik akhir menunjukkan nama host DNS yang dibuat saat membuat titik akhir Amazon VPC.

Anda dapat menggunakan titik akhir standar (`redshift-data.region.amazonaws.com`) atau salah satu titik akhir khusus VPC untuk memanggil API Data dalam Amazon VPC. Titik akhir API Data standar secara otomatis merutekan ke titik akhir Amazon VPC. Perutean ini terjadi karena nama host DNS Pribadi diaktifkan saat titik akhir Amazon VPC dibuat.

Saat Anda menggunakan titik akhir Amazon VPC dalam panggilan API Data, semua lalu lintas antara aplikasi Anda dan API Data tetap berada di Amazon VPC yang berisi semuanya. Anda dapat menggunakan titik akhir Amazon VPC untuk semua jenis panggilan API Data. Lihat informasi selengkapnya tentang memanggil API Data di [Pertimbangan saat memanggil Amazon Redshift Data API](#).

Bergabung dengan grup basis data saat menghubungkan ke klaster

Grup database adalah kumpulan pengguna database. Hak istimewa database dapat diberikan kepada grup. Administrator dapat mengonfigurasi peran IAM sedemikian rupa sehingga grup database ini diperhitungkan saat SQL Anda berjalan dengan API Data. Untuk informasi selengkapnya tentang grup database, lihat [Grup](#) di Panduan Pengembang Database Amazon Redshift.

Anda dapat mengonfigurasi peran IAM pemanggil API Data sehingga pengguna database yang ditentukan dalam panggilan bergabung dengan grup database saat API Data terhubung ke klaster. Kemampuan ini hanya didukung saat menghubungkan ke cluster yang disediakan. Itu tidak didukung saat menghubungkan ke grup kerja Redshift Serverless. Peran IAM dari pemanggil Data API juga harus memungkinkan tindakan. `redshift:JoinGroup`

Konfigurasi ini dengan menambahkan tag ke peran IAM. Administrator peran IAM pemanggil menambahkan tag dengan kunci `RedshiftDbGroups` dan nilai kunci dari daftar grup database. Nilainya adalah daftar nama titik dua (:) dipisahkan dari kelompok database hingga total panjang

256 karakter. Grup database harus didefinisikan sebelumnya dalam database yang terhubung. Jika grup tertentu tidak ditemukan dalam database, itu diabaikan. Misalnya, untuk grup database `accounting` dan `retail`, nilai kunci adalah `accounting:retail`. Pasangan nilai kunci tag `{"Key": "RedshiftDbGroups", "Value": "accounting:retail"}` digunakan oleh Data API untuk menentukan grup database mana yang terkait dengan pengguna database yang disediakan dalam panggilan ke Data API.

Untuk menambahkan grup database sebagai tag ke peran IAM

1. Masuk ke AWS Management Console dan buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi konsol, pilih Peran lalu pilih nama peran yang ingin Anda edit.
3. Pilih tab Tag, lalu pilih Kelola tag.
4. Pilih Tambah tag, lalu tambahkan kunci `RedshiftDbGrup` dan nilai yang merupakan daftar *database-groups-colon-separated*.
5. Pilih Simpan perubahan.

Sekarang ketika prinsipal IAM (dengan peran IAM ini terpasang) memanggil Data API, pengguna database yang ditentukan bergabung dengan grup database yang ditentukan dalam peran IAM.

Untuk informasi selengkapnya tentang cara melampirkan tag ke prinsipal, termasuk peran IAM dan pengguna IAM, lihat [Menandai sumber daya IAM](#) di Panduan Pengguna IAM.

Memanggil API Data

Anda dapat memanggil Data API atau AWS CLI untuk menjalankan pernyataan SQL pada kluster atau grup kerja tanpa server. Operasi utama untuk menjalankan pernyataan SQL adalah [ExecuteStatement](#) dan [BatchExecuteStatement](#) di Referensi API Data Amazon Redshift. Data API mendukung bahasa pemrograman yang didukung oleh AWS SDK. Untuk informasi selengkapnya tentang ini, lihat [Alat untuk Dibangun AWS](#).

Untuk melihat contoh kode pemanggilan Data API, lihat [Memulai dengan Redshift Data API](#) di GitHub Repositori ini memiliki contoh penggunaan AWS Lambda untuk mengakses data Amazon Redshift dari Amazon EC2 AWS Glue Data Catalog,, dan Amazon Runtime. SageMaker Contoh bahasa pemrograman termasuk Python, Go, Java, dan Javascript.

Anda dapat memanggil API Data menggunakan AWS CLI.

Contoh berikut menggunakan AWS CLI untuk memanggil Data API. Untuk menjalankan contoh, edit nilai parameter agar sesuai dengan lingkungan Anda. Dalam banyak contoh, a `cluster-identifier` disediakan untuk dijalankan melawan cluster. Saat Anda menjalankan `workgroup` tanpa server, Anda menyediakan sebagai gantinya. `workgroup-name` Contoh-contoh ini menunjukkan beberapa operasi Data API. Untuk informasi selengkapnya, lihat Referensi Perintah AWS CLI .

Perintah dalam contoh berikut telah dibagi dan diformat agar mudah dibaca.

Untuk menjalankan pernyataan SQL

Untuk menjalankan pernyataan SQL, gunakan `aws redshift-data execute-statement` AWS CLI perintah.

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster dan mengembalikan identifier untuk mengambil hasil. Contoh ini menggunakan metode AWS Secrets Manager otentikasi.

```
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
```

Berikut adalah contoh respons tersebut.

```
{
  "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"
}
```

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster dan mengembalikan identifier untuk mengambil hasil. Contoh ini menggunakan metode otentikasi kredensial sementara.

```
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"
```

Berikut adalah contoh respons tersebut.

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598306924.632,
  "Database": "dev",
  "DbUser": "myuser",
  "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap workgroup tanpa server dan mengembalikan identifier untuk mengambil hasilnya. Contoh ini menggunakan metode otentikasi kredensial sementara.

```
aws redshift-data execute-statement
--database dev
--workgroup-name myworkgroup
--sql "select 1;"
```

Berikut adalah contoh respons tersebut.

```
{
  "CreatedAt": "2022-02-11T06:25:28.748000+00:00",
  "Database": "dev",
  "DbUser": "IAMR:RoleName",
  "Id": "89dd91f5-2d43-43d3-8461-f33aa093c41e",
  "WorkgroupName": "myworkgroup"
}
```

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster dan mengembalikan identifier untuk mengambil hasil. Contoh ini menggunakan metode AWS Secrets Manager otentikasi dan token idempotensi.

```
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
```

Berikut adalah contoh respons tersebut.

```
{
  "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"
}
```

Untuk menjalankan pernyataan SQL dengan parameter

Untuk menjalankan pernyataan SQL, gunakan `aws redshift-data execute-statement` AWS CLI perintah.

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster dan mengembalikan identifier untuk mengambil hasil. Contoh ini menggunakan metode AWS Secrets Manager otentikasi. Teks SQL memiliki parameter `distance` bernama. Dalam hal ini, jarak yang digunakan dalam predikat adalah 5. Dalam pernyataan `SELECT`, parameter bernama untuk nama kolom hanya dapat digunakan dalam predikat. Nilai untuk parameter bernama untuk pernyataan SQL ditentukan dalam `parameters` opsi.

```
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
```

Berikut adalah contoh respons tersebut.

```
{
  "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"
}
```

Contoh berikut menggunakan EVENT tabel dari database sampel. Untuk informasi selengkapnya, lihat [tabel EVENT](#) di Panduan Pengembang Database Amazon Redshift.

Jika Anda belum memiliki EVENT tabel di database Anda, Anda dapat membuatnya menggunakan Data API sebagai berikut:

```
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)"
```

Perintah berikut menyisipkan satu baris ke dalam EVENT tabel.

```
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"}]"
```

Perintah berikut menyisipkan baris kedua ke dalam EVENT tabel. Contoh ini menunjukkan hal berikut:

- Parameter bernama `id` digunakan empat kali dalam teks SQL.
- Konversi tipe implisit diterapkan secara otomatis saat memasukkan parameter. `starttime`
- `venueid` Kolom adalah tipe `cast` ke tipe data `SMALLINT`.
- String karakter yang mewakili tipe data `DATE` secara implisit diubah menjadi tipe data `TIMESTAMP`.
- Komentar dapat digunakan dalam teks SQL.

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "insert into event values(:id, :id::smallint, :id, :id, :eventname, :starttime) /
*this is comment, and it won't apply parameterization for :id, :eventname or :starttime
here*/"
--parameters "[{"name\": \"eventname\", \"value\": \"event 2\"},
                {\"name\": \"starttime\", \"value\": \"2022-02-22\"},
                {\"name\": \"id\", \"value\": \"2\"}]"
```

Berikut ini menunjukkan dua baris yang disisipkan:

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

Perintah berikut menggunakan parameter bernama dalam klausa `WHERE` untuk mengambil baris di mana `eventid` adalah 1

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
```

```
--db-user awsuser
--sql "select * from event where eventid=:id"
--parameters "[{"name": "id", "value": "1"}]"
```

Jalankan perintah berikut untuk mendapatkan hasil SQL dari pernyataan SQL sebelumnya:

```
aws redshift-data get-statement-result --id 7529ad05-b905-4d71-9ec6-8b333836eb5a
```

Memberikan hasil sebagai berikut:

```
{
  "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
}
```

Untuk menjalankan beberapa pernyataan SQL

Untuk menjalankan beberapa pernyataan SQL dengan satu perintah, gunakan `aws redshift-data batch-execute-statement` AWS CLI perintah.

AWS CLI Perintah berikut menjalankan tiga pernyataan SQL terhadap cluster dan mengembalikan identifier untuk mengambil hasil. Contoh ini menggunakan metode otentikasi kredensial sementara.

```
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"
```

Berikut adalah contoh respons tersebut.

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598306924.632,
  "Database": "dev",
  "DbUser": "myuser",
  "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

Untuk daftar metadata tentang pernyataan SQL

Untuk daftar metadata tentang pernyataan SQL, gunakan perintah `aws redshift-data list-statements` AWS CLI Otorisasi untuk menjalankan perintah ini didasarkan pada izin IAM pemanggil.

AWS CLI Perintah berikut mencantumkan pernyataan SQL yang berjalan.

```
aws redshift-data list-statements
  --region us-west-2
  --status ALL
```

Berikut adalah contoh respons tersebut.

```
{
  "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
  }
]
```

Untuk menggambarkan metadata tentang pernyataan SQL

Untuk mendapatkan deskripsi metadata untuk pernyataan SQL, gunakan perintah `aws redshift-data describe-statement` AWS CLI Otorisasi untuk menjalankan perintah ini didasarkan pada izin IAM pemanggil.

AWS CLI Perintah berikut menjelaskan pernyataan SQL.

```
aws redshift-data describe-statement
  --id d9b6c0c9-0747-4bf4-b142-e8883122f766
  --region us-west-2
```

Berikut adalah contoh respons tersebut.

```
{
  "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
}
```

Berikut ini adalah contoh describe-statement respon setelah menjalankan batch-execute-statement perintah dengan beberapa pernyataan SQL.

```
{
  "ClusterIdentifier": "mayo",
  "CreatedAt": 1623979777.126,
  "Duration": 6591877,
  "HasResultSet": true,
  "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652",
  "RedshiftPid": 31459,
  "RedshiftQueryId": 0,
  "ResultRows": 2,
  "ResultSize": 22,
  "Status": "FINISHED",
  "SubStatements": [
    {
      "CreatedAt": 1623979777.274,
      "Duration": 3396637,
      "HasResultSet": true,
      "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:1",
      "QueryString": "select 1;",
      "RedshiftQueryId": -1,
      "ResultRows": 1,
      "ResultSize": 11,
      "Status": "FINISHED",
      "UpdatedAt": 1623979777.903
    },
    {
      "CreatedAt": 1623979777.274,
```

```

        "Duration": 3195240,
        "HasResultSet": true,
        "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2",
        "QueryString": "select 2;",
        "RedshiftQueryId": -1,
        "ResultRows": 1,
        "ResultSize": 11,
        "Status": "FINISHED",
        "UpdatedAt": 1623979778.076
    }
],
"UpdatedAt": 1623979778.183
}

```

Untuk mengambil hasil dari pernyataan SQL

Untuk mengambil hasil dari pernyataan SQL yang berjalan, gunakan perintah. `redshift-data get-statement-result` AWS CLI Anda dapat memberikan Id yang Anda terima sebagai tanggapan terhadap `execute-statement` atau `batch-execute-statement`. IdNilai untuk pernyataan SQL yang dijalankan oleh `batch-execute-statement` dapat diambil dalam hasil `describe-statement` dan diakhiran oleh titik dua dan nomor urut seperti. `b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2` Jika Anda menjalankan beberapa pernyataan SQL dengan `batch-execute-statement`, setiap pernyataan SQL memiliki Id nilai seperti yang ditunjukkan pada. `describe-statement` Otorisasi untuk menjalankan perintah ini didasarkan pada izin IAM pemanggil.

Pernyataan berikut mengembalikan hasil dari pernyataan SQL dijalankan oleh `execute-statement`.

```

aws redshift-data get-statement-result
  --id d9b6c0c9-0747-4bf4-b142-e8883122f766
  --region us-west-2

```

Pernyataan berikut mengembalikan hasil dari pernyataan SQL kedua dijalankan oleh `batch-execute-statement`.

```

aws redshift-data get-statement-result
  --id b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2
  --region us-west-2

```

Berikut ini adalah contoh respons terhadap panggilan `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
}
```

Untuk menggambarkan tabel

Untuk mendapatkan metadata yang menggambarkan tabel, gunakan perintah `aws redshift-data describe-table` AWS CLI

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster dan mengembalikan metadata yang menggambarkan tabel. Contoh ini menggunakan metode AWS Secrets Manager otentikasi.

```
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
```

Berikut adalah contoh respons tersebut.

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

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster yang menggambarkan tabel. Contoh ini menggunakan metode otentikasi kredensial sementara.

```
aws redshift-data describe-table  
--region us-west-2  
--db-user myuser  
--cluster-identifier mycluster-test  
--database dev  
--schema information_schema  
--table sql_features
```

Berikut adalah contoh respons tersebut.

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

Untuk membuat daftar database dalam sebuah cluster

Untuk membuat daftar database dalam sebuah cluster, gunakan `aws redshift-data list-databases` AWS CLI perintah.

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster untuk daftar database. Contoh ini menggunakan metode AWS Secrets Manager otentikasi.

```
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
```

Berikut adalah contoh respons tersebut.

```
{
  "Databases": [
    "dev"
  ]
}
```

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster untuk daftar database. Contoh ini menggunakan metode otentikasi kredensial sementara.

```
aws redshift-data list-databases
--region us-west-2
--db-user myuser
--cluster-identifier mycluster-test
--database dev
```

Berikut adalah contoh respons tersebut.

```
{
  "Databases": [
    "dev"
  ]
}
```

Untuk membuat daftar skema dalam database

Untuk membuat daftar skema dalam database, gunakan `aws redshift-data list-schemas` AWS CLI perintah.

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster untuk daftar skema dalam database. Contoh ini menggunakan metode AWS Secrets Manager otentikasi.

```
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
```

Berikut adalah contoh respons tersebut.

```
{
  "Schemas": [
    "information_schema",
    "pg_catalog",
    "pg_internal",
    "public"
  ]
}
```

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster untuk daftar skema dalam database. Contoh ini menggunakan metode otentikasi kredensial sementara.

```
aws redshift-data list-schemas
--region us-west-2
--db-user mysuser
--cluster-identifier mycluster-test
--database dev
```

Berikut adalah contoh respons tersebut.

```
{
  "Schemas": [
    "information_schema",
    "pg_catalog",
    "pg_internal",
    "public"
  ]
}
```

Untuk daftar tabel dalam database

Untuk daftar tabel dalam database, gunakan `aws redshift-data list-tables` AWS CLI perintah.

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster untuk daftar tabel dalam database. Contoh ini menggunakan metode AWS Secrets Manager otentikasi.

```
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
```

Berikut adalah contoh respons tersebut.

```
{
  "Tables": [
    {
      "name": "sql_features",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    },
    {
      "name": "sql_implementation_info",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    }
  ]
}
```

AWS CLI Perintah berikut menjalankan pernyataan SQL terhadap cluster untuk daftar tabel dalam database. Contoh ini menggunakan metode otentikasi kredensial sementara.

```
aws redshift-data list-tables
  --region us-west-2
  --db-user myuser
  --cluster-identifier mycluster-test
  --database dev
  --schema information_schema
```

Berikut adalah contoh respons tersebut.

```
{
  "Tables": [
    {
      "name": "sql_features",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    },
    {
      "name": "sql_implementation_info",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    }
  ]
}
```

Memecahkan masalah untuk Amazon Redshift Data API

Gunakan bagian berikut, yang berjudul pesan kesalahan umum, untuk membantu memecahkan masalah yang Anda alami dengan API Data.

Topik

- [Paket untuk kueri terlalu besar](#)
- [Respons basis data melebihi batas ukuran](#)

Paket untuk kueri terlalu besar

Jika Anda melihat kesalahan yang menunjukkan bahwa paket untuk kueri terlalu besar, umumnya set hasil yang dikembalikan untuk baris terlalu besar. Batas ukuran API Data adalah 64 KB per baris dalam set hasil yang ditampilkan oleh basis data.

Untuk mengatasi masalah ini, pastikan setiap baris dalam set hasil berukuran 64 KB atau kurang.

Respons basis data melebihi batas ukuran

Jika Anda melihat kesalahan yang menunjukkan bahwa respons database telah melebihi batas ukuran, umumnya ukuran kumpulan hasil yang dikembalikan oleh database terlalu besar. Batas Data API adalah 100 MB dalam kumpulan hasil yang dikembalikan oleh database.

Untuk mengatasi masalah ini, pastikan panggilan ke Data API mengembalikan 100 MB data atau kurang. Jika Anda perlu mengembalikan lebih dari 100 MB, Anda dapat menjalankan beberapa panggilan pernyataan dengan LIMIT klausa dalam kueri Anda.

Menjadwalkan operasi Amazon Redshift Data API dengan Amazon EventBridge

Anda dapat membuat aturan yang cocok dengan peristiwa yang dipilih dan mengarahkannya ke target untuk mengambil tindakan. Anda juga dapat menggunakan aturan untuk mengambil tindakan pada jadwal yang telah ditentukan. Untuk informasi selengkapnya, lihat [Panduan EventBridge Pengguna Amazon](#).

Untuk menjadwalkan operasi Data API dengan EventBridge, peran IAM terkait harus mempercayai prinsipal untuk CloudWatch Acara (events.amazonaws.com). Peran ini harus setara dengan kebijakan terkelola yang AmazonEventBridgeFullAccess dilampirkan. Itu juga harus memiliki izin AmazonRedshiftDataFullAccess kebijakan yang dikelola oleh API Data. Anda dapat membuat peran IAM dengan izin ini di konsol IAM. Saat membuat peran di konsol IAM, pilih entitas terpercaya AWS layanan untuk CloudWatch Acara. Tentukan peran IAM dalam nilai RoleArn JSON di target. EventBridge Untuk informasi selengkapnya tentang membuat peran IAM, lihat [Membuat Peran untuk AWS Layanan \(Konsol\)](#) di Panduan Pengguna IAM.

Aturan name yang Anda buat di Amazon EventBridge harus cocok dengan StatementName diRedshiftDataParameters.

Contoh berikut menunjukkan variasi pembuatan EventBridge aturan dengan satu atau beberapa pernyataan SQL dan dengan cluster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server sebagai gudang data.

Memanggil dengan satu pernyataan SQL dan cluster

Contoh berikut menggunakan AWS CLI untuk membuat EventBridge aturan yang digunakan untuk menjalankan pernyataan SQL terhadap cluster Amazon Redshift.

```
aws events put-rule
--name test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

Kemudian EventBridge target dibuat untuk berjalan pada jadwal yang ditentukan dalam aturan.

```
aws events put-targets
--cli-input-json file://data.json
```

File input data.json adalah sebagai berikut. Kunci `Sql` JSON menunjukkan ada pernyataan SQL tunggal. Nilai `Arn` JSON berisi pengidentifikasi cluster. Nilai `RoleArn` JSON berisi peran IAM yang digunakan untuk menjalankan SQL seperti yang dijelaskan sebelumnya.

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

Memanggil dengan satu pernyataan SQL dan workgroup

Contoh berikut menggunakan AWS CLI untuk membuat EventBridge aturan yang digunakan untuk menjalankan pernyataan SQL terhadap workgroup Amazon Redshift Tanpa Server.

```
aws events put-rule
--name test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

Kemudian EventBridge target dibuat untuk berjalan pada jadwal yang ditentukan dalam aturan.

```
aws events put-targets
--cli-input-json file://data.json
```

File input data.json adalah sebagai berikut. Kunci `Sql` JSON menunjukkan ada pernyataan SQL tunggal. Nilai `Arn` JSON berisi nama workgroup. Nilai `RoleArn` JSON berisi peran IAM yang digunakan untuk menjalankan SQL seperti yang dijelaskan sebelumnya.

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

Memanggil dengan beberapa pernyataan SQL dan cluster

Contoh berikut menggunakan AWS CLI untuk membuat EventBridge aturan yang digunakan untuk menjalankan beberapa pernyataan SQL terhadap cluster Amazon Redshift.

```
aws events put-rule
--name test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

Kemudian EventBridge target dibuat untuk berjalan pada jadwal yang ditentukan dalam aturan.

```
aws events put-targets
--cli-input-json file://data.json
```

File input data.json adalah sebagai berikut. Kunci `Sqls` JSON menunjukkan ada beberapa pernyataan SQL. Nilai `Arn` JSON berisi pengidentifikasi cluster. Nilai `RoleArn` JSON berisi peran IAM yang digunakan untuk menjalankan SQL seperti yang dijelaskan sebelumnya.

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

Memanggil dengan beberapa pernyataan SQL dan workgroup

Contoh berikut menggunakan AWS CLI untuk membuat EventBridge aturan yang digunakan untuk menjalankan beberapa pernyataan SQL terhadap workgroup Amazon Redshift Tanpa Server.

```
aws events put-rule
--name test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

Kemudian EventBridge target dibuat untuk berjalan pada jadwal yang ditentukan dalam aturan.

```
aws events put-targets
--cli-input-json file://data.json
```

File input data.json adalah sebagai berikut. Kunci `Sqls` JSON menunjukkan ada beberapa pernyataan SQL. Nilai `Arn` JSON berisi nama workgroup. Nilai `RoleArn` JSON berisi peran IAM yang digunakan untuk menjalankan SQL seperti yang dijelaskan sebelumnya.

```
{
  "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
  }
}
```

Memantau API Data

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja API Data dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton API Data, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- Amazon EventBridge dapat digunakan untuk mengotomatiskan AWS layanan Anda dan merespons secara otomatis peristiwa sistem, seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirimkan ke EventBridge dalam waktu nyaris nyata. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis mana yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Untuk informasi selengkapnya, lihat [Panduan EventBridge Pengguna Amazon](#).
- AWS CloudTrail menangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk mempelajari selengkapnya tentang cara Amazon Redshift terintegrasi AWS CloudTrail, lihat [Logging](#) with CloudTrail. Untuk informasi selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

Topik

- [Memantau peristiwa untuk Amazon Redshift Data API di Amazon EventBridge](#)

Memantau peristiwa untuk Amazon Redshift Data API di Amazon EventBridge

Anda dapat memantau peristiwa API Data di EventBridge, yang mengirimkan aliran data real-time dari aplikasi, aplikasi software-as-a-service (SaaS), dan layanan Anda sendiri. AWS EventBridge merutekan data tersebut ke target seperti AWS Lambda dan Amazon SNS. Peristiwa ini sama dengan yang muncul di CloudWatch Peristiwa, yang memberikan aliran peristiwa sistem yang mendekati waktu nyata yang menggambarkan perubahan sumber daya. AWS Acara dikirim ke akun yang berisi database Amazon Redshift. Misalnya, jika Anda berperan di akun lain, acara akan dikirim ke akun tersebut. Untuk informasi selengkapnya, lihat [EventBridge Acara Amazon](#) di Panduan EventBridge Pengguna Amazon. .

Peristiwa API data dikirim saat operasi `ExecuteStatement` atau `BatchExecuteStatement` API menetapkan `WithEvent` opsi ke `true`. `stateBidang` acara berisi salah satu nilai berikut:

- DIBATALKAN - Proses kueri dihentikan oleh pengguna.
- GAGAL - Query run gagal.
- SELESAI - Kueri telah selesai berjalan.

Acara disampaikan secara terjamin. Untuk informasi selengkapnya, lihat [Acara dari AWS layanan](#) di Panduan EventBridge Pengguna Amazon.

Contoh untuk acara selesai Data API

Contoh berikut menunjukkan peristiwa untuk Data API saat operasi `ExecuteStatement` API selesai. Dalam contoh ini, sebuah pernyataan bernama `test.testtable` selesai berjalan.

```
{
  "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  
  }  
}
```

Grup parameter Amazon Redshift

Gambaran Umum

Di Amazon Redshift, Anda mengaitkan grup parameter dengan setiap cluster yang Anda buat. Grup parameter adalah sekelompok parameter yang berlaku untuk semua database yang Anda buat di cluster. Parameter ini mengkonfigurasi pengaturan database seperti batas waktu kueri dan gaya tanggal.

Tentang grup parameter

Setiap grup parameter memiliki beberapa parameter untuk mengkonfigurasi pengaturan untuk database. Daftar parameter yang tersedia tergantung pada keluarga kelompok parameter tempat grup parameter berada. Keluarga grup parameter adalah versi mesin Amazon Redshift yang menerapkan parameter dalam grup parameter. Format nama keluarga grup parameter adalah `redshift-version` di mana *versi* adalah versi mesin. Misalnya, versi mesin saat ini adalah `redshift-1.0`.

Amazon Redshift menyediakan satu grup parameter default untuk setiap keluarga grup parameter. Grup parameter default memiliki nilai preset untuk masing-masing parameternya, dan tidak dapat dimodifikasi. Format nama grup parameter default adalah `default.parameter_group_family`, di mana *parameter_group_family* adalah versi mesin tempat grup parameter berada. Misalnya, grup parameter default untuk `redshift-1.0` versi diberi nama `default.redshift-1.0`.

Note

Saat ini, `redshift-1.0` adalah satu-satunya versi mesin Amazon Redshift. Akibatnya, `default.redshift-1.0` adalah satu-satunya kelompok parameter default.

Jika Anda ingin menggunakan nilai parameter yang berbeda dari grup parameter default, Anda harus membuat grup parameter khusus dan kemudian mengaitkan cluster Anda dengannya. Awalnya, nilai parameter dalam grup parameter kustom sama seperti pada grup parameter default. Awal `source` untuk semua parameter adalah `engine-default` karena nilainya telah ditetapkan oleh Amazon Redshift. Setelah Anda mengubah nilai parameter, `source` perubahan `user` untuk menunjukkan bahwa nilai telah dimodifikasi dari nilai defaultnya.

Note

Konsol Amazon Redshift tidak menampilkan setiap `source` parameter. Anda harus menggunakan Amazon Redshift API, the AWS CLI, atau salah satu AWS SDK untuk melihat `source`.


Untuk grup parameter yang Anda buat, Anda dapat mengubah nilai parameter kapan saja, atau Anda dapat mengatur ulang semua nilai parameter ke defaultnya. Anda juga dapat mengaitkan grup parameter yang berbeda dengan cluster. Dalam beberapa kasus, Anda dapat memodifikasi nilai parameter dalam grup parameter yang sudah dikaitkan dengan cluster atau mengaitkan grup parameter yang berbeda dengan cluster. Dalam kasus ini, Anda mungkin perlu me-restart cluster agar nilai parameter yang diperbarui diterapkan. Jika klaster gagal dan dimulai ulang oleh Amazon Redshift, perubahan Anda diterapkan pada saat itu. Perubahan tidak diterapkan jika klaster Anda dimulai ulang selama pemeliharaan. Untuk informasi selengkapnya, lihat [Sifat dinamis dan statis WLM](#).

Nilai parameter default

Tabel berikut menunjukkan nilai parameter default sekilas dengan link ke informasi yang lebih mendalam tentang setiap parameter. Ini adalah nilai default untuk keluarga grup `redshift-1.0` parameter.

Nama parameter	Nilai	Informasi lain
<code>auto_analisis</code>	<code>true</code>	auto_analisis di Panduan Pengembang Basis Data Amazon Redshift
<code>auto_mv</code>	<code>true</code>	Tampilan terwujud otomatis dalam Panduan Pengembang Basis Data Amazon Redshift
<code>datestyle</code>	<code>ISO, MDY</code>	datestyle di Panduan Pengembang Database Amazon Redshift
<code>enable_case_sensitive_identifier</code>	<code>false</code>	enable_case_sensitive_identifier di Panduan Pengembang Basis Data Amazon Redshift

Nama parameter	Nilai	Informasi lain
enable_user_activity_logging	false	Pencatatan audit basis data dalam panduan ini
extra_float_digits	0	extra_float_digits di Panduan Pengembang Basis Data Amazon Redshift
max_concurrency_scaling_clusters	1	max_concurrency_scaling_clusters di Panduan Pengembang Basis Data Amazon Redshift
query_group	default	query_group di Panduan Pengembang Basis Data Amazon Redshift
require_ssl	false	Mengkonfigurasi opsi keamanan untuk koneksi dalam panduan ini
search_path	\$ pengguna, publik	search_path di Panduan Pengembang Basis Data Amazon Redshift
statement_timeout	0	statement_timeout di Panduan Pengembang Basis Data Amazon Redshift
wlm_json_configuration	[{"auto_wlm":true}]	Mengkonfigurasi manajemen beban kerja dalam panduan ini
gunakan_fips_ssl	false	Aktifkan mode SSL yang sesuai dengan FIPS hanya jika sistem Anda harus sesuai dengan FIPS.

 Note

max_cursor_result_set_size Parameter tidak digunakan lagi. Untuk informasi selengkapnya tentang ukuran set hasil kursor, lihat Batasan [kursor di Panduan Pengembang Database Amazon Redshift](#).

Anda dapat mengganti sementara parameter dengan menggunakan SET perintah dalam database. SETPerintah mengesampingkan parameter untuk durasi sesi Anda saat ini saja. Selain parameter yang tercantum dalam tabel sebelumnya, Anda juga dapat menyesuaikan jumlah slot sementara dengan mengatur `wlm_query_slot_count` di database. `wlm_query_slot_count`Parameter tidak tersedia untuk konfigurasi dalam grup parameter. Untuk informasi selengkapnya tentang menyesuaikan jumlah slot, lihat [wlm_query_slot_count](#) di Panduan Pengembang Database Amazon Redshift. Untuk informasi selengkapnya tentang mengganti sementara parameter lain, lihat [Memodifikasi konfigurasi server di Panduan Pengembang](#) Database Amazon Redshift.

Mengkonfigurasi nilai parameter menggunakan AWS CLI

Untuk mengonfigurasi parameter Amazon Redshift dengan menggunakan AWS CLI, Anda menggunakan `modify-cluster-parameter-group` perintah untuk grup parameter tertentu. Anda menentukan kelompok parameter untuk memodifikasiparameter-group-name. Anda menggunakan parameters parameter (untuk `modify-cluster-parameter-group` perintah) untuk menentukan pasangan nama/nilai untuk setiap parameter yang ingin Anda modifikasi dalam kelompok parameter.

Note

Ada pertimbangan khusus saat mengkonfigurasi `wlm_json_configuration` parameter dengan menggunakan AWS CLI. Contoh di bagian ini berlaku untuk semua parameter kecuali `wlm_json_configuration`. Untuk informasi selengkapnya tentang mengonfigurasi `wlm_json_configuration` dengan menggunakan AWS CLI, lihat [Mengkonfigurasi manajemen beban kerja](#).

Setelah Anda memodifikasi nilai parameter, Anda harus me-reboot cluster apa pun yang terkait dengan grup parameter yang dimodifikasi. Status cluster ditampilkan `applying` untuk ParameterApplyStatus sementara nilai-nilai sedang diterapkan, dan kemudian `pending-reboot` setelah nilai-nilai telah diterapkan. Setelah Anda reboot, database di cluster Anda mulai menggunakan nilai parameter baru. Untuk informasi selengkapnya tentang me-reboot cluster, lihat [Melakukan boot ulang klaster](#)

Note

`wlm_json_configuration`Parameter berisi beberapa properti yang dinamis dan tidak mengharuskan Anda untuk me-reboot cluster terkait untuk perubahan yang akan diterapkan.

Untuk informasi selengkapnya tentang properti dinamis dan statis, lihat [Sifat dinamis dan statis WLM](#).

Sintaksis

Sintaks berikut menunjukkan cara menggunakan `modify-cluster-parameter-group` perintah untuk mengkonfigurasi parameter. Anda menentukan *parameter_group_name* dan *mengganti parameter_name* dan *parameter_value dengan parameter aktual untuk dimodifikasi dan nilai* untuk parameter tersebut. Jika Anda ingin memodifikasi lebih dari satu parameter pada saat yang sama, pisahkan setiap parameter dan nilai yang ditetapkan dari parameter berikutnya dengan spasi.

```
aws redshift modify-cluster-parameter-group --parameter-group-name parameter_group_name
--parameters ParameterName=parameter_name,ParameterValue=parameter_value
```

Contoh

Contoh berikut menunjukkan cara mengkonfigurasi `statement_timeout` dan `enable_user_activity_logging` parameter untuk kelompok `myclusterparametergroup` parameter.

Note

Untuk tujuan keterbacaan, contoh ditampilkan pada beberapa baris, tetapi sebenarnya AWS CLI ini adalah satu baris.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name myclusterparametergroup
--parameters ParameterName=statement_timeout,ParameterValue=20000
ParameterName=enable_user_activity_logging,ParameterValue=true
```

Anda dapat mengelola grup parameter menggunakan konsol. Untuk informasi selengkapnya, lihat [Mengelola grup parameter menggunakan konsol](#).

Mengkonfigurasi manajemen beban kerja

Di Amazon Redshift, Anda menggunakan manajemen beban kerja (WLM) untuk menentukan jumlah antrian kueri yang tersedia, dan cara kueri dirutekan ke antrian tersebut untuk diproses. WLM adalah bagian dari konfigurasi grup parameter. Sebuah cluster menggunakan konfigurasi WLM yang ditentukan dalam kelompok parameter terkait.

Saat Anda membuat grup parameter, konfigurasi WLM default berisi satu antrian yang dapat menjalankan hingga lima kueri secara bersamaan. Anda dapat menambahkan antrian tambahan dan mengkonfigurasi properti WLM di masing-masing jika Anda ingin lebih banyak kontrol atas pemrosesan kueri. Setiap antrian yang Anda tambahkan memiliki konfigurasi WLM default yang sama hingga Anda mengonfigurasi propertinya.

Saat Anda menambahkan antrian tambahan, antrian terakhir dalam konfigurasi adalah antrian default. Kecuali kueri dirutekan ke antrian lain berdasarkan kriteria dalam konfigurasi WLM, itu diproses oleh antrian default. Anda dapat menentukan mode dan tingkat konkurensi (slot kueri) untuk antrian default, tetapi Anda tidak dapat menentukan grup pengguna atau grup kueri untuk antrian default.

Seperti parameter lainnya, Anda tidak dapat memodifikasi konfigurasi WLM di grup parameter default. Cluster yang terkait dengan grup parameter default selalu menggunakan konfigurasi WLM default. Untuk memodifikasi konfigurasi WLM, buat grup parameter baru dan kemudian kaitkan grup parameter itu dengan cluster apa pun yang memerlukan konfigurasi WLM kustom Anda.

Sifat dinamis dan statis WLM

Properti konfigurasi WLM bersifat dinamis atau statis. Anda dapat menerapkan properti dinamis ke database tanpa reboot cluster, tetapi properti statis memerlukan reboot cluster agar perubahan diterapkan. Untuk informasi selengkapnya tentang properti statis dan dinamis, lihat properti [konfigurasi dinamis dan statis WLM](#).

Properti untuk parameter `wlm_json_configuration`

Anda dapat mengonfigurasi WLM dengan menggunakan konsol Amazon Redshift, AWS CLI Amazon Redshift API, atau salah satu SDK. AWS Konfigurasi WLM menggunakan beberapa properti untuk menentukan perilaku antrian, seperti alokasi memori di seluruh antrian, jumlah kueri yang dapat berjalan secara bersamaan dalam antrian, dan sebagainya.

Note

Properti berikut muncul dengan nama konsol Amazon Redshift mereka, dengan nama properti JSON yang sesuai dalam deskripsi.

Tabel berikut merangkum apakah properti berlaku untuk WLM otomatis atau WLM manual.

Properti WLM	WLM otomatis	Panduan WLM
WLM otomatis	Ya	Ya
Aktifkan akselerasi kueri singkat	Ya	Ya
Waktu berjalan maksimum untuk kueri singkat	Ya	Ya
Prioritas	Ya	Tidak
Jenis antrian	Ya	Ya
Nama antrian	Ya	Ya
Mode Penskalaan Konkurensi	Ya	Ya
Konkurensi	Tidak	Ya
Grup pengguna	Ya	Ya
Wildcard grup pengguna	Ya	Ya
Grup kueri	Ya	Ya
Wildcard grup kueri	Ya	Ya
Peran pengguna	Ya	Ya
Wildcard peran pengguna	Ya	Ya
Waktu habis	Tidak	Dihentikan

Properti WLM	WLM otomatis	Panduan WLM
Memori	Tidak	Ya
Aturan Pemantauan Kueri	Ya	Ya

Daftar berikut menjelaskan properti WLM yang dapat Anda konfigurasi.

WLM otomatis

Auto WLM diatur untuk `true` mengaktifkan WLM otomatis. WLM otomatis menetapkan nilai untuk `Concurrency` pada main dan `Memory (%)` ke. Auto Amazon Redshift mengelola konkurensi kueri dan alokasi memori. Nilai default-nya `true`.

Properti JSON: `auto_wlm`

Aktifkan akselerasi kueri singkat

Akselerasi kueri singkat (SQA) memprioritaskan kueri jangka pendek yang dipilih sebelum kueri yang berjalan lebih lama. SQA mengeksekusi kueri jangka pendek di ruang khusus, sehingga kueri SQA tidak dipaksa untuk menunggu dalam antrian di belakang kueri yang lebih panjang. Dengan SQA, kueri jangka pendek mulai dijalankan lebih cepat dan pengguna melihat hasilnya lebih cepat. Ketika Anda mengaktifkan SQA, Anda juga dapat menentukan waktu berjalan maksimum untuk kueri singkat. Untuk mengaktifkan SQA, tentukan `true`. Nilai default-nya `false`. Pengaturan ini diterapkan untuk setiap kelompok parameter daripada antrian.

Properti JSON: `short_query_queue`

Waktu berjalan maksimum untuk kueri singkat

Saat Anda mengaktifkan SQA, Anda dapat menentukan 0 untuk membiarkan WLM secara dinamis mengatur waktu berjalan maksimum untuk kueri singkat. Atau, Anda dapat menentukan nilai 1-20 detik, dalam milidetik. Nilai default-nya adalah 0.

Properti JSON: `max_execution_time`

Prioritas

Prioritas menetapkan prioritas kueri yang berjalan dalam antrian. Untuk mengatur prioritas, mode WLM harus diatur ke Auto WLM; artinya, harus. `auto_wlm true` Nilai prioritas dapat berupa `highest, high, normal, low, dan lowest`. Nilai default-nya `normal`.

Properti JSON: `priority`

Jenis antrian

Jenis antrian menunjuk antrian seperti yang digunakan baik oleh Auto WLM atau Manual WLM. Setel `queue_type` ke salah satu `auto` atau `manual`. Jika tidak ditentukan, default-nya adalah `manual`.

Properti JSON: `queue_type`

Nama antrian

Nama antrian. Anda dapat mengatur nama antrian berdasarkan kebutuhan bisnis Anda. Nama antrian harus unik dalam konfigurasi WLM, hingga 64 karakter alfanumerik, garis bawah atau spasi, dan tidak dapat berisi tanda kutip. Misalnya, jika Anda memiliki antrian untuk kueri ETL Anda, Anda dapat menamainya. `ETL_queue` Nama ini digunakan dalam metrik, nilai tabel sistem, dan konsol Amazon Redshift untuk mengidentifikasi antrian. Kueri dan laporan yang menggunakan nama dari sumber-sumber ini harus dapat menangani perubahan nama. Sebelumnya, nama antrian dihasilkan oleh Amazon Redshift. Nama default antrian adalah `Queue 1`, `Queue 2`, ke antrian terakhir bernama. `Default_queue`

Important

Jika Anda mengubah nama antrian, nilai `QueueName` dimensi metrik antrian WLM (seperti, `WLM`, `QueueWait Waktu WLM`, `WLMQueueLength`, `WLM`, `WLM`, dan sebagainya `QueriesCompletedPerSecond`) juga berubah. `QueryDuration` `RunningQueries` Jadi, jika Anda mengubah nama antrian, Anda mungkin perlu mengubah CloudWatch alarm yang telah Anda atur.

Properti JSON: `name`

Mode Penskalaan Konkurensi

Untuk mengaktifkan penskalaan konkurensi pada antrian, setel mode Penskalaan Konkurensi ke. `auto` Ketika jumlah kueri yang dirutekan ke antrian melebihi konkurensi antrian yang dikonfigurasi, kueri yang memenuhi syarat akan masuk ke klaster penskalaan. Ketika slot tersedia, kueri berjalan di cluster utama. Nilai default-nya `off`.

Properti JSON: `concurrency_scaling`

Konkurensi

Jumlah kueri yang dapat berjalan secara bersamaan dalam antrian WLM manual. Properti ini hanya berlaku untuk WLM manual. Jika penskalaan konkurensi diaktifkan, kueri yang memenuhi syarat akan masuk ke kluster penskalaan saat antrian mencapai tingkat konkurensi (slot kueri). Jika penskalaan konkurensi tidak diaktifkan, kueri menunggu dalam antrian sampai slot tersedia. Kisarannya antara 1 dan 50.

Properti JSON: `query_concurrency`

Grup Pengguna

Daftar nama grup pengguna yang dipisahkan koma. Ketika anggota grup pengguna menjalankan kueri dalam database, kueri mereka dirutekan ke antrian yang terkait dengan grup pengguna mereka.

Properti JSON: `user_group`

Grup Pengguna Wildcard

Nilai Boolean yang menunjukkan apakah akan mengaktifkan wildcard untuk grup pengguna. Jika ini 0, wildcard dinonaktifkan; jika ini adalah 1, wildcard diaktifkan. Ketika wildcard diaktifkan, Anda dapat menggunakan "*" atau "?" untuk menentukan beberapa grup pengguna saat menjalankan kueri. Untuk informasi selengkapnya, lihat [Wildcard](#).

Properti JSON: `user_group_wild_card`

Grup Kueri

Daftar grup kueri yang dipisahkan koma. Saat anggota grup kueri menjalankan kueri dalam database, kueri mereka dirutekan ke antrian yang terkait dengan grup kueri mereka.

Properti JSON: `query_group`

Wildcard Grup Kueri

Nilai Boolean yang menunjukkan apakah akan mengaktifkan wildcard untuk grup kueri. Jika ini 0, wildcard dinonaktifkan; jika ini adalah 1, wildcard diaktifkan. Ketika wildcard diaktifkan, Anda dapat menggunakan "*" atau "?" untuk menentukan beberapa grup kueri saat menjalankan kueri. Untuk informasi selengkapnya, lihat [Wildcard](#).

Properti JSON: `query_group_wild_card`

Peran Pengguna

Daftar peran pengguna yang dipisahkan koma. Ketika anggota dengan peran pengguna tersebut menjalankan kueri dalam database, kueri mereka dirutekan ke antrian yang terkait dengan peran pengguna mereka. Untuk informasi selengkapnya tentang peran pengguna, lihat [Kontrol akses berbasis peran \(RBAC\)](#).

Properti JSON: `user_role`

Peran Pengguna Wildcard

Nilai Boolean yang menunjukkan apakah akan mengaktifkan wildcard untuk grup kueri. Jika ini 0, wildcard dinonaktifkan; jika ini adalah 1, wildcard diaktifkan. Ketika wildcard diaktifkan, Anda dapat menggunakan "*" atau "?" untuk menentukan beberapa grup kueri saat menjalankan kueri. Untuk informasi selengkapnya, lihat [Wildcard](#).

Properti JSON: `user_role_wild_card`

Batas waktu (ms)

WLM timeout (`max_execution_time`) tidak digunakan lagi. Ini tidak tersedia saat menggunakan WLM otomatis. Sebagai gantinya, buat aturan pemantauan kueri (QMR) menggunakan `query_execution_time` untuk membatasi waktu eksekusi yang telah berlalu untuk kueri. Untuk informasi selengkapnya, lihat aturan [pemantauan kueri WLM](#).

Waktu maksimum, dalam milidetik, kueri dapat berjalan sebelum dibatalkan. Dalam beberapa kasus, kueri hanya-baca, seperti pernyataan SELECT, mungkin dibatalkan karena batas waktu WLM. Dalam kasus ini, WLM mencoba merutekan kueri ke antrian pencocokan berikutnya berdasarkan aturan penetapan antrian WLM. Jika kueri tidak cocok dengan definisi antrian lainnya, kueri dibatalkan; kueri tidak ditetapkan ke antrian default. Untuk informasi selengkapnya, lihat lompatan [antrian kueri WLM](#). Batas waktu WLM tidak berlaku untuk kueri yang telah mencapai status. `returning` Untuk melihat status kueri, lihat tabel sistem [STV_WLM_QUERY_STATE](#).

Properti JSON: `max_execution_time`

Memori (%)

Persentase memori untuk dialokasikan ke antrian. Jika Anda menentukan persentase memori untuk setidaknya satu antrian, Anda harus menentukan persentase untuk semua antrian lainnya, hingga total 100 persen. Jika alokasi memori Anda di bawah 100 persen di semua antrian, memori yang tidak terisi dikelola oleh layanan. Layanan sementara dapat memberikan memori yang tidak terisi ini ke antrian yang meminta memori tambahan untuk diproses.

Properti JSON: `memory_percent_to_use`

Aturan Pemantauan Kueri

Anda dapat menggunakan aturan pemantauan kueri WLM untuk terus memantau antrian WLM Anda untuk kueri berdasarkan kriteria, atau predikat, yang Anda tentukan. Misalnya, Anda dapat memantau kueri yang cenderung menggunakan sumber daya sistem yang berlebihan, dan kemudian memulai tindakan tertentu ketika kueri melebihi batas kinerja yang ditentukan.

Note

Jika Anda memilih untuk membuat aturan secara terprogram, kami sangat menyarankan menggunakan konsol untuk menghasilkan JSON yang Anda sertakan dalam definisi grup parameter.

Anda mengaitkan aturan pemantauan kueri dengan antrian kueri tertentu. Anda dapat memiliki hingga 25 aturan per antrian, dan batas total untuk semua antrian adalah 25 aturan.

Properti JSON: `rules`

Hirarki properti JSON:

```
rules
  rule_name
  predicate
    metric_name
    operator
    value
  action
    value
```

Untuk setiap aturan, Anda menentukan properti berikut:

- `rule_name`— Nama aturan harus unik dalam konfigurasi WLM. Nama aturan dapat mencapai 32 karakter alfanumerik atau garis bawah, dan tidak dapat berisi spasi atau tanda kutip.
- `predicate`— Anda dapat memiliki hingga tiga predikat per aturan. Untuk setiap predikat, tentukan properti berikut.
 - `metric_name`— Untuk daftar metrik, lihat Metrik [pemantauan kueri di Panduan Pengembang Database Amazon Redshift](#).
 - `operator` Operasi adalah `=`, `<`, dan `>`.

- `value`— Nilai ambang batas untuk metrik tertentu yang memicu tindakan.
- `action`— Setiap aturan dikaitkan dengan satu tindakan. Tindakan yang valid adalah:
 - `log`
 - `hop` (hanya tersedia dengan WLM manual)
 - `abort`
 - `change_query_priority` (hanya tersedia dengan WLM otomatis)

Contoh berikut menunjukkan JSON untuk aturan pemantauan query WLM bernama `rule_1`, dengan dua predikat dan tindakan. `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"
  }
]
```

Untuk informasi selengkapnya tentang masing-masing properti dan strategi untuk mengonfigurasi antrian kueri, lihat [Menerapkan manajemen beban kerja](#) di Panduan Pengembang Database Amazon Redshift.

Mengkonfigurasi parameter `wlm_json_configuration` menggunakan AWS CLI

Untuk mengkonfigurasi WLM, Anda memodifikasi parameter. `wlm_json_configuration` Ukuran maksimum nilai `wlm_json_configuration` properti adalah 8000 karakter. Nilai diformat dalam

JavaScript Object Notation (JSON). Jika Anda mengonfigurasi WLM menggunakan AWS CLI, Amazon Redshift API, atau salah satu SDK, gunakan bagian lainnya untuk mempelajari cara membuat struktur JSON untuk parameter. `wlm_json_configuration`

Note

Jika Anda mengonfigurasi WLM dengan menggunakan konsol Amazon Redshift, Anda tidak perlu memahami pemformatan JSON karena konsol menyediakan cara mudah untuk menambahkan antrian dan mengonfigurasi propertinya. Untuk informasi selengkapnya tentang mengonfigurasi WLM menggunakan konsol, lihat [Mengubah grup parameter](#)

Contoh

Contoh berikut adalah konfigurasi WLM default, yang mendefinisikan satu antrian dengan WLM otomatis.

```
{
  "auto_wlm": true
}
```

Contoh

Contoh berikut adalah konfigurasi WLM kustom, yang mendefinisikan satu antrian WLM manual dengan tingkat konkurensi (slot kueri) lima.

```
{
  "query_concurrency": 5
}
```

Sintaksis

Konfigurasi WLM default sangat sederhana, dengan hanya antrian dan satu properti. Anda dapat menambahkan lebih banyak antrian dan mengkonfigurasi beberapa properti untuk setiap antrian dalam struktur JSON. Sintaks berikut mewakili struktur JSON yang Anda gunakan untuk mengkonfigurasi beberapa antrian dengan beberapa properti:

```
[
  {
```



```
"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",
      ...
    }
  ]"
}
```

Dalam contoh sebelumnya, properti representatif yang dimulai dengan q1 adalah objek dalam array untuk antrian pertama. Masing-masing objek ini adalah pasangan nama/nilai; name dan value bersama-sama mengatur properti WLM untuk antrian pertama. Properti representatif yang dimulai dengan q2 adalah objek dalam array untuk antrian kedua. Jika Anda memerlukan lebih banyak antrian, Anda menambahkan array lain untuk setiap antrian tambahan dan mengatur properti untuk setiap objek.

Ketika Anda memodifikasi konfigurasi WLM, Anda harus menyertakan seluruh struktur untuk antrian Anda, bahkan jika Anda hanya ingin mengubah satu properti dalam antrian. Ini karena seluruh struktur JSON diteruskan sebagai string sebagai nilai untuk `wlm_json_configuration` parameter.

Memformat perintah AWS CLI

`wlm_json_configuration`Parameter memerlukan format tertentu saat Anda menggunakan file AWS CLI. Format yang Anda gunakan tergantung pada sistem operasi klien Anda. Sistem operasi memiliki cara yang berbeda untuk melampirkan struktur JSON sehingga diteruskan dengan benar dari baris perintah. Untuk detail tentang cara membuat perintah yang sesuai di sistem operasi Linux, Mac OS X, dan Windows, lihat bagian berikut. Untuk informasi selengkapnya tentang perbedaan dalam melampirkan struktur data JSON secara umum, lihat [Mengutip string](#) di Panduan Pengguna. AWS CLI AWS Command Line Interface

Contoh

Contoh perintah berikut mengkonfigurasi WLM manual untuk kelompok parameter yang disebut `example-parameter-group`. Konfigurasi ini memungkinkan akselerasi kueri pendek dengan waktu berjalan maksimum untuk kueri pendek yang disetel ke 0, yang menginstruksikan WLM untuk mengatur nilai secara dinamis. `ApplyType` Pengaturannya adalah `dynamic`. Pengaturan ini berarti bahwa setiap perubahan yang dibuat pada properti dinamis dalam parameter diterapkan segera kecuali perubahan statis lainnya telah dilakukan pada konfigurasi. Konfigurasi mendefinisikan tiga antrian dengan yang berikut:

- Antrian pertama memungkinkan pengguna untuk menentukan `report` sebagai label (seperti yang ditentukan dalam `query_group` properti) dalam kueri mereka untuk membantu dalam merutekan kueri ke antrian tersebut. Pencarian wildcard diaktifkan untuk `report*` label, sehingga label tidak perlu tepat untuk kueri yang akan diarahkan ke antrian. Misalnya, `reports` dan `reporting` keduanya cocok dengan grup kueri ini. Antrian dialokasikan 25 persen dari total memori di semua antrian, dan dapat menjalankan hingga empat kueri pada saat yang bersamaan. Kueri dibatasi hingga waktu maksimum 20000 milidetik (ms). `mode` diatur ke `auto`, jadi ketika slot kueri antrian penuh kueri yang memenuhi syarat dikirim ke cluster penskalaan.
- Antrian kedua memungkinkan pengguna yang merupakan anggota `admin` atau `dba` grup dalam database untuk mengarahkan kueri mereka ke antrian untuk diproses. Pencarian wildcard dinonaktifkan untuk grup pengguna, sehingga pengguna harus dicocokkan persis dengan grup dalam database agar kueri mereka dialihkan ke antrian. Antrian dialokasikan 40 persen dari total memori di semua antrian, dan dapat menjalankan hingga lima kueri pada saat yang sama. `mode` diatur ke `off`, sehingga semua kueri yang dikirim oleh anggota `admin` atau grup `dba` berjalan di cluster utama.
- Antrian terakhir dalam konfigurasi adalah antrian default. Antrian ini dialokasikan 35 persen dari total memori di semua antrian, dan dapat memproses hingga lima kueri sekaligus. `Mode` diatur ke `auto`.

Note

Contoh ditampilkan pada beberapa baris untuk tujuan demonstrasi. Perintah yang sebenarnya seharusnya tidak memiliki jeda baris.

```
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}
]'
```

Berikut ini adalah contoh konfigurasi aturan pemantauan kueri WLM untuk konfigurasi WLM otomatis. Contoh membuat grup parameter bernama `example-monitoring-rules`. Konfigurasi mendefinisikan tiga antrian yang sama seperti contoh sebelumnya, tetapi `query_concurrency` dan tidak `memory_percent_to_use` ditentukan lagi. Konfigurasi juga menambahkan aturan dan prioritas kueri berikut:

- Antrian pertama mendefinisikan aturan bernama `rule_1`. Aturan ini memiliki dua predikat: `query_cpu_time > 10000000` dan `query_blocks_read > 1000`. Tindakan aturannya adalah `log`. Prioritas antrian ini adalah `Normal`.
- Antrian kedua mendefinisikan aturan bernama `rule_2`. Aturan ini memiliki dua predikat: `query_execution_time > 600000000` dan `scan_row_count > 1000000000`. Tindakan aturannya adalah `abort`. Prioritas antrian ini adalah `Highest`.
- Antrian terakhir dalam konfigurasi adalah antrian default. Prioritas antrian ini adalah `Low`.

Note

Contoh ditampilkan pada beberapa baris untuk tujuan demonstrasi. Perintah yang sebenarnya seharusnya tidak memiliki jeda baris.

```
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
} ]'

```

Mengkonfigurasi WLM dengan menggunakan AWS CLI di baris perintah dengan file JSON

Anda dapat memodifikasi `wlm_json_configuration` parameter menggunakan AWS CLI dan meneruskan nilai `parameters` argumen sebagai file JSON.

```
aws redshift modify-cluster-parameter-group --parameter-group-name
myclusterparaametergroup --parameters file://modify_pg.json
```

Argumen untuk `--parameters` disimpan dalam file `modify_pg.json`. Lokasi file ditentukan dalam format untuk sistem operasi Anda. Untuk informasi selengkapnya, lihat [Memuat parameter dari file](#). Berikut ini menunjukkan contoh isi file `modify_pg.json` 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"
  }
]
```

Aturan untuk mengkonfigurasi WLM dengan menggunakan baris perintah AWS CLI pada sistem operasi Linux dan macOS X

Ikuti aturan ini untuk menjalankan AWS CLI perintah dengan parameter pada satu baris:

- Seluruh struktur JSON harus dilampirkan dalam tanda kutip tunggal (') dan satu set tanda kurung (()).

- Semua nama parameter dan nilai parameter harus diapit tanda kutip ganda (“”).
- Dalam `ParameterValue` nilai, Anda harus melampirkan seluruh struktur bersarang dalam tanda kutip ganda (“”) dan tanda kurung ([]).
- Dalam struktur bersarang, masing-masing properti dan nilai untuk setiap antrian harus diapit kurung kurawal ({}).
- Dalam struktur bersarang, Anda harus menggunakan karakter escape backslash (\) sebelum setiap tanda kutip ganda (“”).
- Untuk pasangan nama/nilai, titik dua (:) memisahkan setiap properti dari nilainya.
- Setiap pasangan nama/nilai dipisahkan dari yang lain dengan koma (,).
- Beberapa antrian dipisahkan oleh koma (,) antara akhir kurung kurawal antrian (}) dan awal kurung kurawal antrian berikutnya ({}).

Aturan untuk mengkonfigurasi WLM dengan menggunakan di PowerShell Windows AWS CLI pada sistem operasi Microsoft Windows

Ikuti aturan ini untuk menjalankan AWS CLI perintah dengan parameter pada satu baris:

- Seluruh struktur JSON harus dilampirkan dalam tanda kutip tunggal (') dan satu set tanda kurung ([]).
- Semua nama parameter dan nilai parameter harus diapit tanda kutip ganda (“”).
- Dalam `ParameterValue` nilai, Anda harus melampirkan seluruh struktur bersarang dalam tanda kutip ganda (“”) dan tanda kurung ([]).
- Dalam struktur bersarang, masing-masing properti dan nilai untuk setiap antrian harus diapit kurung kurawal ({}).
- Dalam struktur bersarang, Anda harus menggunakan karakter escape backslash (\) sebelum setiap tanda kutip ganda (“”) dan karakter escape garis miring terbalik (\). Persyaratan ini berarti bahwa Anda akan menggunakan tiga garis miring terbalik dan tanda kutip ganda untuk memastikan bahwa properti diteruskan dengan benar (\\”).
- Untuk pasangan nama/nilai, titik dua (:) memisahkan setiap properti dari nilainya.
- Setiap pasangan nama/nilai dipisahkan dari yang lain dengan koma (,).
- Beberapa antrian dipisahkan oleh koma (,) antara akhir kurung kurawal antrian (}) dan awal kurung kurawal antrian berikutnya ({}).

Aturan untuk mengkonfigurasi WLM dengan menggunakan command prompt pada sistem operasi Windows

Ikuti aturan ini untuk menjalankan AWS CLI perintah dengan parameter pada satu baris:

- Seluruh struktur JSON harus diapit tanda kutip ganda (") dan satu set tanda kurung ([]).
- Semua nama parameter dan nilai parameter harus diapit tanda kutip ganda (").
- Dalam ParameterValue nilai, Anda harus melampirkan seluruh struktur bersarang dalam tanda kutip ganda (") dan tanda kurung ([]).
- Dalam struktur bersarang, masing-masing properti dan nilai untuk setiap antrian harus diapit kurung kurawal ({}).
- Dalam struktur bersarang, Anda harus menggunakan karakter escape backslash (\) sebelum setiap tanda kutip ganda (") dan karakter escape garis miring terbalik (\). Persyaratan ini berarti bahwa Anda akan menggunakan tiga garis miring terbalik dan tanda kutip ganda untuk memastikan bahwa properti diteruskan dengan benar (\\").
- Untuk pasangan nama/nilai, titik dua (:) memisahkan setiap properti dari nilainya.
- Setiap pasangan nama/nilai dipisahkan dari yang lain dengan koma (,).
- Beberapa antrian dipisahkan oleh koma (,) antara akhir kurung kurawal antrian (}) dan awal kurung kurawal antrian berikutnya ({}).

Mengelola grup parameter menggunakan konsol

Anda dapat melihat, membuat, memodifikasi, dan menghapus grup parameter di konsol Amazon Redshift.

Anda dapat melihat salah satu grup parameter Anda untuk melihat ringkasan nilai untuk konfigurasi parameter dan manajemen beban kerja (WLM). Parameter grup muncul di tab Parameter, dan antrian beban kerja muncul di Manajemen Beban Kerja tab.

Membuat grup parameter

Jika Anda ingin mengatur nilai parameter yang berbeda dari grup parameter default, Anda dapat membuat grup parameter Anda sendiri,

Untuk membuat grup parameter

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Konfigurasi, lalu pilih Manajemen beban kerja untuk menampilkan halaman Manajemen beban kerja.
3. Pilih Buat untuk menampilkan jendela Buat grup parameter.
4. Masukkan nilai untuk nama grup Parameter dan Deskripsi.
5. Pilih Buat untuk membuat grup parameter.

Mengubah grup parameter

Anda dapat memodifikasi parameter untuk mengubah pengaturan parameter dan properti konfigurasi WLM.

Note

Anda tidak dapat mengubah grup parameter default.

Untuk memodifikasi grup parameter

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Konfigurasi, lalu pilih Manajemen beban kerja untuk menampilkan halaman Manajemen beban kerja.
3. Pilih grup parameter yang ingin Anda modifikasi untuk menampilkan halaman detail, dengan tab untuk Parameter dan manajemen Beban Kerja.
4. Pilih tab Parameter untuk melihat pengaturan parameter saat ini.
5. Pilih Edit parameter untuk mengaktifkan perubahan pengaturan parameter ini:
 - `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`

Untuk informasi selengkapnya tentang parameter ini, lihat [Grup parameter Amazon Redshift](#).

6. Masukkan perubahan Anda dan kemudian pilih Simpan untuk memperbarui grup parameter.

Untuk memodifikasi konfigurasi WLM untuk grup parameter

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Konfigurasi, lalu pilih Manajemen beban kerja untuk menampilkan halaman Manajemen beban kerja.
3. Pilih grup parameter yang ingin Anda modifikasi untuk menampilkan halaman detail dengan tab untuk Parameter dan manajemen Beban Kerja.
4. Pilih tab Manajemen beban kerja untuk melihat konfigurasi WLM saat ini.
5. Pilih Edit antrian beban kerja untuk mengedit konfigurasi WLM,
6. (Opsional) Pilih Aktifkan akselerasi kueri pendek untuk mengaktifkan akselerasi kueri pendek (SQA).


Saat Anda mengaktifkan SQA, Waktu berjalan maksimum untuk kueri singkat (1 hingga 20 detik) diatur ke Dinamis secara default. Untuk mengatur runtime maksimum ke nilai tetap, pilih nilai 1-20.

7. Lakukan satu atau beberapa hal berikut untuk mengubah konfigurasi antrian:
 - Pilih mode Switch WLM untuk memilih antara WLM Otomatis dan WLM Manual.

Dengan WLM Otomatis, Memori dan Konkurensi pada nilai utama diatur ke auto.


- Untuk membuat antrian, pilih Edit antrian beban kerja, lalu pilih Tambah Antrian.
- Untuk mengubah antrian, ubah nilai properti dalam tabel. Tergantung pada jenis antrian, properti dapat mencakup yang berikut:
 - Nama antrian dapat diubah.
 - Memori (%)
 - Konkurensi pada cluster utama
 - Mode penskalaan konkurensi dapat dimatikan atau otomatis
 - Batas waktu (ms)
 - Grup pengguna
 - Grup kueri
 - Peran pengguna

Untuk informasi selengkapnya tentang properti ini, lihat [Properti untuk parameter wlm_json_configuration](#).

 Important

Jika Anda mengubah nama antrian, nilai QueueName dimensi metrik antrian WLM (seperti, WLM, WLM, WLM, WLMQueueLength, WLMQueueWaitTime, dan sebagainyaQueriesCompletedPerSecond) juga berubah. QueryDuration RunningQueries Jadi, jika Anda mengubah nama antrian, Anda mungkin perlu mengubah CloudWatch alarm yang telah Anda atur.

- Untuk mengubah urutan antrian, pilih tombol panah Atas dan Bawah.
 - Untuk menghapus antrian, pilih Hapus di baris antrian dalam tabel.
8. (Opsional) Pilih Tunda perubahan dinamis hingga reboot agar perubahan diterapkan ke cluster setelah reboot berikutnya.

 Note

Beberapa perubahan memerlukan reboot cluster terlepas dari pengaturan ini. Untuk informasi selengkapnya, lihat [Sifat dinamis dan statis WLM](#).

9. Pilih Simpan.

Membuat atau memodifikasi aturan pemantauan kueri menggunakan konsol

Anda dapat menggunakan konsol Amazon Redshift untuk membuat dan memodifikasi aturan pemantauan kueri WLM. Aturan pemantauan kueri adalah bagian dari parameter konfigurasi WLM untuk grup parameter. Jika Anda memodifikasi aturan pemantauan kueri (QMR), perubahan terjadi secara otomatis tanpa perlu memodifikasi cluster. Untuk informasi selengkapnya, lihat aturan [pemantauan kueri WLM](#).

Saat Anda membuat aturan, Anda menentukan nama aturan, satu atau beberapa predikat, dan tindakan.

Saat Anda menyimpan konfigurasi WLM yang menyertakan aturan, Anda dapat melihat kode JSON untuk definisi aturan sebagai bagian dari JSON untuk parameter konfigurasi WLM.

Untuk membuat aturan pemantauan kueri

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Konfigurasi, lalu pilih Manajemen beban kerja untuk menampilkan halaman Manajemen beban kerja.
3. Pilih grup parameter yang ingin Anda modifikasi untuk menampilkan halaman detail dengan tab untuk Parameter dan manajemen Beban Kerja.
4. Pilih tab Manajemen beban kerja, dan pilih Edit antrian beban kerja untuk mengedit konfigurasi WLM,
5. Tambahkan aturan baru baik dengan menggunakan template yang telah ditentukan atau dari awal.

Untuk menggunakan template yang telah ditentukan, lakukan hal berikut:

1. Pilih Tambahkan aturan dari templat di grup Aturan pemantauan kueri. Daftar template aturan ditampilkan.
2. Pilih satu atau beberapa templat aturan. Ketika Anda memilih Simpan, WLM membuat satu aturan untuk setiap template yang Anda pilih.
3. Masukkan atau konfirmasi nilai untuk aturan, termasuk nama Aturan, Predikat, dan Tindakan.
4. Pilih Simpan.

Untuk menambahkan aturan baru dari awal, lakukan hal berikut:

1. Untuk menambahkan predikat tambahan, pilih Tambahkan predikat. Anda dapat memiliki hingga tiga predikat untuk setiap aturan. Jika semua predikat terpenuhi, WLM memicu tindakan terkait.
2. Pilih Tindakan. Setiap aturan memiliki satu tindakan.
3. Pilih Simpan.

Amazon Redshift menghasilkan parameter konfigurasi WLM Anda dalam format JSON dan menampilkannya di bagian JSON.

Menghapus grup parameter

Anda dapat menghapus grup parameter jika Anda tidak lagi membutuhkannya dan tidak terkait dengan cluster apa pun. Anda hanya dapat menghapus grup parameter khusus.

Untuk menghapus grup parameter

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Konfigurasi, lalu pilih Manajemen beban kerja untuk menampilkan halaman Manajemen beban kerja.
3. Untuk grup Parameter, pilih grup parameter yang ingin Anda ubah.

Note

Anda tidak dapat menghapus grup parameter default.

4. Pilih Hapus dan konfirmasi bahwa Anda ingin menghapus grup parameter.

Mengaitkan grup parameter dengan cluster

Saat Anda meluncurkan cluster, Anda harus mengaitkannya dengan grup parameter. Jika Anda ingin mengubah grup parameter nanti, Anda dapat memodifikasi cluster dan memilih grup parameter yang berbeda.

Mengelola grup parameter menggunakan API Amazon Redshift AWS CLI dan Amazon

Anda dapat menggunakan operasi Amazon Redshift berikut di grup parameter AWS CLI untuk mengelola.

- [buat-kluser-parameter-grup](#)
- [hapus-cluster-parameter-grup](#)
- [jelaskan-cluster-parameter](#)
- [jelaskan-cluster-parameter-grup](#)
- [jelaskan-default-cluster-parameter](#)
- [memodifikasi-cluster-parameter-grup](#)
- [reset-cluster-parameter-grup](#)

Anda dapat menggunakan operasi Amazon Redshift API berikut untuk mengelola grup parameter.

- [CreateClusterParameterGroup](#)
- [DeleteClusterParameterGroup](#)
- [DescribeClusterParameter](#)
- [DescribeClusterParameterGroups](#)
- [DescribeDefaultClusterParameters](#)
- [ModifyClusterParameterGroup](#)
- [ResetClusterParameterGroup](#)

Mengintegrasikan Amazon Redshift dengan Mitra AWS

Dengan bekerja sama dengan Amazon Redshift, Anda dapat berintegrasi dengan AWS Partner dari halaman detail Cluster di konsol Amazon Redshift. Dari halaman detail Cluster, Anda dapat mempercepat orientasi data ke gudang data Amazon Redshift AWS dengan aplikasi Partner. Anda juga dapat bergabung dan menganalisis data dari berbagai sumber bersama dengan data yang ada di cluster Anda. Sebelum menyelesaikan integrasi dengan Informatica, Anda harus menambahkan alamat IP mitra ke daftar lalu lintas masuk yang diizinkan. AWS Mitra berikut dapat berintegrasi dengan Amazon Redshift:

- [Datacoral](#)
- [Etleap](#)
- [Fivetran](#)
- [SnapLogic](#)
- [Jahitan](#)
- [Upsolver](#)
- [Matillion \(pratinjau\)](#)
- [Sisense \(pratinjau\)](#)
- [Thoughtspot](#)

AWS Mitra dapat berintegrasi dengan Amazon Redshift menggunakan operasi API Amazon Redshift AWS CLI atau Amazon. Untuk informasi selengkapnya, lihat Referensi AWS CLI Perintah atau Referensi API Amazon Redshift.

Mengintegrasikan dengan AWS Partner menggunakan konsol Amazon Redshift

Gunakan prosedur berikut untuk mengintegrasikan cluster dengan AWS Partner.

Untuk mengintegrasikan cluster Amazon Redshift dengan Partner AWS

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster.

3. Pilih cluster yang ingin Anda integrasikan.
4. Pilih Tambahkan integrasi mitra. Halaman Pilih mitra terbuka dengan detail tentang AWS Mitra yang tersedia.
5. Pilih AWS Mitra, lalu pilih Berikutnya.

Rincian lebih lanjut tentang AWS Partner yang dipilih muncul, bersama dengan detail tentang cluster yang Anda integrasikan. Bagian detail Cluster mencakup informasi yang Anda berikan di situs web AWS Mitra seperti pengenalan Cluster, Endpoint, nama Database, dan nama Pengguna (yang merupakan nama pengguna database). Informasi ini dikirim ke mitra yang Anda pilih.

6. Pilih Tambah mitra untuk membuka situs web AWS Mitra.
7. Konfigurasi integrasi dengan cluster Amazon Redshift Anda di situs web mitra. Di situs web mitra, Anda dapat memilih dan mengonfigurasi sumber data yang dimuat ke cluster Amazon Redshift Anda. Anda juga dapat menentukan transformasi ekstrak, pemuatan, dan transformasi (ELT) tambahan untuk memproses data bisnis Anda, menggabungkannya dengan kumpulan data lain, dan membangun tampilan konsolidasi untuk analisis dan pelaporan.

Anda dapat melihat dan mengelola integrasi AWS Partner dari tab Properties detail cluster. Bagian Integrasi mencantumkan nama Mitra yang dapat Anda gunakan untuk menautkan ke situs web AWS Mitra, Status integrasi, Database yang menerima data, dan koneksi terakhir yang berhasil yang mungkin telah memperbarui klaster.

Nilai status yang mungkin adalah sebagai berikut:

- Aktif — AWS Mitra dapat terhubung ke cluster dan menyelesaikan tugas yang dikonfigurasi.
- Tidak Aktif — Integrasi AWS Mitra tidak ada.
- Kegagalan runtime — AWS Partner dapat terhubung ke cluster tetapi tidak dapat menyelesaikan tugas yang dikonfigurasi.
- Kegagalan koneksi — AWS Mitra tidak dapat terhubung ke cluster.

Setelah Anda menghapus integrasi AWS Partner dari Amazon Redshift, data terus mengalir ke klaster Anda. Selesaikan penghapusan di situs web mitra.

Memuat data dengan AWS mitra

Selain mengintegrasikan mitra dengan cluster Amazon Redshift, Anda juga dapat memindahkan data dari lebih dari 30 sumber ke cluster Amazon Redshift menggunakan alat pemuatan data mitra

kami. Sebelum melakukannya, Anda harus menambahkan alamat IP mitra (ditemukan di bawah) ke daftar aturan masuk yang diizinkan. Untuk informasi selengkapnya tentang menambahkan aturan ke grup keamanan Amazon EC2, lihat [Mengotorisasi Lalu Lintas Masuk untuk Instans Anda di Panduan Pengguna Amazon EC2](#). Perhatikan bahwa meskipun alat Pemuat Data Informatica gratis, biaya masuknya data mungkin berlaku tergantung pada sumber data dan target yang Anda pilih.

Anda dapat memuat data dari mitra berikut:

- [Informatika — Alamat IP](#)

Untuk mengintegrasikan cluster Amazon Redshift dengan Informatica

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih integrasi AWS mitra, lalu pilih mitra yang ingin Anda integrasikan dengan cluster Anda.
3. Pilih Integrasi lengkap<partner-name>. Anda akan diarahkan ke situs integrasi mitra.
4. Masukkan detail yang diperlukan di situs mitra dan selesaikan integrasi.

Membeli node cadangan Amazon Redshift

Gambaran Umum

Di AWS, biaya yang Anda dapatkan untuk menggunakan Amazon Redshift didasarkan pada node komputasi. Setiap node komputasi ditagih dengan tarif per jam. Tarif per jam bervariasi tergantung pada faktor-faktor seperti wilayah, tipe node, dan apakah node menerima harga node sesuai permintaan atau harga node cadangan.

Harga node sesuai permintaan adalah opsi yang paling mahal, tetapi paling fleksibel di Amazon Redshift. Dengan tarif sesuai permintaan, Anda hanya dikenakan biaya untuk node komputasi yang Anda miliki di cluster yang sedang berjalan. Jika Anda mematikan atau menghapus klaster, Anda tidak lagi dikenakan biaya untuk node komputasi yang ada di cluster itu. Anda ditagih hanya untuk node komputasi yang Anda gunakan, dan tidak lebih. Tarif per jam yang dikenakan biaya untuk setiap node komputasi bervariasi tergantung pada faktor-faktor seperti wilayah dan tipe node.

Harga node cadangan lebih murah daripada harga sesuai permintaan karena node komputasi ditagih dengan tarif per jam diskon. Namun, untuk menerima tarif diskon ini, Anda harus membeli penawaran node yang dipesan. Ketika Anda membeli penawaran, Anda membuat reservasi. Reservasi menetapkan tarif diskon untuk setiap node yang Anda pesan selama reservasi. Tarif diskon dalam penawaran bervariasi tergantung pada faktor-faktor seperti wilayah, jenis node, durasi, dan opsi pembayaran.

Anda dapat menetapkan node sebagai node cadangan dengan memanggil operasi `PurchaseReservedNodeOffering` API atau memilih Purchase reserved node di konsol Amazon Redshift. Saat Anda membeli node yang dicadangkan, Anda harus menentukan AWS Region, tipe node, istilah, jumlah node, dan tipe penawaran untuk tipe node cadangan yang berlaku. Node cadangan hanya dapat digunakan di AWS Wilayah yang ditunjuk.

Topik ini membahas apa itu penawaran node cadangan dan bagaimana Anda dapat membelinya untuk mengurangi biaya menjalankan cluster Amazon Redshift Anda. Topik ini membahas tarif secara umum sebagai sesuai permintaan atau diskon sehingga Anda dapat memahami konsep penetapan harga dan bagaimana harga memengaruhi penagihan. Untuk informasi selengkapnya tentang tarif tertentu, buka Harga [Amazon Redshift](#).

Tentang penawaran node yang dicadangkan

Jika Anda berniat untuk menjaga klaster Amazon Redshift Anda berjalan terus menerus untuk waktu yang lama, Anda harus mempertimbangkan untuk membeli penawaran node cadangan. Penawaran ini memberikan penghematan yang signifikan atas harga sesuai permintaan, tetapi mereka mengharuskan Anda untuk memesan node komputasi dan berkomitmen untuk membayar node tersebut untuk durasi satu tahun atau tiga tahun.

Node cadangan adalah konsep penagihan yang digunakan secara ketat untuk menentukan tarif di mana Anda dikenakan biaya untuk node. Reservasi node sebenarnya tidak membuat node apa pun untuk Anda. Anda dikenakan biaya untuk node cadangan terlepas dari penggunaan, yang berarti bahwa Anda harus membayar untuk setiap node yang Anda pesan selama durasi reservasi, terlepas dari apakah Anda memiliki node dalam klaster yang berjalan di mana tarif diskon berlaku atau tidak.

Pada tahap evaluasi proyek Anda atau ketika Anda mengembangkan bukti konsep, harga sesuai permintaan memberi Anda fleksibilitas untuk membayar saat Anda pergi, membayar hanya untuk apa yang Anda gunakan, dan berhenti membayar kapan saja dengan mematikan atau menghapus cluster. Setelah Anda menetapkan kebutuhan lingkungan produksi Anda dan memulai fase implementasi, Anda harus mempertimbangkan untuk memesan node komputasi dengan membeli satu atau lebih penawaran.

Penawaran dapat diterapkan ke satu atau lebih node komputasi. Anda menentukan jumlah node komputasi yang akan dipesan saat Anda membeli penawaran. Anda dapat memilih untuk membeli satu penawaran untuk beberapa node komputasi, atau Anda dapat memilih untuk membeli beberapa penawaran dan menentukan sejumlah node komputasi dalam setiap penawaran.

Misalnya, salah satu dari berikut ini adalah cara yang valid untuk membeli penawaran untuk tiga node komputasi:

- Beli satu penawaran dan tentukan tiga node komputasi.
- Beli dua penawaran, dan tentukan satu node komputasi untuk penawaran pertama dan dua node komputasi untuk penawaran kedua.
- Beli tiga penawaran, dan tentukan satu node komputasi untuk setiap penawaran.

Membandingkan harga di antara penawaran node yang dicadangkan

Amazon Redshift menyediakan beberapa opsi pembayaran untuk penawaran. Opsi pembayaran yang Anda pilih memengaruhi jadwal pembayaran dan tarif diskon yang dikenakan untuk reservasi. Semakin banyak Anda membayar di muka untuk reservasi, semakin baik penghematan keseluruhan.

Opsi pembayaran berikut tersedia untuk penawaran. Penawaran terdaftar dalam urutan dari penghematan paling sedikit hingga paling banyak dibandingkan tingkat permintaan.

Note

Anda dikenakan tarif per jam yang berlaku untuk setiap jam dalam durasi reservasi yang ditentukan, terlepas dari apakah Anda menggunakan node yang dipesan atau tidak. Opsi pembayaran hanya menentukan frekuensi pembayaran dan diskon yang akan diterapkan. Untuk informasi selengkapnya, lihat [Tentang penawaran node yang dicadangkan](#).

Membandingkan penawaran node yang dicadangkan

Opsi pembayaran	Jadwal pembayaran	Tabungan komparatif	Durasi	Biaya di muka	Biaya bulanan berulang
Tidak ada di muka	Angsuran bulanan selama reservasi. Tidak ada pembayaran di muka.	Sekitar 20 persen diskon atas tarif sesuai permintaan.	Jangka waktu satu tahun atau tiga tahun	Tidak ada	Ya
Sebagian di muka	Pembayaran dimuka sebagian, dan cicilan bulanan selama reservasi.	Diskon hingga 41 persen hingga 73 persen tergantung durasi.	Jangka waktu satu tahun atau tiga tahun	Ya	Ya
Semua di muka	Pembayaran dimuka penuh untuk	Diskon hingga 42 persen hingga 76	Jangka waktu	Ya	Tidak ada

Opsi pembayaran	Jadwal pembayaran	Tabungan komparatif	Durasi	Biaya di muka	Biaya bulanan berulang
	reservasi. Tidak ada biaya bulanan.	persen tergantung durasi.	satu tahun atau tiga tahun		

Opsi dan durasi tertentu tergantung pada ketersediaan.

Note

Jika sebelumnya Anda membeli penawaran Pemanfaatan Berat untuk Amazon Redshift, penawaran yang sebanding adalah penawaran Partial Upfront.

Cara kerja node yang dicadangkan

Dengan penawaran node cadangan, Anda membayar sesuai dengan ketentuan pembayaran seperti yang dijelaskan di bagian sebelumnya. Anda membayar dengan cara ini apakah Anda sudah memiliki cluster yang sedang berjalan atau Anda meluncurkan klaster setelah Anda memiliki reservasi.

Ketika Anda membeli penawaran, reservasi Anda memiliki status pembayaran-tertunda sampai reservasi diproses. Jika reservasi gagal diproses, status ditampilkan sebagai pembayaran gagal dan Anda dapat mencoba prosesnya lagi. Setelah reservasi Anda berhasil diproses, statusnya berubah menjadi aktif. Tarif diskon yang berlaku dalam reservasi Anda tidak berlaku untuk tagihan Anda sampai status berubah menjadi aktif. Setelah durasi reservasi berlalu, status berubah menjadi pensiunan tetapi Anda dapat terus mengakses informasi tentang reservasi untuk tujuan historis. Ketika reservasi dihentikan, klaster Anda terus berjalan tetapi Anda mungkin ditagih dengan tarif sesuai permintaan kecuali Anda memiliki reservasi lain yang menerapkan harga diskon ke node.

Node yang dicadangkan khusus untuk wilayah tempat Anda membeli penawaran. Jika Anda membeli penawaran dengan menggunakan konsol Amazon Redshift, pilih AWS wilayah tempat Anda ingin membeli penawaran, lalu selesaikan proses reservasi. Jika Anda membeli penawaran secara terprogram, wilayah ditentukan oleh titik akhir Amazon Redshift yang Anda sambungkan. Untuk informasi selengkapnya tentang wilayah Amazon Redshift, buka [Wilayah dan Titik Akhir](#) di Referensi Umum Amazon Web Services

Untuk memastikan bahwa tingkat diskon diterapkan ke semua node saat Anda meluncurkan klaster, pastikan bahwa wilayah, jenis node, dan jumlah node yang Anda pilih cocok dengan satu atau lebih reservasi aktif. Jika tidak, Anda akan dikenakan tarif sesuai permintaan untuk node yang tidak cocok dengan reservasi aktif.

Dalam klaster yang sedang berjalan, jika Anda melebihi jumlah node yang telah Anda pesan, Anda mulai menambah biaya untuk node tambahan tersebut dengan tarif sesuai permintaan. Akrual ini berarti Anda dapat dikenakan tarif yang bervariasi untuk node di cluster yang sama tergantung pada berapa banyak node yang telah Anda pesan. Anda dapat membeli penawaran lain untuk menutupi node tambahan tersebut, dan kemudian tarif diskon diterapkan ke node tersebut selama sisa durasi setelah status reservasi menjadi aktif.

Jika Anda mengubah ukuran cluster Anda menjadi tipe node yang berbeda dan Anda belum memesan node dari jenis itu, Anda akan dikenakan biaya pada tingkat permintaan. Anda dapat membeli penawaran lain dengan tipe node baru jika Anda ingin menerima tarif diskon untuk klaster yang diubah ukurannya. Namun, Anda juga terus membayar reservasi awal hingga durasinya berlalu. [Jika Anda perlu mengubah reservasi sebelum jangka waktu berakhir, harap buat kasus dukungan menggunakan Konsol.AWS](#)

Node cadangan dan penagihan terkonsolidasi

Manfaat harga dari Node Cadangan dibagikan ketika akun pembelian merupakan bagian dari serangkaian akun yang ditagih di bawah satu akun pembayar tagihan konsolidasi. Penggunaan per jam di semua sub-akun dikumpulkan di akun pembayar setiap bulan. Ini biasanya berguna untuk perusahaan di mana ada tim atau kelompok fungsional yang berbeda; kemudian, logika Node Cadangan normal diterapkan untuk menghitung tagihan. Untuk informasi selengkapnya, lihat [Penagihan Konsolidasi](#) di AWS Billing Panduan Pengguna.

Contoh simpul cadangan

Skenario di bagian ini menunjukkan bagaimana node memperoleh biaya berdasarkan tarif sesuai permintaan dan diskon menggunakan detail reservasi berikut:

- Wilayah: AS Barat (Oregon)
- Jenis Node: ra3.xlplus
- Opsi Pembayaran: Tidak Ada di Muka
- Durasi: satu tahun
- Jumlah Node Cadangan: 16

Contoh 1

Anda memiliki satu cluster di wilayah AS Barat (Oregon) dengan 20 node.

Dalam skenario ini, 16 node menerima tarif diskon dari reservasi, tetapi 4 node tambahan di cluster ditagih pada tingkat permintaan.

Contoh 2

Anda memiliki satu cluster di wilayah AS Barat (Oregon) dengan 12 node.

Dalam skenario ini, semua 12 node di cluster menerima tarif diskon dari reservasi. Namun, Anda juga membayar untuk node cadangan yang tersisa di reservasi meskipun saat ini Anda tidak memiliki klaster yang sedang berjalan yang mereka terapkan.

Contoh 3

Anda memiliki satu cluster di wilayah AS Barat (Oregon) dengan 12 node. Anda menjalankan cluster selama beberapa bulan dengan konfigurasi ini, dan kemudian Anda perlu menambahkan node ke cluster. Anda mengubah ukuran cluster, memilih jenis node yang sama dan menentukan total 16 node.

Dalam skenario ini, Anda ditagih tarif diskon untuk 16 node. Biaya Anda tetap sama untuk durasi setahun penuh karena jumlah node yang Anda miliki di cluster sama dengan jumlah node yang telah Anda pesan.

Contoh 4

Anda memiliki satu cluster di wilayah AS Barat (Oregon) dengan 16 node. Anda menjalankan cluster selama beberapa bulan dengan konfigurasi ini, dan kemudian Anda perlu menambahkan node. Anda mengubah ukuran cluster, memilih jenis node yang sama dan menentukan total 20 node.

Dalam skenario ini, Anda akan ditagih tarif diskon untuk semua node sebelum mengubah ukuran. Setelah mengubah ukuran, Anda akan ditagih tarif diskon untuk 16 node selama sisa tahun ini, dan Anda ditagih pada tingkat permintaan untuk 4 node tambahan yang Anda tambahkan ke cluster.

Contoh 5

Anda memiliki dua kelompok di wilayah AS Barat (Oregon). Salah satu cluster memiliki 6 node, dan yang lainnya memiliki 10 node.

Dalam skenario ini, Anda ditagih pada tingkat diskon untuk semua node karena jumlah total node di kedua cluster sama dengan jumlah node yang telah Anda pesan.

Contoh 6

Anda memiliki dua kelompok di wilayah AS Barat (Oregon). Salah satu cluster memiliki 4 node, dan yang lainnya memiliki 6 node.

Dalam skenario ini, Anda ditagih tarif diskon untuk 10 node yang Anda miliki dalam menjalankan cluster, dan Anda juga membayar tarif diskon untuk tambahan 6 node yang telah Anda pesan meskipun saat ini Anda tidak memiliki cluster berjalan yang mereka terapkan.

Membeli penawaran node cadangan dengan konsol Amazon Redshift

Anda menggunakan halaman Node Cadangan di konsol Amazon Redshift untuk membeli penawaran node cadangan, dan untuk melihat reservasi saat ini dan sebelumnya.

Setelah Anda membeli penawaran, daftar Node Cadangan menampilkan reservasi Anda dan detail masing-masing, seperti jenis node, jumlah node, dan status reservasi. Untuk informasi selengkapnya tentang detail reservasi, lihat [Cara kerja node yang dicadangkan](#).

Untuk membeli node yang dicadangkan

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster, lalu pilih Node cadangan untuk menampilkan daftar node yang dicadangkan.
3. Pilih Purchase reserved nodes untuk menampilkan halaman untuk memilih properti node yang ingin Anda beli.
4. Masukkan properti node, lalu pilih Purchase reserved nodes.

Untuk memutakhirkan node yang dicadangkan, gunakan file AWS CLI.

Anda tidak dapat mengonversi semua jenis node menjadi node yang dicadangkan, dan mungkin juga node cadangan yang ada tidak tersedia untuk pembaruan. Ini mungkin karena tipe node dihentikan. Hubungi dukungan pelanggan untuk memperbarui tipe node yang dihentikan.

Memutakhirkan node yang dicadangkan dengan AWS CLI

Untuk memutakhirkan reservasi node yang dipesan dengan AWS CLI

1. Dapatkan daftar ReservedNodeOffering ID untuk penawaran yang memenuhi persyaratan Anda untuk jenis pembayaran, jangka waktu, dan biaya. Contoh berikut menggambarkan langkah ini.

```
aws redshift get-reserved-node-exchange-offerings --reserved-node-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
{
  "ReservedNodeOfferings": [
    {
      "Duration": 31536000,
      "ReservedNodeOfferingId": "yyyyyyyy-yy-yy-yy-yyy-yyyyyyyyyyyy",
      "UsagePrice": 0.0,
      "NodeType": "dc2.large",
      "RecurringCharges": [
        {
          "RecurringChargeFrequency": "Hourly",
          "RecurringChargeAmount": 0.2
        }
      ],
      "CurrencyCode": "USD",
      "OfferingType": "No Upfront",
      "ReservedNodeOfferingType": "Regular",
      "FixedPrice": 0.0
    }
  ]
}
```

2. Panggil `accept-reserved-node-exchange` dan berikan ID untuk node cadangan DC1 yang ingin Anda tukarkan bersama dengan ReservedNodeOffering ID yang Anda peroleh pada langkah sebelumnya.

Contoh berikut menggambarkan langkah ini.

```
aws redshift accept-reserved-node-exchange --reserved-node-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx --target-reserved-node-offering-id yyyyyyy-yy-yy-yy-yyy-yyyyyyyyyyyy
{
```

```

    "ExchangedReservedNode": {
      "UsagePrice": 0.0,
      "OfferingType": "No Upfront",
      "State": "exchanging",
      "FixedPrice": 0.0,
      "CurrencyCode": "USD",
      "ReservedNodeId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzzz",
      "NodeType": "dc2.large",
      "NodeCount": 1,
      "RecurringCharges": [
        {
          "RecurringChargeFrequency": "Hourly",
          "RecurringChargeAmount": 0.2
        }
      ],
      "ReservedNodeOfferingType": "Regular",
      "StartTime": "2018-06-27T18:02:58Z",
      "ReservedNodeOfferingId": "yyyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyyyy",
      "Duration": 31536000
    }
  }
}

```

Anda dapat mengonfirmasi bahwa pertukaran selesai dengan menelepon [describe-reserved-nodes](#) dan memeriksa nilai `nodeType`.

Membeli penawaran node cadangan menggunakan AWS CLI dan Amazon Redshift API

Anda dapat menggunakan AWS CLI operasi berikut untuk membeli penawaran node yang dipesan.

- [purchase-reserved-node-offering](#)
- [describe-reserved-node-offerings](#)
- [describe-orderable-cluster-options](#)

Anda dapat menggunakan operasi Amazon Redshift API berikut untuk membeli penawaran node cadangan.

- [PurchaseReservedNodeOffering](#)

- [DescribeReservedNodeOfferings](#)
- [DescribeOrderableClusterOptions](#)

Anda tidak dapat mengubah semua jenis node ke node cadangan, dan juga mungkin bahwa node cadangan yang ada tidak tersedia untuk pembaruan. Ini mungkin karena tipe node dihentikan.

Keamanan di Amazon Redshift

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud – AWS berfungsi melindungi infrastruktur yang menjalankan layanan AWS Cloud AWS. AWS juga menyediakan layanan yang dapat Anda gunakan dengan aman. Efektivitas keamanan kami diuji dan diverifikasi secara rutin oleh auditor pihak ketiga sebagai bagian dari [program kepatuhan AWS](#). Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Redshift, lihat [AWSlayanan dalam cakupan berdasarkan program kepatuhan](#).
- Keamanan di cloud – Tanggung jawab Anda ditentukan oleh AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, termasuk sensitivitas data, persyaratan perusahaan, serta hukum dan peraturan yang berlaku.

Akses ke sumber daya Amazon Redshift dikendalikan pada empat level:

- Manajemen cluster — Kemampuan untuk membuat, mengkonfigurasi, dan menghapus cluster dikendalikan oleh izin yang diberikan kepada pengguna atau akun yang terkait dengan kredensi AWS keamanan Anda. Pengguna dengan izin yang tepat dapat menggunakan AWS Management Console, AWS Command Line Interface (CLI), atau Amazon Redshift Application Programming Interface (API) untuk mengelola cluster mereka. Akses ini dikelola dengan menggunakan kebijakan IAM.

Important

Amazon Redshift memiliki kumpulan praktik terbaik untuk mengelola izin, identitas, dan akses aman. Kami menyarankan Anda untuk membiasakan diri dengan ini saat Anda memulai dengan Amazon Redshift. Untuk informasi selengkapnya, lihat [Manajemen identitas dan akses di Amazon Redshift](#).

- Konektivitas kluster — Grup keamanan Amazon Redshift menentukan AWS instans yang diizinkan untuk terhubung ke kluster Amazon Redshift dalam format Classless Inter-Domain Routing (CIDR).

Untuk informasi tentang membuat Amazon Redshift, Amazon EC2, dan grup keamanan Amazon VPC dan mengaitkannya dengan cluster, lihat [Grup keamanan klaster Amazon Redshift](#)

- Akses database — Kemampuan untuk mengakses objek database, seperti tabel dan tampilan, dikendalikan oleh akun pengguna database di database Amazon Redshift. Pengguna hanya dapat mengakses sumber daya dalam database yang akun pengguna mereka telah diberikan izin untuk mengakses. Anda membuat akun pengguna Amazon Redshift ini dan mengelola izin dengan menggunakan pernyataan CREATE [USER](#), [CREATE GROUP](#), [GRANT](#), dan [REVOKE](#) SQL. Untuk informasi selengkapnya, lihat [Mengelola keamanan database](#) di Panduan Pengembang Database Amazon Redshift.
- Kredensi database sementara dan sistem masuk tunggal — Selain membuat dan mengelola pengguna database menggunakan perintah SQL, seperti CREATE USER dan ALTER USER, Anda dapat mengonfigurasi klien SQL Anda dengan driver Amazon Redshift JDBC atau ODBC khusus. Driver ini mengelola proses pembuatan pengguna database dan kata sandi sementara sebagai bagian dari proses logon database.

Driver mengautentikasi pengguna database berdasarkan otentikasi AWS Identity and Access Management (IAM). Jika Anda sudah mengelola identitas pengguna di luar AWS, Anda dapat menggunakan penyedia identitas (IDP) yang sesuai dengan SAMP 2.0 untuk mengelola akses ke sumber daya Amazon Redshift. Anda menggunakan peran IAM untuk mengonfigurasi IDP Anda AWS dan mengizinkan pengguna federasi Anda menghasilkan kredensi database sementara dan masuk ke database Amazon Redshift. Untuk informasi selengkapnya, lihat [Menggunakan otentikasi IAM untuk menghasilkan kredensi pengguna basis data](#).

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon Redshift. Topik berikut menunjukkan cara mengonfigurasi Amazon Redshift untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Amazon Redshift Anda.

Topik

- [Perlindungan data di Amazon Redshift](#)
- [Manajemen identitas dan akses di Amazon Redshift](#)
- [Mengelola kata sandi admin Amazon Redshift menggunakan AWS Secrets Manager](#)
- [Pencatatan dan pemantauan di Amazon Redshift](#)
- [Validasi Kepatuhan untuk Amazon Redshift](#)

- [Ketahanan di Amazon Redshift](#)
- [Keamanan infrastruktur di Amazon Redshift](#)
- [Analisis konfigurasi dan kelemahan di Amazon Redshift](#)

Perlindungan data di Amazon Redshift

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Amazon Redshift. Sebagaimana diuraikan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk memelihara kendali atas isi yang dihost pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam [Pertanyaan Umum Privasi Data](#). Lihat informasi tentang perlindungan data di Eropa di pos blog [Model Tanggung Jawab Bersama dan GDPR AWS](#) di Blog Keamanan AWS.

Untuk tujuan perlindungan data, sebaiknya lindungi kredensial Akun AWS dan siapkan untuk masing-masing pengguna AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya AWS. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pengelolan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama semua kontrol keamanan bawaan dalam Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-2](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon Redshift atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam

tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi data

Perlindungan data mengacu pada melindungi data saat transit (saat bepergian ke dan dari Amazon Redshift) dan saat istirahat (saat disimpan di disk di pusat data Amazon Redshift). Anda dapat melindungi data dalam perjalanan dengan menggunakan SSL atau dengan menggunakan enkripsi sisi klien. Anda memiliki opsi berikut untuk melindungi data saat istirahat di Amazon Redshift.

- Gunakan enkripsi sisi server — Anda meminta Amazon Redshift untuk mengenkripsi data Anda sebelum menyimpannya di disk di pusat datanya dan mendekripsi ketika Anda mengunduh objek.
- Gunakan enkripsi sisi klien — Anda dapat mengenkripsi data sisi klien dan mengunggah data terenkripsi ke Amazon Redshift. Dalam hal ini, Anda mengelola proses enkripsi, kunci enkripsi, dan alat terkait.

Enkripsi diam

Enkripsi sisi server adalah tentang enkripsi data saat istirahat—yaitu, Amazon Redshift secara opsional mengenkripsi data Anda saat menulisnya di pusat datanya dan mendekripsi untuk Anda saat Anda mengaksesnya. Selama Anda mengautentikasi permintaan Anda dan memiliki izin akses, tidak ada perbedaan dalam cara Anda mengakses data terenkripsi atau tidak terenkripsi.

Amazon Redshift melindungi data saat istirahat melalui enkripsi. Secara opsional, Anda dapat melindungi semua data yang disimpan pada disk dalam cluster dan semua cadangan di Amazon S3 dengan Advanced Encryption Standard AES-256.

[Untuk mengelola kunci yang digunakan untuk mengenkripsi dan mendekripsi sumber daya Amazon Redshift, Anda menggunakan \(\). AWS Key Management Service](#) [AWS KMS](#) [AWS KMS](#) menggabungkan perangkat keras dan perangkat lunak yang aman dan sangat tersedia untuk menyediakan sistem manajemen kunci yang diskalakan untuk cloud. Menggunakan AWS KMS, Anda dapat membuat kunci enkripsi dan menetapkan kebijakan yang mengendalikan bagaimana kunci ini dapat digunakan. AWS KMS mendukung AWS CloudTrail, sehingga Anda dapat mengaudit penggunaan kunci untuk memverifikasi bahwa kunci digunakan dengan tepat. Anda dapat menggunakan AWS KMS tombol Anda dalam kombinasi dengan Amazon Redshift dan layanan

yang didukung.. AWS Untuk daftar layanan yang mendukung AWS KMS, lihat [Cara Layanan AWS Menggunakan AWS KMS](#) dalam Panduan Developer AWS Key Management Service.

Jika Anda memilih untuk mengelola kata sandi admin cluster atau namespace tanpa server yang disediakan, Amazon AWS Secrets Manager Redshift juga menerima kunci KMS tambahan AWS yang digunakan untuk mengenkripsi kredensial Anda. AWS Secrets Manager Kunci tambahan ini dapat berupa kunci yang dihasilkan secara otomatis dari AWS Secrets Manager, atau kunci khusus yang Anda berikan.

Editor kueri Amazon Redshift v2 dengan aman menyimpan informasi yang dimasukkan ke dalam editor kueri sebagai berikut:

- Nama Sumber Daya Amazon (ARN) dari kunci KMS yang digunakan untuk mengenkripsi data editor kueri v2.
- Informasi koneksi database.
- Nama dan isi file dan folder.

Editor kueri Amazon Redshift v2 mengenkripsi informasi menggunakan enkripsi tingkat blok dengan kunci KMS Anda atau kunci KMS akun layanan. Enkripsi data Amazon Redshift Anda dikendalikan oleh properti klaster Amazon Redshift Anda.

Topik

- [Enkripsi basis data Amazon Redshift](#)

Enkripsi basis data Amazon Redshift

Di Amazon Redshift, Anda dapat mengaktifkan enkripsi database untuk cluster Anda untuk membantu melindungi data saat istirahat. Saat Anda mengaktifkan enkripsi untuk klaster, blok data dan metadata sistem dienkripsi untuk cluster dan snapshot-nya.

Anda dapat mengaktifkan enkripsi saat meluncurkan klaster, atau memodifikasi klaster yang tidak terenkripsi untuk menggunakan enkripsi AWS Key Management Service (AWS KMS). Untuk melakukannya, Anda dapat menggunakan kunci AWS-managed atau kunci yang dikelola pelanggan. Saat Anda memodifikasi klaster untuk mengaktifkan AWS KMS enkripsi, Amazon Redshift secara otomatis memigrasikan data Anda ke kluster terenkripsi baru. Snapshot yang dibuat dari cluster terenkripsi juga dienkripsi. Anda juga dapat memigrasikan kluster terenkripsi ke klaster yang tidak terenkripsi dengan memodifikasi klaster dan mengubah opsi Enkripsi database. Untuk informasi selengkapnya, lihat [Mengubah enkripsi cluster](#).

Meskipun enkripsi adalah pengaturan opsional di Amazon Redshift, kami menyarankan Anda mengaktifkannya untuk cluster yang berisi data sensitif. Selain itu, Anda mungkin diminta untuk menggunakan enkripsi tergantung pada pedoman atau peraturan yang mengatur data Anda. Misalnya, Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), dan peraturan lainnya memberikan pedoman untuk menangani jenis data tertentu.

Amazon Redshift menggunakan hierarki kunci enkripsi untuk mengenkripsi database. Anda dapat menggunakan AWS Key Management Service (AWS KMS) atau modul keamanan perangkat keras (HSM) untuk mengelola kunci enkripsi tingkat atas dalam hierarki ini. Proses yang digunakan Amazon Redshift untuk enkripsi berbeda tergantung pada cara Anda mengelola kunci. Amazon Redshift secara otomatis terintegrasi dengan AWS KMS tetapi tidak dengan HSM. Saat Anda menggunakan HSM, Anda harus menggunakan sertifikat klien dan server untuk mengonfigurasi koneksi tepercaya antara Amazon Redshift dan HSM Anda.

Peningkatan proses enkripsi untuk kinerja dan ketersediaan yang lebih baik

Enkripsi dengan node RA3

Pembaruan proses enkripsi untuk node RA3 telah membuat pengalaman jauh lebih baik. Kueri baca dan tulis dapat berjalan selama proses dengan dampak kinerja yang lebih sedikit dari enkripsi. Juga, enkripsi selesai jauh lebih cepat. Langkah-langkah proses yang diperbarui mencakup operasi pemulihan dan migrasi metadata cluster ke cluster target. Pengalaman yang ditingkatkan berlaku untuk jenis enkripsi seperti AWS KMS, misalnya. Ketika Anda memiliki volume data skala petabyte, operasi telah berkurang dari minggu ke hari.

Sebelum mengenkripsi cluster Anda, jika Anda berencana untuk terus menjalankan beban kerja database, Anda dapat meningkatkan kinerja dan mempercepat proses dengan menambahkan node dengan mengubah ukuran elastis. Anda tidak dapat menggunakan perubahan ukuran elastis saat enkripsi sedang dalam proses, jadi lakukan sebelum Anda mengenkripsi. Perhatikan bahwa menambahkan node biasanya menghasilkan biaya yang lebih tinggi.

Enkripsi dengan tipe node lainnya

Saat Anda mengenkripsi cluster dengan node DC2, Anda tidak memiliki kemampuan untuk menjalankan kueri tulis, seperti dengan node RA3. Hanya kueri baca yang dapat dijalankan.

Catatan penggunaan untuk enkripsi dengan node RA3

Wawasan dan sumber daya berikut membantu Anda mempersiapkan enkripsi dan memantau prosesnya.

- Menjalankan kueri setelah memulai enkripsi — Setelah enkripsi dimulai, membaca dan menulis tersedia dalam waktu sekitar lima belas menit. Berapa lama waktu yang dibutuhkan proses enkripsi penuh untuk menyelesaikan tergantung pada jumlah data pada cluster dan tingkat beban kerja.
- Berapa lama enkripsi? — Waktu untuk mengenkripsi data Anda tergantung pada beberapa faktor: Ini termasuk jumlah beban kerja yang berjalan, sumber daya komputasi yang digunakan, jumlah node, dan jenis node. Kami menyarankan agar Anda awalnya melakukan enkripsi di lingkungan pengujian. Sebagai aturan praktis, jika Anda bekerja dengan volume data dalam petabyte, kemungkinan akan memakan waktu 1-3 hari untuk menyelesaikan enkripsi.
- Bagaimana saya tahu enkripsi selesai? — Setelah Anda mengaktifkan enkripsi, penyelesaian snapshot pertama mengonfirmasi bahwa enkripsi selesai.
- Menggulung kembali enkripsi - Jika Anda perlu memutar kembali operasi enkripsi, cara terbaik untuk melakukannya adalah memulihkan dari cadangan terbaru yang diambil sebelum enkripsi dimulai. Anda harus menerapkan kembali pembaruan baru (pembaruan/hapus/sisipan) setelah pencadangan terakhir.
- Melakukan pemulihan tabel — Perhatikan bahwa Anda tidak dapat memulihkan tabel dari kluster yang tidak terenkripsi ke kluster terenkripsi.
- Mengenkripsi kluster simpul tunggal — Mengenkripsi kluster simpul tunggal memiliki keterbatasan kinerja. Dibutuhkan waktu lebih lama dari enkripsi untuk cluster multi-node.
- Membuat cadangan setelah enkripsi — Saat Anda mengenkripsi data di kluster Anda, cadangan tidak dibuat sampai cluster sepenuhnya dienkripsi. Jumlah waktu yang dibutuhkan dapat bervariasi. Waktu yang dibutuhkan untuk pencadangan bisa berjam-jam hingga sehari-hari, tergantung pada ukuran cluster. Setelah enkripsi selesai, mungkin ada penundaan sebelum Anda dapat membuat cadangan.

Perhatikan bahwa karena backup-and-restore operasi terjadi selama proses enkripsi, setiap tabel atau tampilan terwujud yang dibuat dengan BACKUP NO tidak dipertahankan. Untuk informasi selengkapnya, lihat [MEMBUAT TABEL](#) atau [MEMBUAT TAMPILAN TERWUJUD](#).

Topik

- [Enkripsi database untuk Amazon Redshift menggunakan AWS KMS](#)
- [Enkripsi untuk Amazon Redshift menggunakan modul keamanan perangkat keras](#)
- [Rotasi kunci enkripsi di Amazon Redshift](#)
- [Mengubah enkripsi cluster](#)
- [Mengkonfigurasi enkripsi basis data menggunakan konsol](#)

- [Mengkonfigurasi enkripsi database menggunakan Amazon Redshift API dan AWS CLI](#)

Enkripsi database untuk Amazon Redshift menggunakan AWS KMS

Saat Anda memilih AWS KMS untuk manajemen kunci dengan Amazon Redshift, ada hierarki kunci enkripsi empat tingkat. Kunci ini, dalam urutan hierarkis, adalah kunci root, kunci enkripsi cluster (CEK), kunci enkripsi database (DEK), dan kunci enkripsi data.

Saat meluncurkan kluster, Amazon Redshift mengembalikan daftar AWS akun AWS KMS keys yang telah dibuat atau memiliki izin untuk digunakan. AWS KMS Anda memilih kunci KMS untuk digunakan sebagai kunci root Anda dalam hierarki enkripsi.

Secara default, Amazon Redshift memilih kunci default Anda sebagai kunci root. Kunci default Anda adalah kunci AWS-managed yang dibuat agar AWS akun Anda dapat digunakan di Amazon Redshift. AWS KMS membuat kunci ini saat pertama kali Anda meluncurkan cluster terenkripsi di AWS Wilayah dan memilih kunci default.

Jika Anda tidak ingin menggunakan kunci default, Anda harus memiliki (atau membuat) kunci KMS yang dikelola pelanggan secara terpisah AWS KMS sebelum meluncurkan kluster di Amazon Redshift. Kunci yang dikelola pelanggan memberi Anda lebih banyak fleksibilitas, termasuk kemampuan untuk membuat, memutar, menonaktifkan, menentukan kontrol akses, dan mengaudit kunci enkripsi yang digunakan untuk membantu melindungi data Anda. Untuk informasi selengkapnya tentang membuat kunci KMS, lihat [Membuat Kunci](#) di Panduan AWS Key Management Service Pengembang.

Jika Anda ingin menggunakan AWS KMS kunci dari AWS akun lain, Anda harus memiliki izin untuk menggunakan kunci dan menentukan Nama Sumber Daya Amazon (ARN) di Amazon Redshift. Untuk informasi selengkapnya tentang akses ke kunci AWS KMS, lihat [Mengontrol Akses ke Kunci Anda](#) di Panduan AWS Key Management Service Pengembang.

Setelah Anda memilih kunci root, Amazon Redshift meminta yang AWS KMS menghasilkan kunci data dan mengenkripsinya menggunakan kunci root yang dipilih. Kunci data ini digunakan sebagai CEK di Amazon Redshift. AWS KMS mengekspor CEK terenkripsi ke Amazon Redshift, di mana ia disimpan secara internal pada disk dalam jaringan terpisah dari cluster bersama dengan hibah ke kunci KMS dan konteks enkripsi untuk CEK. Hanya CEK terenkripsi yang diekspor ke Amazon Redshift; kunci KMS tetap ada. AWS KMS Amazon Redshift juga meneruskan CEK terenkripsi melalui saluran aman ke cluster dan memuatnya ke dalam memori. Kemudian, Amazon Redshift memanggil AWS KMS untuk mendekripsi CEK dan memuat CEK yang didekripsi ke dalam memori.

Untuk informasi selengkapnya tentang hibah, konteks enkripsi, dan konsep AWS KMS terkait lainnya, lihat [Konsep dalam Panduan AWS Key Management Service](#) Pengembang.

Selanjutnya, Amazon Redshift secara acak menghasilkan kunci untuk digunakan sebagai DEK dan memuatnya ke dalam memori di cluster. CEK yang didekripsi digunakan untuk mengenkripsi DEK, yang kemudian melewati saluran aman dari cluster untuk disimpan secara internal oleh Amazon Redshift pada disk di jaringan terpisah dari cluster. Seperti CEK, versi DEK yang dienkripsi dan didekripsi dimuat ke dalam memori di cluster. Versi DEK yang didekripsi kemudian digunakan untuk mengenkripsi kunci enkripsi individu yang dihasilkan secara acak untuk setiap blok data dalam database.

Saat cluster reboot, Amazon Redshift dimulai dengan versi CEK dan DEK yang tersimpan secara internal dan terenkripsi, memuat ulang ke dalam memori, dan kemudian AWS KMS memanggil untuk mendekripsi CEK dengan kunci KMS lagi sehingga dapat dimuat ke dalam memori. CEK yang didekripsi kemudian digunakan untuk mendekripsi DEK lagi, dan DEK yang didekripsi dimuat ke dalam memori dan digunakan untuk mengenkripsi dan mendekripsi kunci blok data sesuai kebutuhan.

Untuk informasi selengkapnya tentang membuat klaster Amazon Redshift yang dienkripsi dengan AWS KMS kunci, lihat dan. [Membuat klaster Mengelola cluster menggunakan API Amazon AWS CLI Redshift dan Amazon](#)

Menyalin AWS KMS—snapshot terenkripsi ke Wilayah lain AWS

AWS KMS kunci khusus untuk suatu AWS Wilayah. Jika Anda mengaktifkan penyalinan snapshot Amazon Redshift ke Wilayah AWS lain, dan cluster sumber serta snapshot-nya dienkripsi menggunakan kunci root AWS KMS dari, Anda perlu mengonfigurasi hibah untuk Amazon Redshift untuk menggunakan kunci root di Wilayah tujuan. AWS Hibah ini memungkinkan Amazon Redshift mengenkripsi snapshot di Wilayah tujuan. AWS Untuk informasi selengkapnya tentang salinan snapshot lintas wilayah, lihat. [Menyalin snapshot ke Wilayah lain AWS](#)

Note

Jika Anda mengaktifkan penyalinan snapshot dari cluster terenkripsi dan digunakan AWS KMS untuk kunci root Anda, Anda tidak dapat mengganti nama cluster Anda karena nama cluster adalah bagian dari konteks enkripsi. Jika Anda harus mengganti nama cluster Anda, Anda dapat menonaktifkan penyalinan snapshot di AWS Wilayah sumber, mengganti nama cluster, dan kemudian mengkonfigurasi dan mengaktifkan penyalinan snapshot lagi.

Proses untuk mengonfigurasi hibah untuk menyalin snapshot adalah sebagai berikut.

1. Di AWS Wilayah tujuan, buat hibah salinan snapshot dengan melakukan hal berikut:
 - Jika Anda belum memiliki AWS KMS kunci untuk digunakan, buat satu. Untuk informasi selengkapnya tentang membuat AWS KMS kunci, lihat [Membuat Kunci](#) di Panduan AWS Key Management Service Pengembang.
 - Tentukan nama untuk hibah salinan snapshot. Nama ini harus unik di AWS Wilayah itu untuk AWS akun Anda.
 - Tentukan ID AWS KMS kunci tempat Anda membuat hibah. Jika Anda tidak menentukan ID kunci, hibah berlaku untuk kunci default Anda.
2. Di AWS wilayah sumber, aktifkan penyalinan snapshot dan tentukan nama hibah salinan snapshot yang Anda buat di Wilayah tujuan. AWS

Proses sebelumnya ini hanya diperlukan jika Anda mengaktifkan penyalinan snapshot menggunakan, AWS CLI Amazon Redshift API, atau SDK. Jika Anda menggunakan konsol, Amazon Redshift menyediakan alur kerja yang tepat untuk mengonfigurasi hibah saat Anda mengaktifkan salinan snapshot lintas wilayah. Untuk informasi selengkapnya tentang mengonfigurasi salinan snapshot lintas wilayah untuk cluster AWS KMS-enkripsi menggunakan konsol, lihat. [Konfigurasi salinan snapshot lintas wilayah untuk kluster yang AWS KMS dienkripsi](#)

Sebelum snapshot disalin ke AWS Wilayah tujuan, Amazon Redshift mendekripsi snapshot menggunakan kunci root di Wilayah AWS sumber dan mengenkripsi ulang sementara menggunakan kunci RSA yang dibuat secara acak yang dikelola Amazon Redshift secara internal. Amazon Redshift kemudian menyalin snapshot melalui saluran aman ke AWS Wilayah tujuan, mendekripsi snapshot menggunakan kunci RSA yang dikelola secara internal, dan kemudian mengenkripsi ulang snapshot menggunakan kunci root di Wilayah tujuan. AWS

Untuk informasi selengkapnya tentang mengonfigurasi hibah salinan snapshot untuk cluster AWS KMS-enkripsi, lihat. [Mengkonfigurasi Amazon Redshift untuk digunakan AWS KMS kunci enkripsi menggunakan Amazon Redshift API dan AWS CLI](#)

Enkripsi untuk Amazon Redshift menggunakan modul keamanan perangkat keras

Jika Anda tidak menggunakan AWS KMS untuk manajemen kunci, Anda dapat menggunakan modul keamanan perangkat keras (HSM) untuk manajemen kunci dengan Amazon Redshift.

⚠ Important

Enkripsi HSM tidak didukung untuk tipe node DC2 dan RA3.

HSM adalah perangkat yang memberikan kontrol langsung atas pembuatan dan manajemen kunci. Mereka memberikan keamanan yang lebih besar dengan memisahkan manajemen kunci dari lapisan aplikasi dan basis data. Amazon Redshift mendukung AWS CloudHSM Classic untuk manajemen kunci. Proses enkripsi berbeda ketika Anda menggunakan HSM untuk mengelola kunci enkripsi Anda alih-alih. AWS KMS

⚠ Important

Amazon Redshift hanya AWS CloudHSM mendukung Klasik. Kami tidak mendukung AWS CloudHSM layanan yang lebih baru.

AWS CloudHSM Klasik tertutup untuk pelanggan baru. Untuk informasi selengkapnya, lihat Harga [Classic CloudHSM](#). AWS CloudHSM Klasik tidak tersedia di semua AWS Wilayah.

Untuk informasi selengkapnya tentang AWS Wilayah yang tersedia, lihat [Tabel AWS Wilayah](#).

Saat Anda mengonfigurasi kluster Anda untuk menggunakan HSM, Amazon Redshift mengirimkan permintaan ke HSM untuk menghasilkan dan menyimpan kunci yang akan digunakan sebagai CEK. Namun, tidak seperti AWS KMS, HSM tidak mengeksport CEK ke Amazon Redshift. Sebaliknya, Amazon Redshift secara acak menghasilkan DEK di cluster dan meneruskannya ke HSM untuk dienkripsi oleh CEK. HSM mengembalikan DEK terenkripsi ke Amazon Redshift, di mana ia dienkripsi lebih lanjut menggunakan kunci root internal yang dihasilkan secara acak dan disimpan secara internal pada disk di jaringan terpisah dari cluster. Amazon Redshift juga memuat versi DEK yang didekripsi dalam memori di cluster sehingga DEK dapat digunakan untuk mengenkripsi dan mendekripsi kunci individual untuk blok data.

Jika cluster di-boot ulang, Amazon Redshift mendekripsi DEK terenkripsi ganda yang disimpan secara internal menggunakan kunci root internal untuk mengembalikan DEK yang disimpan secara internal ke status terenkripsi CEK. DEK yang dienkripsi CEK kemudian diteruskan ke HSM untuk didekripsi dan diteruskan kembali ke Amazon Redshift, di mana ia dapat dimuat dalam memori lagi untuk digunakan dengan kunci blok data individual.

Mengonfigurasi koneksi tepercaya antara Amazon Redshift dan HSM

Ketika Anda memilih untuk menggunakan HSM untuk pengelolaan kunci klaster Anda, Anda perlu mengonfigurasi tautan jaringan tepercaya antara Amazon Redshift dan HSM Anda. Melakukan hal ini memerlukan konfigurasi sertifikat klien dan server. Koneksi tepercaya digunakan untuk meneruskan kunci enkripsi antara HSM dan Amazon Redshift selama operasi enkripsi dan dekripsi.

Amazon Redshift membuat sertifikat klien publik dari key pair private dan public key pair yang dibuat secara acak. Ini dienkripsi dan disimpan secara internal. Anda mengunduh dan mendaftarkan sertifikat klien publik di HSM Anda, dan menetapkannya ke partisi HSM yang berlaku.

Anda memberikan Amazon Redshift dengan alamat IP HSM, nama partisi HSM, kata sandi partisi HSM, dan sertifikat server HSM publik, yang dienkripsi dengan menggunakan kunci root internal. Amazon Redshift menyelesaikan proses konfigurasi dan memverifikasi bahwa ia dapat terhubung ke HSM. Jika tidak bisa, cluster dimasukkan ke dalam status `INCOMPATIBLE_HSM` dan cluster tidak dibuat. Dalam hal ini, Anda harus menghapus cluster yang tidak lengkap dan coba lagi.

Important

Ketika Anda memodifikasi klaster Anda untuk menggunakan partisi HSM yang berbeda, Amazon Redshift memverifikasi bahwa ia dapat terhubung ke partisi baru, tetapi tidak memverifikasi bahwa kunci enkripsi yang valid ada. Sebelum Anda menggunakan partisi baru, Anda harus mereplikasi kunci Anda ke partisi baru. Jika cluster dimulai ulang dan Amazon Redshift tidak dapat menemukan kunci yang valid, restart gagal. Untuk informasi selengkapnya, lihat [Mereplikasi Kunci di Seluruh HSM](#).

Setelah konfigurasi awal, jika Amazon Redshift gagal terhubung ke HSM, sebuah peristiwa dicatat. Untuk informasi selengkapnya tentang peristiwa ini, lihat [Pemberitahuan Acara Amazon Redshift](#).

Rotasi kunci enkripsi di Amazon Redshift

Di Amazon Redshift, Anda dapat memutar kunci enkripsi untuk cluster terenkripsi. Saat Anda memulai proses rotasi kunci, Amazon Redshift memutar CEK untuk cluster yang ditentukan dan untuk snapshot cluster otomatis atau manual apa pun. Amazon Redshift juga memutar DEK untuk cluster yang ditentukan, tetapi tidak dapat memutar DEK untuk snapshot saat disimpan secara internal di Amazon Simple Storage Service (Amazon S3) dan dienkripsi menggunakan DEK yang ada.

Sementara rotasi sedang berlangsung, cluster dimasukkan ke dalam status `ROTATING_KEYS` sampai selesai, pada saat itu cluster kembali ke status `AVAILABLE`. Amazon Redshift menangani dekripsi dan enkripsi ulang selama proses rotasi kunci.

Note

Anda tidak dapat memutar tombol untuk snapshot tanpa cluster sumber. Sebelum Anda menghapus cluster, pertimbangkan apakah snapshot-nya bergantung pada rotasi tombol.

Karena klaster sesaat tidak tersedia selama proses rotasi kunci, Anda harus memutar kunci hanya sesering yang dibutuhkan data Anda atau ketika Anda mencurigai kunci mungkin telah disusupi. Sebagai praktik terbaik, Anda harus meninjau jenis data yang Anda simpan dan merencanakan seberapa sering memutar kunci yang mengenkripsi data tersebut. Frekuensi untuk memutar kunci bervariasi tergantung pada kebijakan perusahaan Anda untuk keamanan data, dan standar industri apa pun mengenai data sensitif dan kepatuhan terhadap peraturan. Pastikan paket Anda menyeimbangkan kebutuhan keamanan dengan pertimbangan ketersediaan untuk klaster Anda.

Untuk informasi selengkapnya tentang tombol putar, lihat [Memutar kunci enkripsi menggunakan konsol Amazon Redshift](#) dan [Memutar kunci enkripsi menggunakan Amazon Redshift API dan AWS CLI](#).

Mengubah enkripsi cluster

Anda dapat memodifikasi klaster yang tidak terenkripsi untuk menggunakan enkripsi AWS Key Management Service (AWS KMS), baik menggunakan kunci AWS-managed atau kunci yang dikelola pelanggan. Saat Anda memodifikasi klaster untuk mengaktifkan AWS KMS enkripsi, Amazon Redshift secara otomatis memigrasikan data Anda ke kluster terenkripsi baru. Anda juga dapat memigrasikan klaster yang tidak terenkripsi ke kluster terenkripsi dengan memodifikasi klaster.

Selama operasi migrasi, klaster Anda tersedia dalam mode hanya-baca, dan status klaster muncul sebagai perubahan ukuran.

Jika klaster Anda dikonfigurasi untuk mengaktifkan salinan snapshot lintas AWS Wilayah, Anda harus menonaktifkannya sebelum mengubah enkripsi. Lihat informasi yang lebih lengkap di [Menyalin snapshot ke Wilayah lain AWS](#) dan [Konfigurasi salinan snapshot lintas wilayah untuk kluster yang AWS KMS dienkripsi](#). Anda tidak dapat mengaktifkan enkripsi modul keamanan perangkat keras (HSM) dengan memodifikasi cluster. Sebagai gantinya, buat cluster baru yang dienkripsi HSM dan

migrasi data Anda ke cluster baru. Untuk informasi selengkapnya, lihat [Migrasi ke cluster terenkripsi HSM](#).

Untuk memodifikasi enkripsi database pada sebuah cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster, lalu pilih cluster yang ingin Anda ubah enkripsi.
3. Pilih Properti.
4. Di bagian Konfigurasi basis data, pilih Edit, lalu pilih Edit enkripsi.
5. Pilih salah satu opsi enkripsi dan pilih Simpan perubahan.

Untuk mengubah enkripsi cluster menggunakan CLI

Untuk memodifikasi cluster yang tidak terenkripsi untuk digunakan AWS KMS, jalankan perintah `modify-cluster` CLI dan tentukan `--encrypted`, seperti yang ditunjukkan berikut. Secara default, kunci KMS default Anda digunakan. Untuk menentukan kunci yang dikelola pelanggan, sertakan `--kms-key-id` opsi.

```
aws redshift modify-cluster --cluster-identifier <value> --encrypted --kms-key-id <value>
```

Untuk menghapus enkripsi dari cluster Anda, jalankan perintah CLI berikut.

```
aws redshift modify-cluster --cluster-identifier <value> --no-encrypted
```

Migrasi ke cluster terenkripsi HSM

Untuk memigrasikan klaster yang tidak terenkripsi ke kluster yang dienkripsi menggunakan modul keamanan perangkat keras (HSM), Anda membuat klaster terenkripsi baru dan memindahkan data Anda ke cluster baru. Anda tidak dapat bermigrasi ke klaster terenkripsi HSM dengan memodifikasi klaster.

Untuk bermigrasi dari klaster yang tidak terenkripsi ke klaster terenkripsi HSM, pertama-tama Anda membongkar data Anda dari kluster sumber yang ada. Kemudian Anda memuat ulang data dalam cluster target baru dengan pengaturan enkripsi yang dipilih. Untuk informasi selengkapnya tentang meluncurkan klaster terenkripsi, lihat [Enkripsi basis data Amazon Redshift](#)

Selama proses migrasi, kluster sumber Anda tersedia untuk kueri hanya-baca hingga langkah terakhir. Langkah terakhir adalah mengganti nama kluster target dan sumber, yang mengalihkan titik akhir sehingga semua lalu lintas diarahkan ke cluster target yang baru. Cluster target tidak tersedia sampai Anda reboot mengikuti penggantian nama. Tangguhkan semua beban data dan operasi penulisan lainnya di cluster sumber saat data sedang ditransfer.

Untuk mempersiapkan migrasi

1. Identifikasi semua sistem dependen yang berinteraksi dengan Amazon Redshift, misalnya alat intelijen bisnis (BI) dan mengekstrak, mengubah, dan memuat (ETL) sistem.
2. Identifikasi kueri validasi untuk menguji migrasi.

Misalnya, Anda dapat menggunakan kueri berikut untuk menemukan jumlah tabel yang ditentukan pengguna.

```
select count(*)
from pg_table_def
where schemaname != 'pg_catalog';
```

Query berikut mengembalikan daftar semua tabel yang ditentukan pengguna dan jumlah baris di setiap tabel.

```
select "table", tbl_rows
from svv_table_info;
```

3. Pilih waktu yang tepat untuk migrasi Anda. Untuk menemukan waktu ketika penggunaan kluster terendah, pantau metrik cluster seperti pemanfaatan CPU dan jumlah koneksi database. Untuk informasi selengkapnya, lihat [Melihat data kinerja cluster](#).
4. Jatuhkan tabel yang tidak digunakan.

Untuk membuat daftar tabel dan berapa kali setiap tabel telah ditanyakan, jalankan kueri berikut.

```
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. Luncurkan cluster baru yang dienkripsi.

Gunakan nomor port yang sama untuk cluster target seperti untuk cluster sumber. Untuk informasi selengkapnya tentang meluncurkan klaster terenkripsi, lihat [Enkripsi basis data Amazon Redshift](#)

6. Siapkan proses bongkar muat dan muat.

Anda dapat menggunakan [Amazon Redshift Unload/Copy Utility untuk membantu memigrasikan data antar cluster](#). Utilitas mengekspor data dari cluster sumber ke lokasi di Amazon S3. Data dienkripsi dengan AWS KMS Utilitas kemudian secara otomatis mengimpor data ke target. Secara opsional, Anda dapat menggunakan utilitas untuk membersihkan Amazon S3 setelah migrasi selesai.

7. Jalankan tes untuk memverifikasi proses Anda dan memperkirakan berapa lama operasi penulisan harus ditangguhkan.

Selama operasi bongkar muat, pertahankan konsistensi data dengan menangguhkan beban data dan operasi penulisan lainnya. Menggunakan salah satu tabel terbesar Anda, jalankan proses pembongkaran dan muat untuk membantu Anda memperkirakan waktu.

8. Buat objek database, seperti skema, tampilan, dan tabel. Untuk membantu Anda menghasilkan pernyataan bahasa definisi data (DDL) yang diperlukan, Anda dapat menggunakan skrip di [AdminViews](#) dalam repositori. AWS GitHub

Untuk memigrasikan klaster Anda

1. Hentikan semua proses ETL pada cluster sumber.

Untuk mengonfirmasi bahwa tidak ada operasi penulisan dalam proses, gunakan Amazon Redshift Management Console untuk memantau penulisan IOPS. Untuk informasi selengkapnya, lihat [Melihat data kinerja cluster](#).

2. Jalankan kueri validasi yang Anda identifikasi sebelumnya untuk mengumpulkan informasi tentang kluster sumber yang tidak terenkripsi sebelum migrasi.
3. (Opsional) Buat satu antrian manajemen beban kerja (WLM) untuk menggunakan sumber daya maksimum yang tersedia di cluster sumber dan target. Misalnya, buat antrian bernama `data_migrate` dan konfigurasi antrian dengan memori 95 persen dan konkurensi 4. Untuk informasi selengkapnya, lihat [Perutean Kueri ke Antrian Berdasarkan Grup Pengguna dan Grup Kueri](#) di Panduan Pengembang Database Amazon Redshift.
4. Menggunakan `data_migrate` antrian, jalankan. `UnloadCopyUtility`

Pantau proses UNLOAD dan COPY menggunakan Amazon Redshift Console.
5. Jalankan kueri validasi lagi dan verifikasi bahwa hasilnya cocok dengan hasil dari cluster sumber.
6. Ganti nama sumber dan kluster target Anda untuk menukar titik akhir. Untuk menghindari gangguan, lakukan operasi ini di luar jam kerja.
7. Verifikasi bahwa Anda dapat terhubung ke cluster target menggunakan semua klien SQL Anda, seperti ETL dan alat pelaporan.
8. Matikan cluster sumber yang tidak terenkripsi.

Mengkonfigurasi enkripsi basis data menggunakan konsol

Anda dapat menggunakan konsol Amazon Redshift untuk mengonfigurasi Amazon Redshift untuk menggunakan HSM dan memutar kunci enkripsi. Untuk informasi tentang cara membuat cluster menggunakan kunci AWS KMS enkripsi, lihat [Membuat klaster](#) dan [Mengelola cluster menggunakan API Amazon AWS CLI Redshift dan Amazon](#).

Untuk memodifikasi enkripsi database pada sebuah cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Clusters, lalu pilih cluster yang ingin Anda pindahkan snapshot.
3. Untuk Tindakan, pilih Ubah untuk menampilkan halaman konfigurasi.
4. Di bagian konfigurasi Database, pilih pengaturan untuk Enkripsi, lalu pilih Modify cluster.

Memutar kunci enkripsi menggunakan konsol Amazon Redshift

Anda dapat menggunakan prosedur berikut untuk memutar kunci enkripsi dengan menggunakan konsol Amazon Redshift.

Untuk memutar kunci enkripsi untuk sebuah cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, lalu pilih cluster yang ingin Anda perbarui kunci enkripsi.
3. Untuk Tindakan, pilih Putar enkripsi untuk menampilkan halaman Putar kunci enkripsi.
4. Pada halaman Putar kunci enkripsi, pilih Putar kunci enkripsi.

Mengkonfigurasi enkripsi database menggunakan Amazon Redshift API dan AWS CLI

Menggunakan API Amazon Redshift dan AWS Command Line Interface (AWS CLI) untuk mengkonfigurasi opsi kunci enkripsi untuk database Amazon Redshift. Untuk informasi selengkapnya tentang enkripsi basis data, lihat [Enkripsi basis data Amazon Redshift](#).

Mengkonfigurasi Amazon Redshift untuk digunakan AWS KMS kunci enkripsi menggunakan Amazon Redshift API dan AWS CLI

Anda dapat menggunakan tindakan Amazon Redshift API berikut untuk mengonfigurasi Amazon Redshift untuk digunakan AWS KMS kunci enkripsi.

- [CreateCluster](#)
- [CreateSnapshotCopyGrant](#)
- [DescribeSnapshotCopyGrants](#)
- [DeleteSnapshotCopyGrant](#)
- [DisableSnapshotCopy](#)
- [EnableSnapshotCopy](#)

Anda dapat menggunakan operasi Amazon Redshift CLI berikut ini untuk mengonfigurasi Amazon Redshift untuk digunakan AWS KMS kunci enkripsi.

- [create-cluster](#)

- [membuat-snapshot-copy-grant](#)
- [describe-snapshot-copy-hibah](#)
- [menghapus-snapshot-copy-grant](#)
- [menonaktifkan-snapshot-copy](#)
- [mengaktifkan-snapshot-copy](#)

Mengkonfigurasi Amazon Redshift untuk menggunakan HSM menggunakan Amazon Redshift API dan AWS CLI

Anda dapat menggunakan tindakan Amazon Redshift API berikut untuk mengelola modul keamanan perangkat keras.

- [CreateHSMClientCertificate](#)
- [CreateHSMConfiguration](#)
- [DeleteHsmClientCertificate](#)
- [DeleteHSMConfiguration](#)
- [DescribeHSMClientCertificates](#)
- [DescribeHSMConfigurations](#)

Anda dapat menggunakan berikut AWS CLI operasi untuk mengelola modul keamanan perangkat keras.

- [membuat-hsm-client-sertifikat](#)
- [create-hsm-konfigurasi](#)
- [menghapus-hsm-client-sertifikat](#)
- [menghapus-hsm-konfigurasi](#)
- [menjelaskan-hsm-client-sertifikat](#)
- [describe-hsm-konfigurasi](#)

Memutar kunci enkripsi menggunakan Amazon Redshift API dan AWS CLI

Anda dapat menggunakan tindakan Amazon Redshift berikut untuk memutar kunci enkripsi.

- [RotateEncryptionKey](#)

Anda dapat menggunakan berikut AWS CLI operasi untuk memutar kunci enkripsi.

- [rotate-enkripsi-kunci](#)

Enkripsi dalam bergerak

Anda dapat mengonfigurasi lingkungan Anda untuk melindungi kerahasiaan dan integritas data dalam perjalanan.

Enkripsi data dalam perjalanan antara cluster Amazon Redshift dan klien SQL melalui JDBC/ODBC:

- Anda dapat terhubung ke cluster Amazon Redshift dari alat klien SQL melalui koneksi Java Database Connectivity (JDBC) dan Open Database Connectivity (ODBC).
- Amazon Redshift mendukung koneksi Secure Sockets Layer (SSL) untuk mengenkripsi data dan sertifikat server untuk memvalidasi sertifikat server yang terhubung dengan klien. Klien terhubung ke node pemimpin cluster Amazon Redshift. Untuk informasi selengkapnya, lihat [Mengkonfigurasi opsi keamanan untuk koneksi](#).
- Untuk mendukung koneksi SSL, Amazon Redshift membuat dan AWS Certificate Manager menginstal (ACM) mengeluarkan sertifikat di setiap klaster. Untuk informasi selengkapnya, lihat [Transisi ke sertifikat ACM untuk koneksi SSL](#).
- Untuk melindungi data Anda saat transit di dalam AWS Cloud, Amazon Redshift menggunakan SSL yang dipercepat perangkat keras untuk berkomunikasi dengan Amazon S3 atau Amazon DynamoDB untuk operasi COPY, UNLOAD, backup, dan restore.

Enkripsi data dalam perjalanan antara cluster Amazon Redshift dan Amazon S3 atau DynamoDB:

- Amazon Redshift menggunakan SSL yang dipercepat perangkat keras untuk berkomunikasi dengan Amazon S3 atau DynamoDB untuk operasi COPY, UNLOAD, backup, dan restore.
- Redshift Spectrum mendukung enkripsi sisi server (SSE) Amazon S3 menggunakan kunci default akun Anda yang dikelola oleh (KMS). AWS Key Management Service
- Enkripsi beban Amazon Redshift dengan Amazon S3 dan. AWS KMS Untuk informasi selengkapnya, lihat [Mengenkripsi Beban Amazon Redshift Anda dengan Amazon S3](#) dan. AWS KMS

Enkripsi dan penandatanganan data dalam transit antara AWS CLI, SDK, atau klien API dan titik akhir Amazon Redshift:

- Amazon Redshift menyediakan titik akhir HTTPS untuk mengenkripsi data dalam perjalanan.
- Untuk melindungi integritas permintaan API ke Amazon Redshift, panggilan API harus ditandatangani oleh pemanggil. Panggilan ditandatangani oleh sertifikat X.509 atau kunci akses AWS rahasia pelanggan sesuai dengan Proses Penandatanganan Versi Tanda Tangan 4 (Sigv4). Untuk informasi selengkapnya, lihat [Proses Penandatanganan Versi Tanda Tangan 4](#) di Referensi Umum AWS.
- Gunakan AWS CLI atau salah satu AWS SDK untuk membuat permintaan. AWS Alat-alat ini secara otomatis menandatangani permintaan untuk Anda dengan kunci akses yang Anda tentukan saat Anda mengonfigurasi alat.

Enkripsi data dalam perjalanan antara cluster Amazon Redshift dan editor kueri Amazon Redshift v2

- Data ditransmisikan antara editor kueri v2 dan cluster Amazon Redshift melalui saluran terenkripsi TLS.

Manajemen kunci

Anda dapat mengonfigurasi lingkungan Anda untuk melindungi data dengan kunci:

- Amazon Redshift secara otomatis terintegrasi dengan AWS Key Management Service (AWS KMS) untuk manajemen kunci. AWS KMS menggunakan enkripsi amplop. Untuk informasi selengkapnya, lihat [Enkripsi Amplop](#).
- Saat kunci enkripsi dikelola AWS KMS, Amazon Redshift menggunakan arsitektur berbasis kunci empat tingkat untuk enkripsi. Arsitektur terdiri dari kunci enkripsi data AES-256 yang dihasilkan secara acak, kunci database, kunci cluster, dan kunci root. Untuk informasi selengkapnya, lihat [Cara Penggunaan Amazon Redshift](#). AWS KMS
- Anda dapat membuat kunci yang dikelola pelanggan Anda sendiri AWS KMS. Untuk informasi selengkapnya, lihat [Membuat Kunci](#).
- Anda juga dapat mengimpor materi kunci Anda sendiri untuk yang baru AWS KMS keys. Untuk informasi selengkapnya, lihat [Mengimpor Materi Utama di AWS Key Management Service \(AWS KMS\)](#).
- Amazon Redshift mendukung pengelolaan kunci enkripsi dalam modul keamanan perangkat keras eksternal (HSM). HSM bisa di tempat atau bisa. AWS CloudHSM Saat Anda menggunakan HSM, Anda harus menggunakan sertifikat klien dan server untuk mengonfigurasi koneksi tepercaya antara Amazon Redshift dan HSM Anda. Amazon Redshift hanya mendukung AWS

CloudHSM Classic untuk manajemen kunci. Untuk informasi selengkapnya, lihat [Enkripsi untuk Amazon Redshift menggunakan modul keamanan perangkat keras](#). Untuk informasi tentang AWS CloudHSM, lihat [Apa yang dimaksud dengan AWS CloudHSM?](#)

- Anda dapat memutar kunci enkripsi untuk cluster terenkripsi.. Untuk informasi selengkapnya, lihat [Rotasi kunci enkripsi di Amazon Redshift](#).

Tokenisasi data

Tokenisasi adalah proses mengganti nilai aktual dengan nilai buram untuk tujuan keamanan data. Aplikasi yang sensitif terhadap keamanan menggunakan tokenisasi untuk mengganti data sensitif seperti informasi identitas pribadi (PII) atau informasi kesehatan yang dilindungi (PHI) dengan token untuk mengurangi risiko keamanan. Detokenisasi membalikkan token dengan nilai aktual untuk pengguna yang berwenang dengan kebijakan keamanan yang sesuai.

Untuk integrasi dengan layanan tokenisasi pihak ketiga, Anda dapat menggunakan fungsi yang ditentukan pengguna Amazon Redshift (UDF) yang Anda buat. [AWS Lambda](#) Untuk informasi selengkapnya, lihat [Fungsi yang ditentukan pengguna Lambda](#) di Panduan Pengembang Database Amazon Redshift. Misalnya, lihat [Protegrity](#).

Amazon Redshift mengirimkan permintaan tokenisasi ke server tokenisasi yang diakses melalui REST API atau titik akhir yang telah ditentukan sebelumnya. Dua atau lebih fungsi Lambda gratis memproses permintaan tokenisasi dan detokenisasi. Untuk pemrosesan ini, Anda dapat menggunakan fungsi Lambda yang disediakan oleh penyedia tokenisasi pihak ketiga. Anda juga dapat menggunakan fungsi Lambda yang Anda daftarkan sebagai Lambda UDF di Amazon Redshift.

Misalnya, misalkan kueri dikirimkan yang memanggil UDF tokenisasi atau detokenisasi pada kolom. Cluster Amazon Redshift menggulung baris argumen yang berlaku dan mengirimkan baris tersebut dalam batch ke fungsi Lambda secara paralel. Transfer data antara node komputasi Amazon Redshift dan Lambda dalam koneksi jaringan terpisah dan terisolasi yang tidak dapat diakses oleh klien. Fungsi Lambda meneruskan data ke titik akhir server tokenisasi. Server tokenisasi memberi token atau mendetokenisasi data seperlunya dan mengembalikannya. Fungsi Lambda kemudian mengirimkan hasilnya ke cluster Amazon Redshift untuk diproses lebih lanjut, jika perlu, dan kemudian mengembalikan hasil kueri.

Privasi lalu lintas jaringan internet

Untuk merutekan lalu lintas antara Amazon Redshift dan klien dan aplikasi di jaringan perusahaan:

- Siapkan koneksi pribadi antara virtual private cloud (VPC) dan jaringan perusahaan Anda. Siapkan koneksi VPN IPsec melalui internet atau koneksi fisik pribadi menggunakan AWS Direct Connect koneksi. AWS Direct Connect memungkinkan Anda untuk membuat antarmuka virtual pribadi dari jaringan lokal Anda langsung ke VPC Amazon Anda, memberi Anda koneksi jaringan bandwidth tinggi pribadi antara jaringan Anda dan VPC Anda. Dengan beberapa antarmuka virtual, Anda bahkan dapat membangun konektivitas pribadi ke beberapa VPC sambil mempertahankan isolasi jaringan. Untuk informasi selengkapnya, lihat [Apa itu AWS VPN Site-to-Site?](#) dan [Apa itu AWS Direct Connect?](#)

Untuk merutekan lalu lintas antara cluster Amazon Redshift di bucket VPC dan Amazon S3 di Wilayah yang sama: AWS

- Siapkan titik akhir VPC pribadi Amazon S3 untuk mengakses data Amazon S3 secara pribadi dari pemuatan atau pembongkaran ETL. Untuk informasi selengkapnya, lihat [Titik Akhir untuk Amazon S3](#).
- Aktifkan “Perutean VPC yang Ditingkatkan” untuk kluster Amazon Redshift, yang menentukan titik akhir VPC Amazon S3 target. Lalu lintas yang dihasilkan oleh perintah Amazon Redshift COPY, UNLOAD, atau CREATE LIBRARY kemudian dirutekan melalui titik akhir pribadi. Untuk informasi selengkapnya, lihat [Perutean VPC yang disempurnakan](#).

Manajemen identitas dan akses di Amazon Redshift

Akses ke Amazon Redshift memerlukan kredensial yang AWS dapat digunakan untuk mengautentikasi permintaan Anda. Kredensi tersebut harus memiliki izin untuk mengakses AWS sumber daya, seperti kluster Amazon Redshift. Bagian berikut memberikan detail tentang bagaimana Anda dapat menggunakan [AWS Identity and Access Management \(IAM\)](#) dan Amazon Redshift untuk membantu mengamankan sumber daya Anda dengan mengontrol siapa yang dapat mengaksesnya:

- [Mengautentikasi dengan identitas](#)
- [Kontrol akses](#)

Important

Topik ini berisi kumpulan praktik terbaik untuk mengelola izin, identitas, dan akses aman. Kami menyarankan Anda untuk membiasakan diri dengan praktik terbaik untuk menggunakan IAM dengan Amazon Redshift. Ini termasuk menggunakan peran IAM untuk

menerapkan izin. Memiliki pemahaman yang baik tentang bagian-bagian ini akan membantu Anda mempertahankan gudang data Amazon Redshift yang lebih aman.

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS](#).

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [Menandatangani permintaan AWS API](#) di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat [Autentikasi multi-faktor](#) dalam Panduan Pengguna AWS IAM Identity Center dan [Menggunakan autentikasi multi-faktor \(MFA\) dalam AWS](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan

untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat [Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang](#) dalam Panduan Pengguna IAM.

[Grup IAM](#) adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat [Kapan harus membuat pengguna IAM \(bukan peran\)](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan [beralih peran](#). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat [Menggunakan peran IAM](#) dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Membuat peran untuk Penyedia Identitas pihak ketiga](#) dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat [Set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM](#).
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
- Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses maju](#).
- Peran layanan – Peran layanan adalah [peran IAM](#) yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2](#) dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat [Kapan harus membuat peran IAM \(bukan pengguna\)](#) dalam Panduan Pengguna IAM.

Kontrol akses

Anda dapat memiliki kredensi yang valid untuk mengautentikasi permintaan Anda, tetapi kecuali Anda memiliki izin, Anda tidak dapat membuat atau mengakses sumber daya Amazon Redshift. Misalnya, Anda harus memiliki izin untuk membuat klaster Amazon Redshift, membuat snapshot, menambahkan langganan acara, dan sebagainya.

Bagian berikut menjelaskan cara mengelola izin untuk Amazon Redshift. Anda sebaiknya membaca gambaran umum terlebih dahulu.

- [Ikhtisar mengelola izin akses ke sumber daya Amazon Redshift](#)
- [Menggunakan kebijakan berbasis identitas \(kebijakan IAM\) untuk Amazon Redshift](#)

Ikhtisar mengelola izin akses ke sumber daya Amazon Redshift

Setiap AWS sumber daya dimiliki oleh AWS akun, dan izin untuk membuat atau mengakses sumber daya diatur oleh kebijakan izin. Administrator akun dapat melampirkan kebijakan izin ke identitas IAM (yaitu, pengguna, grup, dan peran), dan beberapa layanan (seperti AWS Lambda) juga mendukung melampirkan kebijakan izin ke sumber daya.

Note

Administrator akun (atau pengguna administrator) adalah pengguna dengan hak akses administrator. Untuk informasi selengkapnya, lihat [Praktik terbaik IAM](#) dalam Panduan Pengguna IAM.

Saat memberikan izin, Anda memutuskan siapa yang mendapatkan izin, sumber daya mana yang mereka dapatkan izin, dan tindakan spesifik yang ingin Anda izinkan pada sumber daya tersebut.

Sumber daya dan operasi Amazon Redshift

Amazon Redshift menyediakan sumber daya, tindakan, dan kunci konteks kondisi khusus layanan untuk digunakan dalam kebijakan izin IAM.

Amazon Redshift, Amazon Redshift Tanpa Server, Amazon Redshift Data API, dan izin akses editor kueri Amazon Redshift v2

Saat menyiapkan [Kontrol akses](#), Anda menulis kebijakan izin yang dapat dilampirkan ke identitas IAM (kebijakan berbasis identitas). Untuk informasi referensi terperinci, lihat topik berikut di Referensi Otorisasi Layanan:

- Untuk Amazon Redshift, lihat [Tindakan, sumber daya, dan kunci kondisi untuk Amazon Redshift](#) yang menggunakan awalan. `redshift`:
- Untuk Amazon Redshift Tanpa Server, lihat [Tindakan, sumber daya, dan kunci kondisi untuk Amazon Redshift Tanpa Server yang menggunakan awalan](#). `redshift-serverless`:
- Untuk Amazon Redshift Data API, lihat [Tindakan, sumber daya, dan kunci kondisi untuk Amazon Redshift Data API](#) yang menggunakan awalan. `redshift-data`:
- Untuk editor kueri Amazon Redshift v2, lihat [Tindakan, sumber daya, dan kunci kondisi untuk AWS SQL Workbench \(editor kueri Amazon Redshift v2\)](#) yang menggunakan awalan. `sqlworkbench`:

Editor kueri v2 menyertakan tindakan khusus izin yang tidak secara langsung sesuai dengan operasi API. Tindakan ini ditunjukkan dalam Referensi Otorisasi Layanan dengan `[permission only]`.

Referensi Otorisasi Layanan berisi informasi tentang operasi API mana yang dapat digunakan dalam kebijakan IAM. Ini juga mencakup AWS sumber daya yang dapat Anda berikan izin, dan kunci kondisi

yang dapat Anda sertakan untuk kontrol akses berbutir halus. Untuk informasi lebih lanjut tentang syarat, lihat [Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci](#).

Anda menentukan tindakan di bidang Action kebijakan, nilai sumber daya di bidang Resource kebijakan, dan syarat di bidang Condition kebijakan. Untuk menentukan tindakan Amazon Redshift, gunakan `redshift:` awalan yang diikuti dengan nama operasi API (misalnya,).

```
redshift:CreateCluster
```

Memahami kepemilikan sumber daya

Pemilik sumber daya adalah AWS akun yang membuat sumber daya. Artinya, pemilik sumber daya adalah AWS akun entitas utama (akun root, pengguna IAM, atau peran IAM) yang mengautentikasi permintaan yang membuat sumber daya. Contoh berikut menggambarkan cara kerjanya:

- Jika Anda menggunakan kredensi akun root AWS akun Anda untuk membuat cluster DB, AWS akun Anda adalah pemilik sumber daya Amazon Redshift.
- Jika Anda membuat peran IAM di AWS akun Anda dengan izin untuk membuat sumber daya Amazon Redshift, siapa pun yang dapat mengambil peran tersebut dapat membuat sumber daya Amazon Redshift. AWS Akun Anda, tempat perannya berada, memiliki sumber daya Amazon Redshift.
- Jika Anda membuat pengguna IAM di AWS akun Anda dan memberikan izin untuk membuat sumber daya Amazon Redshift kepada pengguna tersebut, pengguna dapat membuat sumber daya Amazon Redshift. Namun, AWS akun Anda, tempat pengguna berada, memiliki sumber daya Amazon Redshift. Dalam kebanyakan kasus, metode ini tidak disarankan. Sebaiknya buat peran IAM dan melampirkan izin ke peran tersebut, lalu menetapkan peran tersebut ke pengguna.

Mengelola akses ke sumber daya

Kebijakan izin menjelaskan siapa yang memiliki akses ke apa. Bagian berikut menjelaskan opsi yang tersedia untuk membuat kebijakan izin.

Note

Bagian ini membahas penggunaan IAM dalam konteks Amazon Redshift. Bagian ini tidak memberikan informasi yang mendetail tentang layanan IAM. Untuk dokumentasi lengkap IAM, lihat [Apa yang Dimaksud dengan IAM?](#) dalam Panduan Pengguna IAM. Untuk informasi

tentang sintaksis dan penjelasan kebijakan IAM, lihat [AWS Referensi Kebijakan IAM](#) dalam Panduan Pengguna IAM.

Kebijakan yang terlampir pada identitas IAM disebut kebijakan (kebijakan IAM) berbasis identitas dan kebijakan yang dilampirkan pada sumber daya disebut kebijakan berbasis sumber daya. Amazon Redshift hanya mendukung kebijakan berbasis identitas (kebijakan IAM).

Kebijakan berbasis identitas (kebijakan IAM)

Anda dapat menetapkan izin dengan melampirkan kebijakan ke peran IAM dan kemudian menetapkan peran tersebut ke pengguna atau grup. Berikut ini adalah contoh kebijakan yang berisi izin untuk membuat, menghapus, memodifikasi, dan me-reboot klaster Amazon Redshift untuk akun Anda. AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowManageClusters",
      "Effect": "Allow",
      "Action": [
        "redshift:CreateCluster",
        "redshift>DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": "*"
    }
  ]
}
```

Untuk informasi selengkapnya tentang penggunaan kebijakan berbasis identitas dengan Amazon Redshift, lihat. [Menggunakan kebijakan berbasis identitas \(kebijakan IAM\) untuk Amazon Redshift](#) Untuk informasi lebih lanjut tentang pengguna, kelompok, peran, dan izin, lihat [Identitas \(Pengguna, Grup, dan Peran\)](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Layanan lain, seperti Amazon S3, juga mendukung kebijakan izin berbasis sumber daya. Misalnya, Anda dapat melampirkan kebijakan ke bucket S3 untuk mengelola izin akses ke bucket tersebut. Amazon Redshift tidak mendukung kebijakan berbasis sumber daya.

Menentukan elemen kebijakan: Tindakan, efek, sumber daya, dan prinsipal

[Untuk setiap resource Amazon Redshift \(lihat Sumber daya dan operasi Amazon Redshift\), layanan mendefinisikan satu set operasi API \(lihat Tindakan\).](#) Untuk memberikan izin untuk operasi API ini, Amazon Redshift mendefinisikan serangkaian tindakan yang dapat Anda tentukan dalam kebijakan. Melakukan operasi API akan memerlukan izin untuk lebih dari satu tindakan.

Berikut ini adalah elemen-elemen kebijakan dasar:

- Sumber daya – Dalam kebijakan, Anda menggunakan Amazon Resource Name (ARN) untuk mengidentifikasi sumber daya yang diatur kebijakan. Untuk informasi selengkapnya, lihat [Sumber daya dan operasi Amazon Redshift](#).
- Tindakan – Anda menggunakan kata kunci tindakan untuk mengidentifikasi operasi sumber daya yang ingin Anda izinkan atau tolak. Misalnya, `redshift:DescribeClusters` izin memungkinkan izin pengguna untuk melakukan operasi Amazon DescribeClusters Redshift.
- Efek – Anda menentukan efek ketika pengguna meminta tindakan tertentu—efek ini dapat berupa pemberian izin atau penolakan. Jika Anda tidak secara eksplisit memberikan akses ke (mengizinkan) sumber daya, akses akan ditolak secara implisit. Anda juga dapat secara eksplisit menolak akses ke sumber daya, yang mungkin Anda lakukan untuk memastikan bahwa pengguna tidak dapat mengaksesnya, meskipun kebijakan yang berbeda memberikan akses.
- Principal – Dalam kebijakan berbasis identitas (Kebijakan IAM), pengguna yang kebijakannya terlampir adalah principal yang implisit. Untuk kebijakan berbasis sumber daya, Anda menentukan pengguna, akun, layanan, atau entitas lain yang diinginkan untuk menerima izin (berlaku hanya untuk kebijakan berbasis sumber daya). Amazon Redshift tidak mendukung kebijakan berbasis sumber daya.

Untuk mempelajari lebih lanjut tentang sintaks dan deskripsi kebijakan IAM, lihat [referensi kebijakan AWS IAM](#) di Panduan Pengguna IAM.

Untuk tabel yang menunjukkan semua tindakan Amazon Redshift API dan resource yang diterapkan, lihat [Amazon Redshift, Amazon Redshift Tanpa Server, Amazon Redshift Data API, dan izin akses editor kueri Amazon Redshift v2](#)

Menentukan kondisi dalam kebijakan

Ketika Anda memberikan izin, Anda dapat menggunakan bahasa kebijakan akses untuk menentukan syarat kapan kebijakan akan berlaku. Misalnya, Anda mungkin ingin kebijakan diterapkan hanya setelah tanggal tertentu. Untuk informasi selengkapnya tentang menentukan kondisi dalam bahasa kebijakan akses, lihat [elemen kebijakan IAM JSON: Kondisi](#) dalam Panduan Pengguna IAM.

Untuk mengidentifikasi kondisi di mana kebijakan izin berlaku, sertakan `Condition` elemen dalam kebijakan izin IAM Anda. Misalnya, Anda dapat membuat kebijakan yang mengizinkan pengguna membuat kluster menggunakan `redshift:CreateCluster` tindakan, dan Anda dapat menambahkan `Condition` elemen untuk membatasi pengguna tersebut agar hanya membuat kluster di wilayah tertentu. Lihat perinciannya di [Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci](#). Untuk daftar yang menampilkan semua nilai kunci kondisi dan tindakan serta sumber daya Amazon Redshift yang diterapkan, lihat [Amazon Redshift, Amazon Redshift Tanpa Server, Amazon Redshift Data API, dan izin akses editor kueri Amazon Redshift v2](#)

Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci

Di Amazon Redshift, Anda dapat menggunakan tombol kondisi untuk membatasi akses ke sumber daya berdasarkan tag untuk sumber daya tersebut. Berikut ini adalah kunci kondisi Amazon Redshift yang umum.

Kunci syarat	Deskripsi
<code>aws:RequestTag</code>	Mengharuskan pengguna untuk menyertakan kunci tag (nama) dan nilai setiap kali mereka membuat sumber daya. Untuk informasi selengkapnya, lihat aws: RequestTag di Panduan Pengguna IAM.
<code>aws:ResourceTag</code>	Membatasi akses pengguna ke sumber daya berdasarkan kunci dan nilai tag tertentu. Untuk informasi selengkapnya, lihat aws: ResourceTag di Panduan Pengguna IAM.
<code>aws:TagKeys</code>	Gunakan kunci ini untuk membandingkan kunci tanda dalam permintaan dengan kunci yang Anda sebutkan dalam kebijakan. Untuk informasi selengkapnya, lihat aws: TagKeys di Panduan Pengguna IAM.

Untuk informasi tentang tag, lihat [Ikhtisar penandaan](#).

Untuk daftar tindakan API yang mendukung kunci `redshift:RequestTag` dan `redshift:ResourceTag` kondisi, lihat [Amazon Redshift](#), [Amazon Redshift Tanpa Server](#), [Amazon Redshift Data API](#), dan [izin akses editor kueri Amazon Redshift v2](#).

Kunci kondisi berikut dapat digunakan dengan tindakan Amazon Redshift `GetClusterCredentials`.

Kunci syarat	Deskripsi
<code>redshift:DurationSeconds</code>	Membatasi jumlah detik yang dapat ditentukan untuk durasi.
<code>redshift:DbName</code>	Membatasi nama database yang dapat ditentukan.
<code>redshift:DbUser</code>	Membatasi nama pengguna database yang dapat ditentukan.

Contoh 1: Membatasi akses dengan menggunakan `aws:ResourceTag` condition key

Gunakan kebijakan IAM berikut untuk mengizinkan pengguna memodifikasi kluster Amazon Redshift hanya untuk akun AWS tertentu di `us-west-2` wilayah dengan tag `environment` bernama dengan nilai tag sebesar `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"
      }
    }
  }
}
```

Contoh 2: Membatasi akses dengan menggunakan aws: RequestTag condition key

Gunakan kebijakan IAM berikut untuk mengizinkan pengguna membuat kluster Amazon Redshift hanya jika perintah untuk membuat kluster menyertakan tag usage bernama dan nilai tag. production Kondisi dengan aws:TagKeys dan ForAllValues pengubah menentukan bahwa hanya kunci costcenter dan usage dapat ditentukan dalam permintaan.

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

Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk Amazon Redshift

Topik ini memberikan contoh kebijakan berbasis identitas di mana administrator akun dapat melampirkan kebijakan izin ke identitas IAM (yaitu, pengguna, grup, dan peran).

Important

Kami menyarankan Anda terlebih dahulu meninjau topik pengantar yang menjelaskan konsep dasar dan opsi yang tersedia bagi Anda untuk mengelola akses ke sumber daya Amazon

Redshift Anda. Untuk informasi selengkapnya, lihat [Ikhtisar mengelola izin akses ke sumber daya Amazon Redshift](#).

Berikut adalah contoh kebijakan izin. Kebijakan ini memungkinkan pengguna untuk membuat, menghapus, memodifikasi, dan me-reboot semua kluster, lalu menolak izin untuk menghapus atau memodifikasi kluster tempat pengenalan kluster dimulai dengan in dan. production Wilayah AWS us-west-2 Akun AWS 123456789012

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowClusterManagement",
      "Action": [
        "redshift:CreateCluster",
        "redshift>DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "DenyDeleteModifyProtected",
      "Action": [
        "redshift>DeleteCluster",
        "redshift:ModifyCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:cluster:production*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

Kebijakan tersebut memiliki dua pernyataan:

- Pernyataan pertama memberikan izin bagi pengguna kepada pengguna untuk membuat, menghapus, memodifikasi, dan me-reboot cluster. Pernyataan tersebut menetapkan karakter wildcard (*) sebagai Resource nilai sehingga kebijakan tersebut berlaku untuk semua resource Amazon Redshift yang dimiliki oleh akun root. AWS
- Pernyataan kedua menolak izin untuk menghapus atau memodifikasi cluster. Pernyataan tersebut menentukan klaster Amazon Resource Name (ARN) untuk nilai Resource yang menyertakan karakter wildcard (*). Akibatnya, pernyataan ini berlaku untuk semua cluster Amazon Redshift yang dimiliki oleh AWS akun root tempat pengidentifikasi cluster dimulai. `production`

AWS kebijakan terkelola untuk Amazon Redshift

AWS mengatasi banyak kasus penggunaan umum dengan menyediakan kebijakan IAM mandiri yang dibuat dan dikelola oleh AWS Kebijakan terkelola memberikan izin yang diperlukan untuk kasus penggunaan umum sehingga Anda tidak perlu menyelidiki izin apa yang diperlukan. Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

Anda juga dapat membuat kebijakan IAM kustom Anda sendiri untuk mengizinkan izin untuk operasi dan sumber daya Amazon Redshift API. Anda dapat melampirkan kebijakan kustom ini ke IAM role atau grup yang memerlukan izin tersebut.

Bagian berikut menjelaskan kebijakan AWS terkelola, yang dapat Anda lampirkan ke pengguna di akun Anda, dan khusus untuk Amazon Redshift.

AmazonRedshiftReadOnlyAkses

Memberikan akses hanya-baca ke semua sumber daya Amazon Redshift untuk sebuah akun. AWS

Anda dapat menemukan kebijakan [AmazonRedshiftReadOnlyAccess](#) di konsol IAM dan [AmazonRedshiftReadOnlyAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AmazonRedshiftFullAccess

Memberikan akses penuh ke semua sumber daya Amazon Redshift untuk AWS sebuah akun. Selain itu, kebijakan ini memberikan akses penuh ke semua sumber daya Amazon Redshift Tanpa Server.

Anda dapat menemukan [AmazonRedshiftFullAccess](#) kebijakan di konsol IAM dan [AmazonRedshiftFullAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AmazonRedshiftQueryEditor

Memberikan akses penuh ke editor kueri di konsol Amazon Redshift.

Anda dapat menemukan [AmazonRedshiftQueryEditor](#) kebijakan di konsol IAM dan [AmazonRedshiftQueryEditor](#) di Panduan Referensi Kebijakan AWS Terkelola.

AmazonRedshiftDataFullAkses

Memberikan akses penuh ke operasi Amazon Redshift Data API dan sumber daya untuk AWS akun.

Anda dapat menemukan kebijakan [AmazonRedshiftDataFullAccess](#) di konsol IAM dan [AmazonRedshiftDataFullAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AmazonRedshiftQueryEditorV2 FullAccess

Memberikan akses penuh ke operasi dan sumber daya Amazon Redshift query editor v2. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan.

Anda dapat menemukan FullAccess kebijakan [AmazonRedshiftQueryEditorV2](#) di konsol IAM dan [AmazonRedshiftQueryEditorV2 FullAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AmazonRedshiftQueryEditorV2 NoSharing

Memberikan kemampuan untuk bekerja dengan editor kueri Amazon Redshift v2 tanpa berbagi sumber daya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Prinsipal yang menggunakan kebijakan ini tidak dapat menandai sumber dayanya (seperti kueri) untuk membagikannya dengan prinsipal lain dalam hal yang sama. Akun AWS

Anda dapat menemukan NoSharing kebijakan [AmazonRedshiftQueryEditorV2](#) di konsol IAM dan [AmazonRedshiftQueryEditorV2 NoSharing](#) di Panduan Referensi Kebijakan AWS Terkelola.

AmazonRedshiftQueryEditorV2 ReadSharing

Memberikan kemampuan untuk bekerja dengan editor kueri Amazon Redshift v2 dengan berbagi sumber daya yang terbatas. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Prinsipal yang menggunakan kebijakan ini dapat menandai sumber dayanya (seperti kueri) untuk membagikannya dengan prinsipal lain dalam hal yang sama. Akun AWS Prinsipal yang diberikan dapat membaca sumber daya yang dibagikan dengan timnya tetapi tidak dapat memperbaruinya.

Anda dapat menemukan ReadSharing kebijakan [AmazonRedshiftQueryEditorV2](#) di konsol IAM dan [AmazonRedshiftQueryEditorV2 ReadSharing](#) di Panduan Referensi Kebijakan AWS Terkelola.

AmazonRedshiftQueryEditorReadWriteBerbagi V2

Memberikan kemampuan untuk bekerja dengan editor kueri Amazon Redshift v2 dengan berbagi sumber daya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Prinsipal yang menggunakan kebijakan ini dapat menandai sumber dayanya (seperti kueri) untuk membagikannya dengan prinsipal lain dalam hal yang sama. Akun AWS Kepala sekolah yang diberikan dapat membaca dan memperbarui sumber daya yang dibagikan dengan timnya.

Anda dapat menemukan kebijakan [ReadWriteBerbagi AmazonRedshift QueryEditor V2](#) di konsol IAM dan [ReadWriteBerbagi AmazonRedshift QueryEditor V2](#) di Panduan Referensi Kebijakan AWS Terkelola.

AmazonRedshiftServiceLinkedRolePolicy

Anda tidak dapat melampirkan AmazonRedshiftServiceLinkedRolePolicy ke entitas IAM Anda. Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan Amazon Redshift mengakses sumber daya akun. Untuk informasi selengkapnya, lihat [Menggunakan peran terkait layanan untuk Amazon Redshift](#).

Anda dapat menemukan [AmazonRedshiftServiceLinkedRolePolicy](#) kebijakan di konsol IAM dan [AmazonRedshiftServiceLinkedRolePolicy](#) di Panduan Referensi Kebijakan AWS Terkelola.

AmazonRedshiftAllCommandsFullAccess

Memberikan kemampuan untuk menggunakan peran IAM yang dibuat dari konsol Amazon Redshift dan mengaturnya sebagai default untuk cluster untuk menjalankan perintah COPY dari Amazon S3, UNLOAD, CREATE EXTERNAL SCHEMA, CREATE EXTERNAL FUNCTION, dan CREATE MODEL. Kebijakan ini juga memberikan izin untuk menjalankan pernyataan SELECT untuk layanan terkait, seperti Amazon S3, CloudWatch Log, Amazon SageMaker, atau AWS Glue

Anda dapat menemukan [AmazonRedshiftAllCommandsFullAccess](#) kebijakan di konsol IAM dan [AmazonRedshiftAllCommandsFullAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

Anda juga dapat membuat kebijakan IAM kustom Anda sendiri untuk mengizinkan izin untuk operasi dan sumber daya Amazon Redshift API. Anda dapat melampirkan kebijakan kustom ini ke IAM role atau grup yang memerlukan izin tersebut.

Pembaruan Amazon Redshift ke kebijakan terkelola AWS

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon Redshift sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Amazon Redshift.

Perubahan	Deskripsi	Tanggal
AmazonRedshiftQueryEditorV2 FullAccess — Pembaruan ke kebijakan yang sudah ada	Izin untuk tindakan <code>redshift-serverless:ListNamespaces</code> dan <code>redshift-serverless:ListWorkgroups</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk mencantumkan ruang nama tanpa server dan grup kerja tanpa server di gudang data Amazon Redshift.	Februari 21, 2024
AmazonRedshiftQueryEditorV2 NoSharing – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>redshift-serverless:ListNamespaces</code> dan <code>redshift-serverless:ListWorkgroups</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk mencantumkan ruang nama tanpa server dan grup kerja tanpa server di gudang data Amazon Redshift.	Februari 21, 2024
AmazonRedshiftQueryEditorV2 ReadSharing –	Izin untuk tindakan <code>redshift-serverless</code>	Februari 21, 2024

Perubahan	Deskripsi	Tanggal
Pembaruan ke kebijakan yang ada	s:ListNamespaces dan redshift-serverless:ListWorkgroups ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk mencantumkan ruang nama tanpa server dan grup kerja tanpa server di gudang data Amazon Redshift.	
AmazonRedshiftQueryEditorReadWriteBerbagi V2 – Pembaruan ke kebijakan yang ada	Izin untuk tindakan redshift-serverless:ListNamespaces dan redshift-serverless:ListWorkgroups ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk mencantumkan ruang nama tanpa server dan grup kerja tanpa server di gudang data Amazon Redshift.	Februari 21, 2024
AmazonRedshiftReadOnlyAkses – Pembaruan ke kebijakan yang ada	Izin untuk tindakan redshift:ListRecommendations ditambahkan ke kebijakan terkelola. Ini memberikan izin untuk mencantumkan rekomendasi Amazon Redshift Advisor.	Februari 7, 2024

Perubahan	Deskripsi	Tanggal
AmazonRedshiftServiceLinkedRolePolicy – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>ec2:AssignIpv6Addresses</code> dan <code>ec2:UnassignIpv6Addresses</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk menetapkan dan membatalkan penetapan alamat IP.	31 Oktober 2023
AmazonRedshiftQueryEditorV2 NoSharing – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:GetAutocompletionMetadata</code> dan <code>sqlworkbench:GetAutocompletionResource</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk menghasilkan dan mengambil informasi database untuk penyelesaian otomatis SQL saat mengedit kueri.	16 Agustus 2023
AmazonRedshiftQueryEditorV2 ReadSharing – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:GetAutocompletionMetadata</code> dan <code>sqlworkbench:GetAutocompletionResource</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk menghasilkan dan mengambil informasi database untuk penyelesaian otomatis SQL saat mengedit kueri.	16 Agustus 2023

Perubahan	Deskripsi	Tanggal
AmazonRedshiftQueryEditorReadWriteBerbagi V2 – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:GetAutocompletionMetadata</code> dan <code>sqlworkbench:GetAutocompletionResource</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk menghasilkan dan mengambil informasi database untuk penyelesaian otomatis SQL saat mengedit kueri.	16 Agustus 2023

Perubahan	Deskripsi	Tanggal
AmazonRedshiftServiceLinkedRolePolicy – Pembaruan ke kebijakan yang ada	<p>Izin untuk tindakan AWS Secrets Manager untuk membuat dan mengelola rahasia ditambahkan ke kebijakan terkelola. Izin yang ditambahkan adalah sebagai berikut:</p> <ul style="list-style-type: none">• <code>secretsmanager:GetRandomPassword</code>• <code>secretsmanager:DescribeSecret</code>• <code>secretsmanager:PutSecretValue</code>• <code>secretsmanager:UpdateSecret</code>• <code>secretsmanager:UpdateSecretVersionStage</code>• <code>secretsmanager:RotateSecret</code>• <code>secretsmanager>DeleteSecret</code>	Agustus 14, 2023

Perubahan	Deskripsi	Tanggal
AmazonRedshiftServiceLinkedRolePolicy – Pembaruan ke kebijakan yang ada	<p>Izin untuk tindakan di Amazon EC2 untuk membuat dan mengelola grup keamanan dan aturan perutean dihapus dari kebijakan terkelola. Izin ini berkaitan dengan pembuatan subnet dan VPC. Izin yang dihapus adalah sebagai berikut:</p> <ul style="list-style-type: none">• <code>ec2:AuthorizeSecurityGroupEgress</code>• <code>ec2:AuthorizeSecurityGroupIngress</code>• <code>ec2:UpdateSecurityGroupRuleDescriptionsEgress</code>• <code>ec2:ReplaceRouteTableAssociation</code>• <code>ec2:CreateRouteTable</code>• <code>ec2:AttachInternetGateway</code>• <code>ec2:UpdateSecurityGroupRuleDescriptionsIngress</code>• <code>ec2:AssociateRouteTable</code>• <code>ec2:RevokeSecurityGroupIngress</code>• <code>ec2:CreateRoute</code>• <code>ec2:CreateSecurityGroup</code>	08 Mei 2023

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none"> • ec2:RevokeSecurityGroupEgress • ec2:ModifyVpcAttribute • ec2:CreateSubnet • ec2:CreateInternetGateway • ec2:CreateVpc <p>Ini terkait dengan tag Purpose: RedshiftMigrate ToVpc resource. Tag membatasi cakupan izin untuk tugas untuk Amazon EC2 Classic ke migrasi VPC Amazon EC2. Untuk informasi selengkapnya tentang tag sumber daya, lihat Mengontrol akses ke AWS sumber daya menggunakan tag.</p>	
AmazonRedshiftData FullAkses – Pembaruan ke kebijakan yang ada	Izin untuk tindakan redshift:GetClusterCredentialsWithIAM ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk mendapatkan kredensial sementara yang disempurnakan untuk mengakses database Amazon Redshift dengan yang ditentukan. Akun AWS	April 7, 2023

Perubahan	Deskripsi	Tanggal
AmazonRedshiftServiceLinkedRolePolicy – Pembaruan ke kebijakan yang ada	Izin untuk tindakan di Amazon EC2 untuk pembuatan dan pengelolaan aturan grup keamanan ditambahkan ke kebijakan terkelola. Grup dan aturan keamanan ini secara khusus terkait dengan tag <code>aws:RequestTag/Redshift</code> sumber daya Amazon Redshift. Ini membatasi ruang lingkup izin untuk sumber daya Amazon Redshift tertentu.	April 06, 2023
AmazonRedshiftQueryEditorV2 NoSharing – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:GetSchemaInference</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk mendapatkan kolom dan tipe data yang disimpulkan dari file.	21 Maret 2023
AmazonRedshiftQueryEditorV2 ReadSharing – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:GetSchemaInference</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk mendapatkan kolom dan tipe data yang disimpulkan dari file.	21 Maret 2023

Perubahan	Deskripsi	Tanggal
AmazonRedshiftQueryEditorReadWriteBerbagi V2 – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:GetSchemaInference</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk mendapatkan kolom dan tipe data yang disimpulkan dari file.	21 Maret 2023
AmazonRedshiftQueryEditorV2 NoSharing – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:AssociateNotebookWithTab</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk membuat dan memperbarui tab yang ditautkan ke buku catatan pengguna sendiri.	2 Februari 2023
AmazonRedshiftQueryEditorV2 ReadSharing – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:AssociateNotebookWithTab</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk membuat dan memperbarui tab yang ditautkan ke buku catatan pengguna sendiri atau ke buku catatan yang dibagikan dengannya.	2 Februari 2023

Perubahan	Deskripsi	Tanggal
AmazonRedshiftQueryEditorReadWriteBerbagi V2 – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:AssociateNotebookWithTab</code> ditambahkan ke kebijakan terkelola. Menambahkannya memberikan izin untuk membuat dan memperbarui tab yang ditautkan ke buku catatan pengguna sendiri atau ke buku catatan yang dibagikan dengannya.	2 Februari 2023

Perubahan	Deskripsi	Tanggal
<p>AmazonRedshiftQueryEditorV2 NoSharing – Pembaruan ke kebijakan yang ada</p>	<p>Untuk memberikan izin menggunakan buku catatan, Amazon Redshift menambahkan izin untuk tindakan berikut:</p> <ul style="list-style-type: none"> • <code>sqlworkbench:ListNotebooks</code> • <code>sqlworkbench:CreateNotebook</code> • <code>sqlworkbench:DuplicateNotebook</code> • <code>sqlworkbench:CreateNotebookFromVersion</code> • <code>sqlworkbench:ImportNotebook</code> • <code>sqlworkbench:GetNotebook</code> • <code>sqlworkbench:UpdateNotebook</code> • <code>sqlworkbench>DeleteNotebook</code> • <code>sqlworkbench:CreateNotebookCell</code> • <code>sqlworkbench>DeleteNotebookCell</code> • <code>sqlworkbench:UpdateNotebookCellContent</code> • <code>sqlworkbench:UpdateNotebookCellLayout</code> 	<p>Oktober 17, 2022</p>

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none">• <code>sqlworkbench:BatchGetNotebookCell</code>• <code>sqlworkbench:ListNotebookVersions</code>• <code>sqlworkbench:CreateNotebookVersion</code>• <code>sqlworkbench:GetNotebookVersion</code>• <code>sqlworkbench>DeleteNotebookVersion</code>• <code>sqlworkbench:RestoreNotebookVersion</code>• <code>sqlworkbench:ExportNotebook</code>	

Perubahan	Deskripsi	Tanggal
<p>AmazonRedshiftQueryEditorV2 ReadSharing – Pembaruan ke kebijakan yang ada</p>	<p>Untuk memberikan izin menggunakan buku catatan, Amazon Redshift menambahkan izin untuk tindakan berikut:</p> <ul style="list-style-type: none"> • <code>sqlworkbench:ListNotebooks</code> • <code>sqlworkbench:CreateNotebook</code> • <code>sqlworkbench:DuplicateNotebook</code> • <code>sqlworkbench:CreateNotebookFromVersion</code> • <code>sqlworkbench:ImportNotebook</code> • <code>sqlworkbench:GetNotebook</code> • <code>sqlworkbench:UpdateNotebook</code> • <code>sqlworkbench>DeleteNotebook</code> • <code>sqlworkbench:CreateNotebookCell</code> • <code>sqlworkbench>DeleteNotebookCell</code> • <code>sqlworkbench:UpdateNotebookCellContent</code> • <code>sqlworkbench:UpdateNotebookCellLayout</code> 	<p>Oktober 17, 2022</p>

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none">• <code>sqlworkbench:BatchGetNotebookCell</code>• <code>sqlworkbench:ListNotebookVersions</code>• <code>sqlworkbench:CreateNotebookVersion</code>• <code>sqlworkbench:GetNotebookVersion</code>• <code>sqlworkbench>DeleteNotebookVersion</code>• <code>sqlworkbench:RestoreNotebookVersion</code>• <code>sqlworkbench:ExportNotebook</code>	

Perubahan	Deskripsi	Tanggal
<p>AmazonRedshiftQueryEditorReadWriteBerbagi V2 – Pembaruan ke kebijakan yang ada</p>	<p>Untuk memberikan izin menggunakan buku catatan, Amazon Redshift menambahkan izin untuk tindakan berikut:</p> <ul style="list-style-type: none"> • <code>sqlworkbench:ListNotebooks</code> • <code>sqlworkbench:CreateNotebook</code> • <code>sqlworkbench:DuplicateNotebook</code> • <code>sqlworkbench:CreateNotebookFromVersion</code> • <code>sqlworkbench:ImportNotebook</code> • <code>sqlworkbench:GetNotebook</code> • <code>sqlworkbench:UpdateNotebook</code> • <code>sqlworkbench>DeleteNotebook</code> • <code>sqlworkbench:CreateNotebookCell</code> • <code>sqlworkbench>DeleteNotebookCell</code> • <code>sqlworkbench:UpdateNotebookCellContent</code> • <code>sqlworkbench:UpdateNotebookCellLayout</code> 	<p>Oktober 17, 2022</p>

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none"> • <code>sqlworkbench:BatchGetNotebookCell</code> • <code>sqlworkbench:ListNotebookVersions</code> • <code>sqlworkbench:CreateNotebookVersion</code> • <code>sqlworkbench:GetNotebookVersion</code> • <code>sqlworkbench>DeleteNotebookVersion</code> • <code>sqlworkbench:RestoreNotebookVersion</code> • <code>sqlworkbench:ExportNotebook</code> 	
AmazonRedshiftServiceLinkedRolePolicy – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan namespace AWS/Redshift untuk memungkinkan metrik penerbitan. CloudWatch	7 September 2022
AmazonRedshiftQueryEditorV2 NoSharing – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin ke tindakan <code>sqlworkbench:ListQueryExecutionHistory</code> dan <code>sqlworkbench:GetQueryExecutionHistory</code> Ini memberikan izin untuk melihat riwayat kueri.	30 Agustus 2022

Perubahan	Deskripsi	Tanggal
AmazonRedshiftQueryEditorV2 ReadSharing – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin ke tindakan <code>sqlworkbench:ListQueryExecutionHistory</code> dan <code>sqlworkbench:GetQueryExecutionHistory</code> . Ini memberikan izin untuk melihat riwayat kueri.	30 Agustus 2022
AmazonRedshiftQueryEditorReadWriteBerbagi V2 – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin ke tindakan <code>sqlworkbench:ListQueryExecutionHistory</code> dan <code>sqlworkbench:GetQueryExecutionHistory</code> . Ini memberikan izin untuk melihat riwayat kueri.	30 Agustus 2022
AmazonRedshiftFullAccess – Pembaruan ke kebijakan yang ada	Izin untuk Amazon Redshift Tanpa Server ditambahkan ke kebijakan terkelola yang ada. <code>AmazonRedshiftFullAccess</code>	22 Juli 2022

Perubahan	Deskripsi	Tanggal
AmazonRedshiftData FullAkses – Pembaruan ke kebijakan yang ada	Amazon Redshift memperbarui kondisi pelingkupan <code>redshift-serverless:GetCredentials default aws:ResourceTag/RedshiftDataFullAccess</code> izin tag dari <code>StringEquals</code> untuk memberikan akses <code>StringLike</code> ke sumber daya yang ditandai dengan kunci <code>RedshiftDataFullAccess</code> tag dan nilai tag apa pun.	Juli 11, 2022
AmazonRedshiftData FullAkses – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin baru <code>redshift-serverless:GetCredentials</code> untuk memungkinkan kredensial sementara ke Amazon Redshift Tanpa Server.	8 Juli 2022
AmazonRedshiftQueryEditorV2 NoSharing – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin untuk tindakan tersebut. <code>sqlworkbench:GetAccountSettings</code> Ini memberikan izin untuk mendapatkan pengaturan akun.	15 Juni 2022

Perubahan	Deskripsi	Tanggal
AmazonRedshiftQueryEditorV2 ReadSharing – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin untuk tindakan tersebut. <code>sqlworkbench:GetAccountSettings</code> Ini memberikan izin untuk mendapatkan pengaturan akun.	15 Juni 2022
AmazonRedshiftQueryEditorReadWriteBerbagi V2 – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin untuk tindakan tersebut. <code>sqlworkbench:GetAccountSettings</code> Ini memberikan izin untuk mendapatkan pengaturan akun.	15 Juni 2022
AmazonRedshiftServiceLinkedRolePolicy – Pembaruan ke kebijakan yang ada	Untuk mengaktifkan akses publik ke titik akhir Amazon Redshift Serverless baru, Amazon Redshift mengalokasikan dan mengaitkan alamat IP Elastic ke antarmuka jaringan Elastic titik akhir VPC di akun pelanggan. Ini dilakukan melalui izin yang diberikan melalui peran terkait layanan. Untuk mengaktifkan kasus penggunaan ini, tindakan untuk mengalokasikan dan merilis alamat IP Elastis ditambahkan ke peran terkait layanan Amazon Redshift Tanpa Server.	26 Mei 2022

Perubahan	Deskripsi	Tanggal
AmazonRedshiftQueryEditorV2 FullAccess – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:ListTaggedResources</code> . Ini dicakup secara khusus untuk sumber daya editor kueri Amazon Redshift v2. Pembaruan kebijakan ini memberikan hak untuk menelepon <code>tag:GetResources</code> hanya melalui editor kueri v2.	Februari 22, 2022
AmazonRedshiftQueryEditorV2 NoSharing – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:ListTaggedResources</code> . Ini dicakup secara khusus untuk sumber daya editor kueri Amazon Redshift v2. Pembaruan kebijakan ini memberikan hak untuk menelepon <code>tag:GetResources</code> hanya melalui editor kueri v2.	Februari 22, 2022
AmazonRedshiftQueryEditorV2 ReadSharing – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:ListTaggedResources</code> . Ini dicakup secara khusus untuk sumber daya editor kueri Amazon Redshift v2. Pembaruan kebijakan ini memberikan hak untuk menelepon <code>tag:GetResources</code> hanya melalui editor kueri v2.	Februari 22, 2022

Perubahan	Deskripsi	Tanggal
AmazonRedshiftQueryEditorReadWriteBerbagi V2 – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:ListTaggedResources</code> . Ini dicakup secara khusus untuk sumber daya editor kueri Amazon Redshift v2. Pembaruan kebijakan ini memberikan hak untuk menelepon <code>tag:GetResources</code> hanya melalui editor kueri v2.	Februari 22, 2022
AmazonRedshiftQueryEditorV2 ReadSharing – Pembaruan ke kebijakan yang ada	Izin untuk tindakan <code>sqlworkbench:AssociateQueryWithTab</code> ditambahkan ke kebijakan terkelola. Menambahkannya memungkinkan pelanggan untuk membuat tab editor yang ditautkan ke kueri yang dibagikan dengan mereka.	Februari 22, 2022
AmazonRedshiftServiceLinkedRolePolicy – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin untuk tindakan baru guna memungkinkan pengelolaan jaringan Amazon Redshift dan sumber daya VPC.	22 November 2021

Perubahan	Deskripsi	Tanggal
AmazonRedshiftAllCommandsFullAccess – Kebijakan baru	Amazon Redshift menambahkan kebijakan baru untuk mengizinkan penggunaan peran IAM yang dibuat dari konsol Amazon Redshift dan mengaturnya sebagai default untuk kluster untuk menjalankan perintah COPY dari Amazon S3, UNLOAD, CREATE EXTERNAL SCHEMA, CREATE EXTERNAL FUNCTION, CREATE MODEL, atau CREATE LIBRARY.	18 November 2021
AmazonRedshiftServiceLinkedRolePolicy – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin untuk tindakan baru guna memungkinkan pengelolaan grup CloudWatch log Amazon Redshift dan aliran log, termasuk ekspor log audit.	15 November 2021
AmazonRedshiftFullAccess – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin baru untuk memungkinkan penjelasan model, DynamoDB, Redshift Spectrum, dan federasi Amazon RDS.	Oktober 07, 2021
AmazonRedshiftQueryEditorV2 FullAccess – Kebijakan baru	Amazon Redshift menambahkan kebijakan baru untuk mengizinkan akses penuh ke editor kueri Amazon Redshift v2.	24 September 2021

Perubahan	Deskripsi	Tanggal
AmazonRedshiftQueryEditorV2 NoSharing – Kebijakan baru	Amazon Redshift menambahkan kebijakan baru untuk mengizinkan penggunaan editor kueri Amazon Redshift v2 tanpa berbagi sumber daya.	24 September 2021
AmazonRedshiftQueryEditorV2 ReadSharing – Kebijakan baru	Amazon Redshift menambahkan kebijakan baru untuk mengizinkan berbagi baca dalam editor kueri Amazon Redshift v2.	24 September 2021
AmazonRedshiftQueryEditorReadWriteBerbagi V2 – Kebijakan baru	Amazon Redshift menambahkan kebijakan baru untuk mengizinkan pembacaan dan pembaruan berbagi dalam editor kueri Amazon Redshift v2.	24 September 2021
AmazonRedshiftFullAccess – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin baru untuk mengizinkan. <code>sagemaker:*Job*</code>	18 Agustus 2021
AmazonRedshiftDataFullAkses – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin baru untuk mengizinkan. <code>AuthorizeDataShare</code>	Agustus 12, 2021
AmazonRedshiftDataFullAkses – Pembaruan ke kebijakan yang ada	Amazon Redshift menambahkan izin baru untuk mengizinkan. <code>BatchExecuteStatement</code>	27 Juli 2021
Amazon Redshift mulai melacak perubahan	Amazon Redshift mulai melacak perubahan untuk kebijakan AWS terkelolanya.	27 Juli 2021

Izin diperlukan untuk menggunakan Redshift Spectrum

Amazon Redshift Spectrum memerlukan izin ke layanan AWS lain untuk mengakses sumber daya. Untuk detail tentang izin dalam kebijakan IAM untuk Redshift Spectrum, lihat kebijakan [IAM untuk Amazon Redshift Spectrum di Panduan Pengembang Database Amazon](#) Redshift.

Izin diperlukan untuk menggunakan konsol Amazon Redshift

Agar pengguna dapat bekerja dengan konsol Amazon Redshift, pengguna tersebut harus memiliki seperangkat izin minimum yang memungkinkan pengguna mendeskripsikan sumber daya Amazon Redshift untuk akun mereka. AWS Izin ini juga harus memungkinkan pengguna untuk menjelaskan informasi terkait lainnya, termasuk keamanan Amazon EC2, Amazon, CloudWatch Amazon SNS, dan informasi jaringan.

Jika Anda membuat kebijakan IAM yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk pengguna dengan kebijakan IAM. Untuk memastikan bahwa pengguna tersebut masih dapat menggunakan konsol Amazon Redshift, lampirkan juga kebijakan `AmazonRedshiftReadOnlyAccess` terkelola ke pengguna. Cara melakukan ini dijelaskan dalam [AWS kebijakan terkelola untuk Amazon Redshift](#).

Untuk informasi yang dapat memberi pengguna akses ke editor kueri di konsol Amazon Redshift, lihat. [Izin diperlukan untuk menggunakan editor kueri konsol Amazon Redshift](#)

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau Amazon Redshift API.

Izin diperlukan untuk menggunakan editor kueri konsol Amazon Redshift

Agar pengguna dapat bekerja dengan editor kueri Amazon Redshift, pengguna tersebut harus memiliki set izin minimum untuk operasi Amazon Redshift dan Amazon Redshift Data API. Untuk terhubung ke database menggunakan rahasia, Anda juga harus memiliki izin Secrets Manager.

Untuk memberi pengguna akses ke editor kueri di konsol Amazon Redshift, lampirkan kebijakan `AmazonRedshiftQueryEditor` dan `AmazonRedshiftReadOnlyAccess` AWS terkelola. `AmazonRedshiftQueryEditor` Kebijakan ini memungkinkan izin pengguna untuk mengambil hasil hanya pernyataan SQL mereka sendiri. Artinya, pernyataan yang diajukan sama `aws:userid` seperti yang ditunjukkan pada bagian kebijakan yang `AmazonRedshiftQueryEditor` AWS dikelola ini.

```
{
```

```

    "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}"
        }
    }
}

```

Untuk memungkinkan pengguna mengambil hasil pernyataan SQL orang lain dalam peran IAM yang sama, buat kebijakan Anda sendiri tanpa syarat untuk membatasi akses ke pengguna saat ini. Batasi juga akses untuk mengubah kebijakan ke administrator.

Izin yang diperlukan untuk menggunakan editor kueri v2

Agar pengguna dapat bekerja dengan editor kueri Amazon Redshift v2, pengguna tersebut harus memiliki set izin minimum untuk Amazon Redshift, operasi editor kueri v2, dan AWS layanan lain seperti AWS Key Management Service, dan layanan penandaan. AWS Secrets Manager

Untuk memberi pengguna akses penuh ke editor kueri v2, lampirkan kebijakan `AmazonRedshiftQueryEditorV2FullAccess` AWS terkelola.

`AmazonRedshiftQueryEditorV2FullAccess` kebijakan ini memungkinkan izin pengguna untuk berbagi sumber daya editor kueri v2, seperti kueri, dengan orang lain di tim yang sama. Untuk detail tentang cara akses ke resource editor kueri v2 dikendalikan, lihat definisi kebijakan terkelola khusus untuk editor kueri v2 di konsol IAM.

Beberapa kebijakan AWS terkelola Amazon Redshift query editor v2 menggunakan AWS tag dalam kondisi untuk cakupan akses ke sumber daya. Dalam editor kueri v2, kueri berbagi didasarkan pada kunci tag dan nilai `"aws:ResourceTag/sqlworkbench-team": "${aws:PrincipalTag/sqlworkbench-team}"` dalam kebijakan IAM yang dilampirkan pada prinsipal (peran IAM). Prinsipal yang sama Akun AWS dengan nilai tag yang sama (misalnya, `accounting-team`), berada di tim yang sama di editor kueri v2. Anda hanya dapat dikaitkan dengan satu tim pada satu waktu. Pengguna dengan izin administratif dapat mengatur tim di konsol IAM dengan memberi semua anggota tim nilai yang sama untuk tag tersebut `sqlworkbench-team`. Jika nilai tag diubah

untuk pengguna IAM atau peran IAM, mungkin ada penundaan hingga perubahan tercermin dalam sumber daya bersama. `sqlworkbench-team` Jika nilai tag sumber daya (seperti kueri) diubah, sekali lagi mungkin ada penundaan hingga perubahan tercermin. Anggota tim juga harus memiliki tag `:GetResources` izin untuk berbagi.

Contoh: Untuk menambahkan **accounting-team** tag untuk peran IAM

1. Masuk ke AWS Management Console dan buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi konsol, pilih Peran lalu pilih nama peran yang ingin Anda edit.
3. Pilih tab Tag dan kemudian pilih Tambahkan tag.
4. Tambahkan kunci tag `sqlworkbench-team` dan nilainya. `accounting-team`
5. Pilih Simpan perubahan.

Sekarang ketika prinsipal IAM (dengan peran IAM ini terlampir) berbagi kueri dengan tim, prinsipal lain dengan nilai `accounting-team` tag yang sama dapat melihat kueri.

Untuk informasi selengkapnya tentang cara melampirkan tag ke prinsipal, termasuk peran IAM dan pengguna IAM, lihat [Menandai sumber daya IAM](#) di Panduan Pengguna IAM.

Anda juga dapat mengatur tim di tingkat sesi menggunakan Penyedia Identitas (iDP). Hal ini memungkinkan beberapa pengguna yang menggunakan peran IAM yang sama untuk memiliki tim yang berbeda. Kebijakan kepercayaan peran IAM harus memungkinkan `sts:TagSession` operasi. Untuk informasi selengkapnya, lihat [Izin yang diperlukan untuk menambahkan tag sesi](#) di Panduan Pengguna IAM. Tambahkan atribut tag utama ke pernyataan SAMP yang disediakan oleh idP Anda.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:sqlworkbench-team">
  <AttributeValue>accounting-team</AttributeValue>
</Attribute>
```

Ikuti petunjuk untuk penyedia Identitas (iDP) Anda untuk mengisi atribut SAMP dengan konten yang berasal dari direktori Anda. Untuk informasi selengkapnya tentang Penyedia identitas (IdPs) dan Amazon Redshift, lihat [Menggunakan otentikasi IAM untuk menghasilkan kredensi pengguna basis data](#) dan [Penyedia identitas dan federasi](#) di Panduan Pengguna IAM.

`sqlworkbench>CreateNotebookVersion` Memberikan izin untuk mendapatkan konten sel notebook saat ini dan membuat versi buku catatan di akun Anda. Artinya,

pada saat pembuatan versi, konten notebook saat ini sama dengan konten versi. Kemudian, konten sel dalam versi tetap sama dengan notebook saat ini diperbarui. `sqlworkbench:GetNotebookVersion` memberikan izin untuk mendapatkan versi notebook. Pengguna yang tidak memiliki `sqlworkbench:BatchGetNotebookCell` izin tetapi memiliki `sqlworkbench>CreateNotebookVersion` dan `sqlworkbench:GetNotebookVersion` izin pada notebook memiliki akses ke sel notebook dalam versi. Pengguna ini tanpa `sqlworkbench:BatchGetNotebookCell` izin masih dapat mengambil konten sel notebook dengan terlebih dahulu membuat versi dan kemudian mendapatkan versi yang dibuat ini.

Izin diperlukan untuk menggunakan penjadwal Amazon Redshift

Saat Anda menggunakan penjadwal Amazon Redshift, Anda menyiapkan peran IAM dengan hubungan kepercayaan dengan penjadwal Amazon Redshift (**`scheduler.redshift.amazonaws.com`**) untuk memungkinkan penjadwal menerima izin atas nama Anda. Anda juga melampirkan kebijakan (izin) ke peran untuk operasi Amazon Redshift API yang ingin Anda jadwalkan.

Contoh berikut menunjukkan dokumen kebijakan dalam format JSON untuk menyiapkan hubungan kepercayaan dengan penjadwal Amazon Redshift dan Amazon Redshift.

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

Untuk informasi selengkapnya tentang entitas trust, lihat [Membuat peran untuk mendelegasikan izin ke AWS layanan di Panduan Pengguna IAM](#).

Anda juga harus menambahkan izin untuk operasi Amazon Redshift yang ingin Anda jadwalkan.

Agar penjadwal dapat menggunakan `ResizeCluster` operasi, tambahkan izin yang mirip dengan kebijakan IAM Anda berikut ini. Tergantung pada lingkungan Anda, Anda mungkin ingin membuat kebijakan lebih ketat.

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

Untuk langkah-langkah membuat peran bagi penjadwal Amazon Redshift, lihat [Membuat peran untuk AWS layanan \(konsol\)](#) di Panduan Pengguna IAM. Buat pilihan ini saat Anda membuat peran di konsol IAM:

- Untuk Pilih layanan yang akan menggunakan peran ini: Pilih Redshift.
- Untuk Pilih kasus penggunaan Anda: Pilih Redshift - Scheduler.
- Buat atau lampirkan kebijakan ke peran yang memungkinkan operasi Amazon Redshift dijadwalkan. Pilih Buat kebijakan atau ubah peran untuk melampirkan kebijakan. Masukkan kebijakan JSON untuk operasi yang akan dijadwalkan.
- Setelah Anda membuat peran, edit Hubungan Kepercayaan peran IAM untuk menyertakan `layanaredshift.amazonaws.com`.

Peran IAM yang Anda buat memiliki entitas tepercaya `scheduler.redshift.amazonaws.com` dan `redshift.amazonaws.com`. Ini juga memiliki kebijakan terlampir yang memungkinkan tindakan Amazon Redshift API yang didukung, seperti, `"redshift:ResizeCluster"`

Izin diperlukan untuk menggunakan penjadwal Amazon EventBridge

Saat Anda menggunakan EventBridge penjadwal Amazon, Anda menyiapkan peran IAM dengan hubungan kepercayaan dengan EventBridge scheduler (**`events.amazonaws.com`**) untuk memungkinkan penjadwal menerima izin atas nama Anda. Anda juga melampirkan kebijakan (izin) ke peran untuk operasi Amazon Redshift Data API yang ingin Anda jadwalkan dan kebijakan untuk operasi Amazon EventBridge .

Anda menggunakan EventBridge penjadwal saat membuat kueri terjadwal dengan editor kueri Amazon Redshift di konsol.

Anda dapat membuat peran IAM untuk menjalankan kueri terjadwal di konsol IAM. Dalam peran IAM ini, lampirkan `AmazonEventBridgeFullAccess` dan `AmazonRedshiftDataFullAccess`.

Contoh berikut menunjukkan dokumen kebijakan dalam format JSON untuk mengatur hubungan kepercayaan dengan EventBridge penjadwal.

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

Untuk informasi selengkapnya tentang entitas trust, lihat [Membuat peran untuk mendelegasikan izin ke AWS layanan di Panduan Pengguna IAM](#).

Untuk langkah-langkah membuat peran bagi EventBridge penjadwal, lihat [Membuat peran untuk AWS layanan \(konsol\)](#) di Panduan Pengguna IAM. Buat pilihan ini saat Anda membuat peran di konsol IAM:

- Untuk Pilih layanan yang akan menggunakan peran ini: Pilih CloudWatch Acara.
- Untuk Pilih kasus penggunaan Anda: Pilih CloudWatch Acara.
- Lampirkan kebijakan izin berikut: `AmazonEventBridgeFullAccess` dan `AmazonRedshiftDataFullAccess`.

Peran IAM yang Anda buat memiliki entitas tepercaya. `events.amazonaws.com` Ini juga memiliki kebijakan terlampir yang memungkinkan tindakan API Data Amazon Redshift yang didukung, seperti, `"redshift-data:*"`

Izin yang diperlukan untuk menggunakan machine learning Amazon Redshift (ML)

Berikut ini, Anda dapat menemukan deskripsi izin yang diperlukan untuk menggunakan pembelajaran mesin Amazon Redshift (ML) untuk berbagai kasus penggunaan.

Agar pengguna Anda dapat menggunakan Amazon Redshift ML dengan Amazon SageMaker, buat peran IAM dengan kebijakan yang lebih ketat daripada default. Anda dapat menggunakan kebijakan berikut. Anda juga dapat mengubah kebijakan ini untuk memenuhi kebutuhan Anda.

Kebijakan berikut menunjukkan izin yang diperlukan untuk menjalankan SageMaker Autopilot dengan penjelasan model dari Amazon Redshift.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
      ],
      "Resource": [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",

```

```

        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:PutMetricData"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "cloudwatch:namespace": [
                "SageMaker",
                "/aws/sagemaker/Endpoints",
                "/aws/sagemaker/ProcessingJobs",
                "/aws/sagemaker/TrainingJobs",
                "/aws/sagemaker/TransformJobs"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
    ]
}

```



```

    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetBucketAcl",
      "s3:GetBucketCors",
      "s3:GetEncryptionConfiguration",
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets",
      "s3:ListMultipartUploadParts",
      "s3:ListBucketMultipartUploads",
      "s3:PutObject",
      "s3:PutBucketAcl",
      "s3:PutBucketCors",
      "s3:DeleteObject",
      "s3:AbortMultipartUpload",
      "s3:CreateBucket"
    ],
    "Resource": [
      "arn:aws:s3:::redshift-downloads",
      "arn:aws:s3:::redshift-downloads/*",
      "arn:aws:s3::*:redshift*",
      "arn:aws:s3::*:redshift/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetBucketAcl",
      "s3:GetBucketCors",
      "s3:GetEncryptionConfiguration",
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets",
      "s3:ListMultipartUploadParts",
      "s3:ListBucketMultipartUploads",
      "s3:PutObject",
      "s3:PutBucketAcl",
      "s3:PutBucketCors",

```

```

        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
    ],
    "Resource": "*",
    "Condition": {
        "StringEqualsIgnoreCase": {
            "s3:ExistingObjectTag/Redshift": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::*:role/*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "redshift.amazonaws.com",
                "sagemaker.amazonaws.com"
            ]
        }
    }
}
]
}

```

Kebijakan berikut menunjukkan izin minimal penuh untuk mengizinkan akses ke Amazon DynamoDB, Redshift Spectrum, dan federasi Amazon RDS.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateAutoMLJob",
                "sagemaker:CreateCompilationJob",
                "sagemaker:CreateEndpoint",
                "sagemaker:DescribeAutoMLJob",
            ]
        }
    ]
}

```

```

        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
    ],
    "Resource": [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:PutMetricData"
    ],

```

```

    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "cloudwatch:namespace": [
          "SageMaker",
          "/aws/sagemaker/Endpoints",
          "/aws/sagemaker/ProcessingJobs",
          "/aws/sagemaker/TrainingJobs",
          "/aws/sagemaker/TransformJobs"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ecr:BatchCheckLayerAvailability",
      "ecr:BatchGetImage",
      "ecr:GetAuthorizationToken",
      "ecr:GetDownloadUrlForLayer"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetBucketAcl",
      "s3:GetBucketCors",
      "s3:GetEncryptionConfiguration",
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets",
      "s3:ListMultipartUploadParts",
      "s3:ListBucketMultipartUploads",
      "s3:PutObject",
      "s3:PutBucketAcl",
      "s3:PutBucketCors",
      "s3:DeleteObject",
      "s3:AbortMultipartUpload",
      "s3:CreateBucket"
    ],
    "Resource": [
      "arn:aws:s3:::redshift-downloads",

```

```

        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3::*redshift*",
        "arn:aws:s3::*redshift*/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3>DeleteObject",
        "s3:AbortMultipartUpload",
        "s3>CreateBucket"
    ],
    "Resource": "*",
    "Condition": {
        "StringEqualsIgnoreCase": {
            "s3:ExistingObjectTag/Redshift": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "dynamodb:Scan",
        "dynamodb:DescribeTable",
        "dynamodb:Getitem"
    ],
    "Resource": [
        "arn:aws:dynamodb::*:table/*redshift*",
        "arn:aws:dynamodb::*:table/*redshift*/index/*"
    ]
},
{

```

```

    "Effect": "Allow",
    "Action": [
        "elasticmapreduce:ListInstances"
    ],
    "Resource": [
        "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "elasticmapreduce:ListInstances"
    ],
    "Resource": "*",
    "Condition": {
        "StringEqualsIgnoreCase": {
            "elasticmapreduce:ResourceTag/Redshift": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": "arn:aws:lambda:*:*:function:*redshift*"
},
{
    "Effect": "Allow",
    "Action": [
        "glue:CreateDatabase",
        "glue>DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue>DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue>DeletePartition",
    ]
}

```

```

        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
    ],
    "Resource": [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
    ],
    "Resource": [
        "arn:aws:secretsmanager:*:*:secret:*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "secretsmanager:ResourceTag/Redshift": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "arn:aws:iam:*:*:role/*",
    "Condition": {

```

```

        "StringEquals": {
            "iam:PassedToService": [
                "redshift.amazonaws.com",
                "glue.amazonaws.com",
                "sagemaker.amazonaws.com",
                "athena.amazonaws.com"
            ]
        }
    ]
}

```

Secara opsional, untuk menggunakan AWS KMS kunci enkripsi, tambahkan izin berikut ke kebijakan.

```

{
    "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>"
    ]
}

```

Untuk mengizinkan Amazon Redshift dan SageMaker mengasumsikan peran IAM sebelumnya untuk berinteraksi dengan layanan lain, tambahkan kebijakan kepercayaan berikut ke peran tersebut.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "redshift.amazonaws.com",
                    "sagemaker.amazonaws.com",
                    "forecast.amazonaws.com"
                ]
            }
        }
    ]
}

```



```

    },
    "Action": "sts:AssumeRole"
  }
]
}

```

Di urutan sebelumnya, `redshift-downloads/redshift-ml/` bucket Amazon S3 adalah lokasi penyimpanan data sampel yang digunakan untuk langkah dan contoh lain. Anda dapat menghapus bucket ini jika Anda tidak perlu memuat data dari Amazon S3. Atau ganti dengan bucket Amazon S3 lain yang Anda gunakan untuk memuat data ke Amazon Redshift.

your-s3-bucketNilai**your-account-id**,**your-role**, dan adalah ID akun, peran, dan bucket yang Anda tentukan dalam perintah CREATE MODEL.

Secara opsional, Anda dapat menggunakan bagian AWS KMS kunci dari kebijakan sampel jika Anda menentukan AWS KMS kunci untuk digunakan dengan Amazon Redshift ML. **your-kms-key**Nilai adalah kunci yang Anda gunakan sebagai bagian dari perintah CREATE MODEL Anda.

Saat Anda menentukan private virtual private cloud (VPC) untuk pekerjaan tuning hyperparameter, tambahkan izin berikut.

```

{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
    ]
}

```

Untuk bekerja dengan penjelasan model, pastikan Anda memiliki izin untuk memanggil operasi SageMaker API. Kami menyarankan Anda menggunakan kebijakan `AmazonSageMakerFullAccess` terkelola. Jika Anda ingin membuat peran IAM dengan kebijakan yang lebih ketat, gunakan kebijakan berikut ini.

```
{
  "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": "*"
    }
  ]
}
```

Untuk informasi selengkapnya tentang kebijakan `AmazonSageMakerFullAccess` terkelola, lihat [AmazonSageMakerFullAkses](#) di Panduan SageMaker Pengembang Amazon.

Jika Anda ingin membuat model Forecast, sebaiknya gunakan kebijakan `AmazonForecastFullAccess` terkelola. Jika Anda ingin menggunakan kebijakan yang lebih ketat, tambahkan kebijakan berikut ke peran IAM Anda.

```
{
  "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": "*"
}
]
}

```

[Untuk informasi selengkapnya tentang Amazon Redshift ML, lihat Menggunakan machine learning di Amazon Redshift atau CREATE MODEL.](#)

Izin untuk konsumsi streaming

Streaming ingestion bekerja dengan dua layanan. Ini adalah Kinesis Data Streams dan Amazon MSK.

Izin yang diperlukan untuk menggunakan konsumsi streaming dengan Kinesis Data Streams

Prosedur dengan contoh kebijakan terkelola tersedia di [Memulai dengan konsumsi streaming dari Amazon Kinesis Data Streams](#).

Izin yang diperlukan untuk menggunakan streaming ingestion dengan Amazon MSK

Prosedur dengan contoh kebijakan terkelola tersedia di [Memulai dengan konsumsi streaming dari Amazon Managed Streaming for Apache Kafka](#).

Izin yang diperlukan untuk menggunakan operasi API berbagi data

Untuk mengontrol akses ke operasi API berbagi data, gunakan kebijakan berbasis tindakan IAM. Untuk informasi tentang cara mengelola kebijakan IAM, lihat [Mengelola kebijakan IAM](#) di Panduan Pengguna IAM.

Secara khusus, anggaplah administrator cluster produser perlu menggunakan `AuthorizeDataShare` panggilan untuk mengotorisasi jalan keluar untuk datashare di luar file. Akun AWS Dalam hal ini, Anda menyiapkan kebijakan berbasis tindakan IAM untuk memberikan izin ini. Gunakan `DeauthorizeDataShare` panggilan untuk mencabut jalan keluar.

Saat menggunakan kebijakan berbasis tindakan IAM, Anda juga dapat menentukan sumber daya IAM dalam kebijakan, seperti. DataShareARN Berikut ini menunjukkan format dan contoh untuk 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
```

Anda dapat membatasi `AuthorizeDataShare` akses ke datashare tertentu dengan menentukan nama datashare dalam kebijakan IAM.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/SalesShare"
      ],
      "Effect": "Deny"
    }
  ]
}
```

Anda juga dapat membatasi kebijakan IAM untuk semua datashares yang dimiliki oleh cluster produsen tertentu. Untuk melakukannya, ganti **datashare-name** nilai dalam kebijakan dengan wildcard atau tanda bintang. Pertahankan namespace-guid nilai cluster.

```
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/*
```

Berikut ini adalah kebijakan IAM yang mencegah entitas memanggil `AuthorizeDataShare` datashares yang dimiliki oleh cluster produsen tertentu.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
```

```

    ],
    "Resource": [
      "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/*"
    ],
    "Effect": "Deny"
  }
]
}

```

DataShareARN membatasi akses berdasarkan nama datashare dan global unique ID (GUID) untuk namespace cluster yang memiliki. Ini dilakukan dengan menentukan nama sebagai tanda bintang.

Kebijakan sumber daya untuk GetClusterCredentials

Untuk terhubung ke database cluster menggunakan koneksi JDBC atau ODBC dengan kredensial database IAM, atau untuk memanggil `GetClusterCredentials` tindakan secara terprogram, Anda memerlukan set izin minimum. Minimal, Anda memerlukan izin untuk memanggil `redshift:GetClusterCredentials` tindakan dengan akses ke `dbuser` sumber daya.

Jika Anda menggunakan koneksi JDBC atau ODBC, bukan `server` dan `port` Anda dapat menentukan `cluster_id` dan `region`, tetapi untuk melakukannya kebijakan Anda harus mengizinkan `redshift:DescribeClusters` tindakan dengan akses ke sumber daya `cluster`.

Jika Anda memanggil `GetClusterCredentials` dengan parameter opsional `AutocreateDbGroups`, `DbName`, dan, pastikan juga mengizinkan tindakan dan mengizinkan akses ke sumber daya yang tercantum dalam tabel berikut.

GetClusterCredentials parameter	Tindakan	Sumber Daya
Autocreate	<code>redshift:CreateClusterUser</code>	<code>dbuser</code>
DbGroups	<code>redshift:JoinGroup</code>	<code>dbgroup</code>

GetClusterCredentials parameter	Tindakan	Sumber Daya
DbName	TA	dbname

Untuk informasi selengkapnya tentang sumber daya, lihat [Sumber daya dan operasi Amazon Redshift](#).

Anda juga dapat memasukkan ketentuan berikut dalam polis Anda:

- `redshift:DurationSeconds`
- `redshift:DbName`
- `redshift:DbUser`

Untuk informasi lebih lanjut tentang syarat, lihat [Menentukan kondisi dalam kebijakan](#).

Contoh kebijakan yang dikelola pelanggan

Di bagian ini, Anda dapat menemukan contoh kebijakan pengguna yang memberikan izin untuk berbagai tindakan Amazon Redshift. Kebijakan ini berfungsi saat Anda menggunakan Amazon Redshift API, AWS SDK, atau file. AWS CLI

Note

Semua contoh menggunakan Region US West (Oregon) (`us-west-2`) dan berisi ID akun fiktif.

Contoh 1: Izinkan pengguna akses penuh ke semua tindakan dan sumber daya Amazon Redshift

Kebijakan berikut memungkinkan akses ke semua tindakan Amazon Redshift di semua sumber daya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
    "Sid": "AllowRedshift",
    "Action": [
      "redshift:*"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
```

Nilai `redshift:*` dalam `Action` elemen menunjukkan semua tindakan di Amazon Redshift.

Contoh 2: Tolak akses pengguna ke serangkaian tindakan Amazon Redshift

Secara default, semua izin ditolak. Namun, terkadang Anda perlu secara eksplisit menolak akses ke tindakan atau serangkaian tindakan tertentu. Kebijakan berikut memungkinkan akses ke semua tindakan Amazon Redshift dan secara eksplisit menolak akses ke tindakan Amazon Redshift di mana nama dimulai. `Delete` Kebijakan ini berlaku untuk semua sumber daya Amazon Redshift di `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:*"
    }
  ]
}
```

Contoh 3: Izinkan pengguna untuk mengelola cluster

Kebijakan berikut memungkinkan pengguna untuk membuat, menghapus, memodifikasi, dan me-reboot semua cluster, lalu menolak izin untuk menghapus klaster mana pun di mana nama cluster dimulai. `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"
    }
  ]
}
```

Contoh 4: Izinkan pengguna untuk mengotorisasi dan mencabut akses snapshot

Kebijakan berikut memungkinkan pengguna, misalnya Pengguna A, untuk melakukan hal berikut:

- Otorisasi akses ke snapshot apa pun yang dibuat dari cluster bernama. `shared`
- Cabut akses snapshot untuk snapshot apa pun yang dibuat dari `shared` cluster tempat nama snapshot dimulai. `revokable`


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSharedSnapshots",
      "Action": [
        "redshift:AuthorizeSnapshotAccess"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:shared/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "AllowRevokableSnapshot",
      "Action": [
        "redshift:RevokeSnapshotAccess"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/revokable*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Jika Pengguna A telah mengizinkan Pengguna B mengakses snapshot, Pengguna B harus memiliki kebijakan seperti berikut ini untuk mengizinkan Pengguna B memulihkan klaster dari snapshot. Kebijakan berikut memungkinkan Pengguna B untuk mendeskripsikan dan memulihkan dari snapshot, dan membuat cluster. Nama cluster ini harus dimulai dengan `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"
  }
]
}

```

Contoh 5: Izinkan pengguna menyalin snapshot cluster dan memulihkan cluster dari snapshot

Kebijakan berikut memungkinkan pengguna untuk menyalin snapshot apa pun yang dibuat dari kluster bernama `big-cluster-1`, dan memulihkan snapshot apa pun tempat nama snapshot dimulai. `snapshot-for-restore`

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCopyClusterSnapshot",
      "Action": [
        "redshift:CopyClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:big-cluster-1/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "AllowRestoreFromClusterSnapshot",
      "Action": [
        "redshift:RestoreFromClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/snapshot-for-restore*",
        "arn:aws:redshift:us-west-2:123456789012:cluster:*"
      ]
    }
  ]
}

```

```

    ],
    "Effect": "Allow"
  }
]
}

```

Contoh 6: Izinkan pengguna mengakses Amazon Redshift, serta tindakan serta sumber daya umum untuk layanan terkait AWS

Kebijakan contoh berikut memungkinkan akses ke semua tindakan dan sumber daya untuk Amazon Redshift, Amazon Simple Notification Service (Amazon SNS), dan Amazon CloudWatch. Ini juga memungkinkan tindakan yang ditentukan pada semua sumber daya Amazon EC2 terkait di bawah akun.

Note

Izin tingkat sumber daya tidak didukung untuk tindakan Amazon EC2 yang ditentukan dalam kebijakan contoh ini.

```

{
  "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": [
      "*"
    ]
  }
]
}

```

Contoh 7: Izinkan pengguna menandai sumber daya dengan konsol Amazon Redshift

Kebijakan contoh berikut memungkinkan pengguna untuk menandai sumber daya dengan konsol Amazon Redshift menggunakan AWS Resource Groups Kebijakan ini dapat dilampirkan ke peran pengguna yang memanggil konsol Amazon Redshift baru atau asli. Untuk informasi lebih lanjut tentang penandaan, lihat [Menandai sumber daya di Amazon Redshift](#).

```

{
  "Version": "2012-10-17",

```

```

    "Statement": [
      {
        "Sid": "Tagging permissions",
        "Effect": "Allow",
        "Action": [
          "redshift:DeleteTags",
          "redshift:CreateTags",
          "redshift:DescribeTags",
          "tag:UntagResources",
          "tag:TagResources"
        ],
        "Resource": "*"
      }
    ]
  }

```

Contoh kebijakan untuk menggunakan GetClusterCredentials

Kebijakan berikut menggunakan nilai parameter sampel ini:

- Wilayah: us-west-2
- AWS Akun: 123456789012
- Nama cluster: examplecluster

Kebijakan berikut memungkinkan `GetCredentials`, `CreateClusterUser`, dan `JoinGroup` tindakan. Kebijakan ini menggunakan kunci kondisi untuk mengizinkan `GetClusterCredentials` dan `CreateClusterUser` tindakan hanya jika ID AWS pengguna cocok `"AIDI0DR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"`. Akses IAM diminta untuk `"testdb"` database saja. Kebijakan ini juga memungkinkan pengguna untuk bergabung dengan grup bernama `"common_group"`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GetClusterCredsStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:GetClusterCredentials"
      ],
      "Resource": [

```

```

    "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
    ${redshift:DbUser}",
    "arn:aws:redshift:us-west-2:123456789012:dbname:examplecluster/testdb",
    "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
  ],
  "Condition": {
    "StringEquals": {
      "aws:userid": "AIDIO4R4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
    }
  }
},
{
  "Sid": "CreateClusterUserStatement",
  "Effect": "Allow",
  "Action": [
    "redshift:CreateClusterUser"
  ],
  "Resource": [
    "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
    ${redshift:DbUser}"
  ],
  "Condition": {
    "StringEquals": {
      "aws:userid": "AIDIO4R4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
    }
  }
},
{
  "Sid": "RedshiftJoinGroupStatement",
  "Effect": "Allow",
  "Action": [
    "redshift:JoinGroup"
  ],
  "Resource": [
    "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
  ]
}
]
}

```

Federasi penyedia identitas asli (iDP) untuk Amazon Redshift

Mengelola identitas dan izin untuk Amazon Redshift menjadi lebih mudah dengan federasi penyedia identitas asli karena memanfaatkan penyedia identitas yang ada untuk menyederhanakan autentikasi dan mengelola izin. Ini dilakukan dengan memungkinkan untuk berbagi metadata identitas ke Redshift dari penyedia identitas Anda. Untuk iterasi pertama fitur ini, penyedia identitas yang didukung adalah [Microsoft Azure Active Directory \(Azure AD\)](#).

Untuk mengonfigurasi Amazon Redshift sehingga dapat mengautentikasi identitas dari penyedia identitas pihak ketiga, Anda mendaftarkan penyedia identitas dengan Amazon Redshift. Melakukan hal ini memungkinkan Redshift untuk mengautentikasi pengguna dan peran yang ditentukan oleh penyedia identitas. Dengan demikian Anda dapat menghindari keharusan melakukan manajemen identitas terperinci di penyedia identitas pihak ketiga Anda dan di Amazon Redshift, karena informasi identitas dibagikan.

Untuk informasi tentang penggunaan peran sesi yang ditransfer dari grup penyedia identitas (IDP), lihat [PG_GET_SESSION_ROLES](#) di Panduan Pengembang Database Amazon Redshift.

Menyiapkan penyedia identitas di Amazon Redshift

Bagian ini menunjukkan langkah-langkah untuk mengonfigurasi penyedia identitas dan Amazon Redshift untuk menjalin komunikasi bagi federasi penyedia identitas asli. Anda memerlukan akun aktif dengan penyedia identitas Anda. Sebelum mengonfigurasi Amazon Redshift, Anda mendaftarkan Redshift sebagai aplikasi dengan penyedia identitas Anda, memberikan persetujuan administrator.

Selesaikan langkah-langkah berikut di Amazon Redshift:

1. Anda menjalankan pernyataan SQL untuk mendaftarkan penyedia identitas, termasuk deskripsi metadata aplikasi Azure. Untuk membuat penyedia identitas di Amazon Redshift, jalankan perintah berikut setelah mengganti nilai parameter issuer, client_id, client_secret, dan audience. Parameter ini khusus untuk Microsoft Azure AD. Ganti nama penyedia identitas dengan nama yang Anda pilih, dan ganti namespace dengan nama unik untuk memuat pengguna dan peran dari direktori penyedia identitas Anda.

```
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"]
}'
```

Jenis ini azure menunjukkan bahwa penyedia secara khusus memfasilitasi komunikasi dengan Microsoft Azure AD. Ini adalah satu-satunya penyedia identitas pihak ketiga yang didukung.

- penerbit - ID penerbit untuk dipercaya ketika token diterima. Pengidentifikasi unik untuk tenant_id ditambahkan ke penerbit.
- client_id - Pengidentifikasi publik yang unik dari aplikasi yang terdaftar dengan penyedia identitas. Ini dapat disebut sebagai ID aplikasi.
- client_secret - Pengidentifikasi rahasia, atau kata sandi, yang hanya diketahui oleh penyedia identitas dan aplikasi terdaftar.
- audiens - ID Aplikasi yang ditugaskan ke aplikasi di Azure.

Alih-alih menggunakan rahasia klien bersama, Anda dapat mengatur parameter untuk menentukan sertifikat, kunci pribadi, dan kata sandi kunci pribadi saat membuat penyedia identitas.

```
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"}';
```

Kata sandi kunci pribadi, client_pk_password, adalah opsional.

2. Opsional: Jalankan perintah SQL di Amazon Redshift untuk membuat pengguna dan peran sebelumnya. Ini memfasilitasi pemberian izin terlebih dahulu. Nama peran di Amazon Redshift adalah seperti berikut: < GroupName pada Azure <Namespace>AD>. Misalnya, ketika Anda membuat grup di Microsoft Azure AD dipanggil rsgroup dan namespace dipanggil aad, nama peran adalah. aad:rsgroup Nama pengguna dan peran di Amazon Redshift ditentukan dari nama pengguna dan keanggotaan grup ini di namespace penyedia identitas.

Pemetaan untuk peran dan pengguna termasuk memverifikasi `external_id` nilainya, untuk memastikannya mutakhir. ID eksternal memetakan ke pengenalan grup atau pengguna di penyedia identitas. Misalnya, ID eksternal peran memetakan ke ID grup Azure AD yang sesuai. Demikian pula, ID eksternal setiap pengguna memetakan ke ID mereka di penyedia identitas.

```
create role "aad:rsgroup";
```

3. Berikan izin yang relevan untuk peran sesuai kebutuhan Anda. Sebagai contoh:

```
GRANT SELECT on all tables in schema public to role "aad:rsgroup";
```

4. Anda juga dapat memberikan izin kepada pengguna tertentu.

```
GRANT SELECT on table foo to aad:alice@example.com
```

Perhatikan bahwa keanggotaan peran pengguna eksternal federasi hanya tersedia di sesi pengguna tersebut. Ini memiliki implikasi untuk membuat objek database. Ketika pengguna eksternal federasi membuat tampilan atau prosedur tersimpan, misalnya, pengguna yang sama tidak dapat mendelegasikan izin objek tersebut ke pengguna dan peran lain.

Penjelasan ruang nama

Namespace memetakan pengguna atau peran ke penyedia identitas tertentu. Misalnya, awalan untuk pengguna yang dibuat di AWS IAM adalah `iam`: Awalan ini mencegah tabrakan nama pengguna dan memungkinkan dukungan untuk beberapa penyimpanan identitas. Jika pengguna `alice@example.com` dari sumber identitas yang terdaftar dengan namespace `aad` masuk, pengguna `aad:alice@example.com` dibuat di Redshift jika belum ada. Perhatikan bahwa namespace pengguna dan peran memiliki fungsi yang berbeda dari namespace kluster Amazon Redshift, yang merupakan pengenalan unik yang terkait dengan cluster.

Cara kerja login dengan federasi penyedia identitas asli (iDP)

Untuk menyelesaikan penyiapan awal antara penyedia identitas dan Amazon Redshift, Anda melakukan beberapa langkah: Pertama, Anda mendaftarkan Amazon Redshift sebagai aplikasi pihak ketiga dengan penyedia identitas Anda, meminta izin API yang diperlukan. Kemudian Anda membuat pengguna dan grup di penyedia identitas. Terakhir, Anda mendaftarkan penyedia identitas dengan Amazon Redshift, menggunakan pernyataan SQL, yang menetapkan parameter otentikasi yang unik untuk penyedia identitas. Sebagai bagian dari mendaftarkan penyedia identitas dengan Redshift,

Anda menetapkan namespace untuk memastikan pengguna dan peran dikelompokkan dengan benar.

Dengan penyedia identitas yang terdaftar di Amazon Redshift, komunikasi diatur antara Redshift dan penyedia identitas. Klien kemudian dapat meneruskan token dan mengautentikasi ke Redshift sebagai entitas penyedia identitas. Amazon Redshift menggunakan informasi keanggotaan grup IDP untuk memetakan ke peran Redshift. Jika pengguna sebelumnya tidak ada di Redshift, pengguna dibuat. Peran dibuat yang memetakan ke grup penyedia identitas, jika tidak ada. Administrator Amazon Redshift memberikan izin pada peran, dan pengguna dapat menjalankan kueri dan melakukan tugas database lainnya.

Langkah-langkah berikut menguraikan cara kerja federasi penyedia identitas asli, saat pengguna masuk:

1. Ketika pengguna log in menggunakan opsi iDP asli, dari klien, token penyedia identitas dikirim dari klien ke driver.
2. Pengguna diautentikasi. Jika pengguna belum ada di Amazon Redshift, pengguna baru akan dibuat. Redshift memetakan grup penyedia identitas pengguna ke peran Redshift.
3. Izin ditetapkan, berdasarkan peran Redshift pengguna. Ini diberikan kepada pengguna dan peran oleh administrator.
4. Pengguna dapat menanyakan Redshift.

Menggunakan alat klien desktop untuk terhubung ke Amazon Redshift

Untuk petunjuk tentang cara menggunakan federasi penyedia identitas asli untuk terhubung ke Amazon Redshift dengan Power BI, lihat posting blog [Mengintegrasikan federasi iDP asli Amazon Redshift dengan Microsoft Azure Active Directory](#) (AD) dan Power BI. Ini menjelaskan step-by-step implementasi penyiapan iDP asli Amazon Redshift dengan Azure AD. Ini merinci langkah-langkah untuk mengatur koneksi klien untuk Power BI Desktop atau layanan Power BI. Langkah-langkahnya meliputi pendaftaran aplikasi, mengonfigurasi izin, dan mengonfigurasi kredensial.

Untuk mempelajari cara mengintegrasikan federasi iDP asli Amazon Redshift dengan Azure AD, menggunakan Power BI Desktop dan JDBC Client-SQL Workbench/J, tonton video berikut:

Untuk petunjuk tentang cara menggunakan federasi penyedia identitas asli untuk terhubung ke Amazon Redshift dengan klien SQL, khususnya DBeaver atau SQL Workbench/J, lihat posting blog [Mengintegrasikan federasi iDP asli Amazon Redshift](#) dengan Microsoft Azure AD menggunakan klien SQL.

Hubungkan Redshift dengan IAM Identity Center untuk memberi pengguna pengalaman masuk tunggal

Anda dapat mengelola akses pengguna dan grup ke gudang data Amazon Redshift melalui propagasi identitas terpercaya. Ini bekerja melalui koneksi antara Redshift dan AWS IAM Identity Center, yang memberi pengguna Anda pengalaman masuk tunggal. Ini membuatnya sehingga Anda dapat membawa pengguna dan grup dari direktori Anda dan menetapkan izin langsung kepada mereka. Selanjutnya, koneksi ini mendukung pengikatan alat dan layanan tambahan. Untuk mengilustrasikan satu end-to-end kasus, Anda dapat menggunakan Amazon QuickSight dasbor atau editor kueri Amazon Redshift v2 untuk mengakses Redshift. Akses dalam hal ini didasarkan pada grup Pusat Identitas IAM. Redshift dapat menentukan siapa pengguna dan keanggotaan grup mereka. IAM Identity Center juga memungkinkan untuk menghubungkan dan mengelola identitas melalui penyedia identitas pihak ketiga (iDP) seperti Okta atau PingOne

Setelah administrator Anda mengatur koneksi antara Redshift dan IAM Identity Center, mereka dapat mengonfigurasi akses berbutir halus berdasarkan grup penyedia identitas untuk mengotorisasi akses pengguna ke data.

Manfaat integrasi Redshift dengan AWS IAM Identity Center

Menggunakan IAM Identity Center dengan Redshift dapat menguntungkan organisasi Anda dengan cara berikut:

- Penulis dasbor Amazon QuickSight dapat terhubung ke sumber data Redshift tanpa harus memasukkan kembali kata sandi atau mengharuskan administrator untuk mengatur peran IAM dengan izin yang kompleks.
- IAM Identity Center menyediakan lokasi pusat bagi pengguna tenaga kerja Anda. AWS Anda dapat membuat pengguna dan grup secara langsung di Pusat Identitas IAM atau menghubungkan pengguna dan grup yang ada yang Anda kelola di penyedia identitas berbasis standar seperti Okta, PingOne atau Microsoft Entra ID (Azure AD). IAM Identity Center mengarahkan otentikasi ke sumber kebenaran yang Anda pilih untuk pengguna dan grup, dan memelihara direktori pengguna dan grup untuk diakses oleh Redshift. Untuk informasi selengkapnya, lihat [Mengelola sumber identitas Anda](#) dan [Penyedia identitas yang didukung](#) di Panduan Pengguna Pusat AWS Identitas IAM.
- Anda dapat berbagi satu instans Pusat Identitas IAM dengan beberapa cluster dan grup kerja Redshift dengan kemampuan penemuan otomatis dan koneksi yang sederhana. Ini membuatnya cepat untuk menambahkan cluster tanpa upaya ekstra untuk mengonfigurasi koneksi Pusat

Identitas IAM untuk masing-masing, dan memastikan bahwa semua cluster dan kelompok kerja memiliki pandangan pengguna, atribut, dan grup yang konsisten. Perhatikan bahwa instans Pusat Identitas IAM organisasi Anda harus berada di wilayah yang sama dengan rangkaian data Redshift yang Anda sambungkan.

- Karena identitas pengguna diketahui dan dicatat bersama dengan akses data, lebih mudah bagi Anda untuk memenuhi peraturan kepatuhan melalui audit akses pengguna. AWS CloudTrail

Menyiapkan integrasi Pusat Identitas IAM dengan Amazon Redshift

Administrator kluster Amazon Redshift atau administrator Amazon Redshift Tanpa Server Anda harus melakukan beberapa langkah untuk mengonfigurasi Redshift sebagai aplikasi yang diaktifkan Pusat Identitas IAM. Ini membuatnya sehingga Redshift dapat menemukan dan terhubung ke IAM Identity Center secara otomatis untuk menerima layanan login dan direktori pengguna. Setelah ini, ketika administrator Redshift Anda membuat cluster atau workgroup, mereka dapat mengaktifkan gudang data baru untuk menggunakan IAM Identity Center untuk mengelola akses database.

Tujuan mengaktifkan Redshift sebagai aplikasi yang dikelola Pusat Identitas IAM adalah agar Anda dapat mengontrol izin pengguna dan grup dari dalam Pusat Identitas IAM, atau dari penyedia identitas pihak ketiga yang terintegrasi dengannya. Saat pengguna database Anda masuk ke database Redshift, misalnya analis atau ilmuwan data, database akan memeriksa grup mereka di Pusat Identitas IAM dan ini cocok dengan nama peran di Redshift. Dengan cara ini, grup yang mendefinisikan nama untuk peran database Redshift dapat mengakses satu set tabel untuk analisis penjualan, misalnya. Bagian berikut menunjukkan cara mengatur ini.

Prasyarat

Ini adalah prasyarat untuk mengintegrasikan IAM Identity Center dengan Amazon Redshift:

- Konfigurasi akun — Anda harus mengonfigurasi Pusat Identitas IAM di akun manajemen AWS organisasi jika Anda berencana untuk memiliki kasus penggunaan lintas akun, atau jika Anda menggunakan kluster Redshift di akun yang berbeda dengan instans Pusat Identitas IAM yang sama. Ini termasuk mengonfigurasi sumber identitas Anda. Untuk informasi selengkapnya, lihat [Memulai](#), [identitas tenaga kerja](#), dan [penyedia identitas yang didukung di Panduan Pengguna](#) Pusat AWS Identitas IAM. Anda harus memastikan bahwa Anda telah membuat pengguna atau grup di Pusat Identitas IAM, atau menyinkronkan pengguna dan grup dari sumber identitas Anda sebelum Anda dapat menetakannya ke data di Redshift.

Note

Anda memiliki opsi untuk menggunakan instance akun IAM Identity Center, asalkan Redshift dan IAM Identity Center berada di akun yang sama. Anda dapat membuat instance ini menggunakan widget saat membuat dan mengonfigurasi cluster atau workgroup Redshift.

- Mengonfigurasi penerbit token terpercaya — Dalam beberapa kasus, Anda mungkin perlu menggunakan penerbit token terpercaya, yang merupakan entitas yang dapat mengeluarkan dan memverifikasi token kepercayaan. Sebelum Anda dapat melakukannya, langkah-langkah awal diperlukan sebelum administrator Redshift yang mengonfigurasi integrasi IAM Identity Center dapat memilih penerbit token terpercaya dan menambahkan atribut yang diperlukan untuk menyelesaikan konfigurasi. Ini dapat mencakup mengonfigurasi penyedia identitas eksternal untuk berfungsi sebagai penerbit token terpercaya dan menambahkan atributnya di konsol Pusat Identitas IAM. Untuk menyelesaikan langkah-langkah ini, lihat [Menggunakan aplikasi dengan penerbit token terpercaya](#).

Note

Menyiapkan penerbit token terpercaya tidak diperlukan untuk semua koneksi eksternal. Menyambungkan ke database Redshift Anda dengan editor kueri Amazon Redshift v2 tidak memerlukan konfigurasi penerbit token terpercaya. Tetapi itu dapat berlaku untuk aplikasi pihak ketiga seperti dasbor atau aplikasi khusus yang mengautentikasi dengan penyedia identitas Anda.

- Mengkonfigurasi peran atau peran IAM — Bagian yang mengikuti menyebutkan izin yang harus dikonfigurasi. Anda harus menambahkan izin per praktik terbaik IAM. Izin khusus dirinci dalam prosedur berikut.

Untuk informasi selengkapnya, lihat [Memulai dengan Pusat Identitas IAM](#).

Mengkonfigurasi penyedia identitas Anda untuk bekerja dengan IAM Identity Center

Langkah pertama dalam mengendalikan manajemen identitas pengguna dan grup adalah terhubung ke IAM Identity Center dan mengkonfigurasi penyedia identitas Anda. Anda dapat menggunakan IAM Identity Center sendiri sebagai penyedia identitas Anda, atau Anda dapat menghubungkan toko identitas pihak ketiga, seperti Okta, misalnya. Untuk informasi selengkapnya tentang menyiapkan

sambungan ke dan mengonfigurasi penyedia identitas Anda, lihat [Connect ke penyedia identitas eksternal di panduan](#) pengguna IAM Identity Center. Pastikan pada akhir proses ini bahwa Anda memiliki koleksi kecil pengguna dan grup yang ditambahkan ke IAM Identity Center, untuk tujuan pengujian.

Izin Administratif

Izin diperlukan untuk manajemen siklus hidup aplikasi RedShift/IAM Identity Center

Anda harus membuat identitas IAM, yang digunakan administrator Redshift untuk mengonfigurasi Redshift untuk digunakan dengan IAM Identity Center. Paling umum, Anda akan membuat peran IAM dengan izin dan menetakannya ke identitas lain sesuai kebutuhan. Itu harus memiliki izin yang terdaftar untuk melakukan tindakan berikut.

Membuat aplikasi RedShift/IAM Identity Center

- `sso:PutApplicationAssignmentConfiguration`- Untuk keamanan.
- `sso:CreateApplication`— Digunakan untuk membuat aplikasi IAM Identity Center.
- `sso:PutApplicationAuthenticationMethod`— Memberikan akses otentikasi Redshift.
- `sso:PutApplicationGrant`— Digunakan untuk mengubah informasi penerbit token tepercaya.
- `sso:PutApplicationAccessScope`— Untuk pengaturan aplikasi Redshift IAM Identity Center. Ini termasuk untuk AWS Lake Formation dan untuk Hibah [Akses Amazon S3](#).
- `redshift:CreateRedshiftIdcApplication`— Digunakan untuk membuat aplikasi Redshift IDC.

Menjelaskan aplikasi RedShift/IAM Identity Center

- `sso:GetApplicationGrant`— Digunakan untuk mencantumkan informasi penerbit token tepercaya.
- `sso:ListApplicationAccessScopes`— Untuk pengaturan aplikasi Redshift IAM Identity Center untuk mencantumkan integrasi hilir, seperti for AWS Lake Formation dan S3 Access Grants.
- `redshift:DescribeRedshiftIdcApplications`— Digunakan untuk menggambarkan aplikasi IAM Identity Center yang ada.

Mengubah aplikasi RedShift/IAM Identity Center

- `redshift:ModifyRedshiftIdcApplication`— Digunakan untuk mengubah aplikasi Redshift yang ada.
- `sso:UpdateApplication`— Digunakan untuk memperbarui aplikasi Pusat Identitas IAM.
- `sso:GetApplicationGrant`— Mendapatkan informasi penerbit token kepercayaan.
- `sso:ListApplicationAccessScopes`— Untuk pengaturan aplikasi Redshift IAM Identity Center.
- `sso>DeleteApplicationGrant`— Menghapus informasi penerbit token kepercayaan.
- `sso:PutApplicationGrant`— Digunakan untuk mengubah informasi penerbit token terpercaya.
- `sso:PutApplicationAccessScope`— Untuk pengaturan aplikasi Redshift IAM Identity Center. Ini termasuk untuk AWS Lake Formation dan untuk Hibah [Akses Amazon S3](#).
- `sso>DeleteApplicationAccessScope`— Untuk menghapus pengaturan aplikasi Redshift IAM Identity Center. Ini termasuk untuk AWS Lake Formation dan untuk Hibah [Akses Amazon S3](#).

Menghapus aplikasi RedShift/IAM Identity Center

- `sso>DeleteApplication`— Digunakan untuk menghapus aplikasi IAM Identity Center.
- `redshift>DeleteRedshiftIdcApplication`— Memberikan kemampuan untuk menghapus aplikasi Redshift IDC yang ada.

Izin diperlukan untuk manajemen siklus hidup aplikasi RedShift/editor kueri v2

Anda harus membuat identitas IAM, yang digunakan administrator Redshift untuk mengonfigurasi Redshift untuk digunakan dengan IAM Identity Center. Paling umum, Anda akan membuat peran IAM dengan izin dan menentukannya ke identitas lain sesuai kebutuhan. Itu harus memiliki izin yang terdaftar untuk melakukan tindakan berikut.

Membuat aplikasi query editor v2

- `redshift>CreateQev2IdcApplication`— Digunakan untuk membuat aplikasi QEV2.
- `sso:CreateApplication`— Memberikan kemampuan untuk membuat aplikasi IAM Identity Center.
- `sso:PutApplicationAuthenticationMethod`— Memberikan akses otentikasi Redshift.
- `sso:PutApplicationGrant`— Digunakan untuk mengubah informasi penerbit token terpercaya.
- `sso:PutApplicationAccessScope`— Untuk pengaturan aplikasi Redshift IAM Identity Center. Ini termasuk editor kueri v2.

- `sso:PutApplicationAssignmentConfiguration`- Untuk keamanan.

Jelaskan aplikasi editor kueri v2

- `redshift:DescribeQev2IdcApplications`— Digunakan untuk menggambarkan aplikasi IAM Identity Center QEV2.

Ubah aplikasi editor kueri v2

- `redshift:ModifyQev2IdcApplication`— Digunakan untuk mengubah aplikasi IAM Identity Center QEV2.
- `sso:UpdateApplication`— Digunakan untuk mengubah aplikasi IAM Identity Center QEV2.

Hapus aplikasi editor kueri v2

- `redshift>DeleteQev2IdcApplication`— Digunakan untuk menghapus aplikasi QEV2.
- `sso>DeleteApplication`— Digunakan untuk menghapus aplikasi QEV2.

Note

Di Amazon Redshift SDK, API berikut tidak tersedia:

- `CreateQev2 IdcApplication`
- `DescribeQev2 IdcApplications`
- `ModifyQev2 IdcApplication`
- `DeleteQev2 IdcApplication`

Tindakan ini khusus untuk melakukan integrasi IAM Identity Center dengan Redshift QEV2 di konsol. AWS Untuk informasi selengkapnya, lihat [Tindakan yang ditentukan oleh Amazon Redshift](#).

Izin yang diperlukan bagi administrator database untuk menghubungkan sumber daya baru di konsol

Izin ini diperlukan untuk menghubungkan kluster baru yang disediakan atau grup kerja Amazon Redshift Tanpa Server selama proses pembuatan. Jika Anda memiliki izin ini, pilihan muncul di konsol untuk memilih untuk terhubung ke aplikasi yang dikelola Pusat Identitas IAM untuk Redshift.

- `redshift:DescribeRedshiftIdcApplications`
- `sso:ListApplicationAccessScopes`
- `sso:GetApplicationAccessScope`
- `sso:GetApplicationGrant`


Sebagai praktik terbaik, kami merekomendasikan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Manajemen identitas dan akses di Amazon Redshift](#).

Menyiapkan Redshift sebagai aplikasi AWS terkelola dengan IAM Identity Center

Sebelum Pusat Identitas IAM dapat mengelola identitas untuk kluster yang disediakan Amazon Redshift atau grup kerja Tanpa Server Amazon Redshift, administrator Redshift harus menyelesaikan langkah-langkah untuk menjadikan Redshift sebagai aplikasi yang dikelola Pusat Identitas IAM:

1. Pilih integrasi Pusat Identitas IAM di menu konsol Amazon Redshift atau Amazon Redshift Tanpa Server, lalu pilih Connect to IAM Identity Center. Dari sana Anda melangkah melalui serangkaian pilihan untuk mengisi properti untuk integrasi IAM Identity Center.
2. Pilih nama tampilan dan nama unik untuk aplikasi terkelola IDC Redshift.
3. Tentukan namespace untuk organisasi Anda. Ini biasanya merupakan versi singkat dari nama organisasi Anda. Ini ditambahkan sebagai awalan untuk pengguna dan peran yang dikelola IDC dalam database Redshift.
4. Pilih peran IAM yang akan digunakan. Peran IAM ini harus terpisah dari yang lain yang digunakan untuk Redshift, dan kami menyarankan agar tidak digunakan untuk tujuan lain. Izin kebijakan khusus yang diperlukan adalah sebagai berikut:
 - `sso:DescribeApplication`— Diperlukan untuk membuat entri penyedia identitas (iDP) di katalog.
 - `sso:DescribeInstance`— Digunakan untuk membuat peran atau pengguna federasi IDP secara manual.

5. Konfigurasi koneksi klien dan penerbit token tepercaya. Mengkonfigurasi penerbit token tepercaya memfasilitasi propagasi identitas tepercaya dengan mengatur hubungan dengan penyedia identitas eksternal. Propagasi identitas memungkinkan pengguna, misalnya, untuk masuk ke satu aplikasi dan mengakses data tertentu di aplikasi lain. Hal ini memungkinkan pengguna untuk mengumpulkan data dari lokasi yang berbeda dengan lebih mulus. Pada langkah ini, di konsol, Anda menetapkan atribut untuk setiap penerbit token tepercaya. Atribut termasuk nama dan klaim audiens (atau klaim aud), yang mungkin harus Anda dapatkan dari atribut konfigurasi alat atau layanan. Anda mungkin juga perlu memberikan nama aplikasi dari JSON Web Token (JWT) alat pihak ketiga.

 Note

Yang `aud claim` diperlukan dari setiap alat atau layanan pihak ketiga dapat bervariasi, berdasarkan jenis token, yang dapat berupa token akses yang dikeluarkan oleh penyedia identitas, atau jenis lain, seperti token ID. Setiap vendor bisa berbeda. Saat Anda menerapkan propagasi identitas tepercaya dan berintegrasi dengan Redshift, Anda harus memberikan nilai `aud` yang benar untuk jenis token yang dikirimkan oleh alat pihak ketiga. AWS Periksa rekomendasi dari vendor alat atau layanan Anda.

Untuk informasi terperinci mengenai propagasi identitas tepercaya, lihat [Cara kerja propagasi identitas tepercaya](#). Juga, lihat dokumentasi beta untuk IAM Identity Center yang menyertai dokumentasi ini.

Setelah administrator Redshift menyelesaikan langkah-langkah dan menyimpan konfigurasi, properti IAM Identity Center muncul di konsol Redshift. Anda juga dapat menanyakan tampilan sistem [SVV_IDENTITY_PROVIDERS](#) untuk memverifikasi properti aplikasi. Ini termasuk nama aplikasi dan namespace. Anda menggunakan namespace sebagai awalan untuk objek database Redshift yang terkait dengan aplikasi. Menyelesaikan tugas-tugas ini membuat Redshift menjadi aplikasi yang diaktifkan Pusat Identitas IAM. Properti di konsol termasuk status integrasi. Dikatakan Diaktifkan ketika integrasi selesai. Setelah proses ini, integrasi IAM Identity Center dapat diaktifkan pada setiap cluster baru.

Setelah konfigurasi, Anda dapat menyertakan pengguna dan grup dari Pusat Identitas IAM di Redshift dengan memilih tab Pengguna atau Grup dan memilih Tetapkan.

Mengaktifkan integrasi IAM Identity Center untuk cluster Amazon Redshift baru atau grup kerja Amazon Redshift Serverless

Administrator database Anda mengonfigurasi sumber daya Redshift baru agar berfungsi sejajar dengan IAM Identity Center untuk mempermudah proses masuk dan akses data. Ini dilakukan sebagai bagian dari langkah-langkah untuk membuat klaster yang disediakan atau grup kerja Tanpa Server. Siapa pun yang memiliki izin untuk membuat sumber daya Redshift dapat melakukan tugas integrasi Pusat Identitas IAM ini. Saat membuat klaster yang disediakan, Anda mulai dengan memilih Create Cluster di konsol Amazon Redshift. Langkah-langkah berikut menunjukkan cara mengaktifkan manajemen IAM Identity Center untuk database. (Itu tidak termasuk semua langkah untuk membuat cluster.)

1. Pilih Aktifkan untuk <your cluster name>di bagian untuk integrasi IAM Identity Center dalam langkah-langkah create-cluster.
2. Ada langkah dalam proses ketika Anda mengaktifkan integrasi. Anda melakukan ini dengan memilih Aktifkan integrasi IAM Identity Center di konsol.
3. Untuk cluster atau workgroup baru, buat peran database di Redshift menggunakan perintah SQL. Berikut ini adalah perintahnya:

```
CREATE ROLE <idnamespace:rolename>;
```

Namespace dan nama peran adalah sebagai berikut:

- Awalan namespace IAM Identity Center — Ini adalah namespace yang Anda tentukan saat Anda mengatur koneksi antara IAM Identity Center dan Redshift.
- Nama peran - Peran database Redshift ini harus cocok dengan nama grup di Pusat Identitas IAM.

Redshift terhubung dengan IAM Identity Center dan mengambil informasi yang diperlukan untuk membuat dan memetakan peran database ke grup IAM Identity Center.

Perhatikan bahwa ketika gudang data baru dibuat, peran IAM yang ditentukan untuk integrasi IDC secara otomatis dilampirkan ke klaster yang disediakan atau grup kerja Amazon Redshift Serverless. Setelah Anda selesai memasukkan metadata cluster yang diperlukan dan membuat sumber daya, Anda dapat memeriksa status integrasi Pusat Identitas IAM di properti. Jika nama grup Anda di IAM

Identity Center memiliki spasi, Anda harus menggunakan tanda kutip di SQL saat Anda membuat peran yang cocok.

Setelah Anda mengaktifkan database Redshift dan membuat peran, Anda siap untuk terhubung ke database dengan Amazon Redshift query editor v2 atau. Amazon QuickSight Rinciannya dijelaskan lebih lanjut di bagian berikutnya.

Menyiapkan default **RedshiftIdcApplication** menggunakan API

Pengaturan dilakukan oleh administrator identitas Anda. Menggunakan API, Anda membuat dan mengisi `RedshiftIdcApplication`, yang mewakili aplikasi Redshift dalam IAM Identity Center.

1. Untuk memulai, Anda dapat membuat pengguna dan menambahkannya ke grup di Pusat Identitas IAM. Anda melakukan ini di AWS konsol untuk IAM Identity Center (IDC).
2. Panggilan `create-redshift-idc-application` untuk membuat aplikasi IDC dan membuatnya kompatibel dengan penggunaan Redshift. Anda membuat aplikasi dengan mengisi nilai yang diperlukan. Nama tampilan adalah nama yang akan ditampilkan di dasbor IDC. Peran IAM ARN adalah ARN yang memiliki izin untuk IAM Identity Center dan juga dapat diasumsikan oleh Redshift.

```
aws redshift create-redshift-idc-application
--idc-instance-arn 'arn:aws:sso:::instance/ssoins-1234a01a1b12345d'
--identity-namespace 'MYCO'
--idc-display-name 'TEST-NEW-APPLICATION'
--iam-role-arn 'arn:aws:redshift:us-east-1:012345678901:role/TestRedshiftRole'
--redshift-idc-application-name 'myredshiftidcapplication'
```

Contoh berikut menunjukkan `RedshiftIdcApplication` respons sampel yang dikembalikan dari panggilan ke `create-redshift-idc-application`.

```
"RedshiftIdcApplication": {
  "IdcInstanceArn": "arn:aws:sso:::instance/ssoins-1234a01a1b12345d",
  "RedshiftIdcApplicationName": "test-application-1",
  "RedshiftIdcApplicationArn": "arn:aws:redshift:us-east-1:012345678901:redshiftidcapplication:12aaa111-3ab2-3ab1-8e90-b2d72aea588b",
  "IdentityNamespace": "MYCO",
  "IdcDisplayName": "Redshift-Idc-Application",
  "IamRoleArn": "arn:aws:redshift:us-east-1:012345678901:role/TestRedshiftRole",
  "IdcManagedApplicationArn": "arn:aws:sso:::012345678901:application/ssoins-1234a01a1b12345d/apl-12345678910",
```

```

      "IdcOnboardStatus": "arn:aws:redshift:us-
east-1:123461817589:redshiftidcapplication",
      "RedshiftIdcApplicationArn": "Completed",
      "AuthorizedTokenIssuerList": [
        "TrustedTokenIssuerArn": ...,
        "AuthorizedAudiencesList": [...]...
      ]}

```

3. Anda dapat menggunakan `create-application-assignment` untuk menetapkan grup tertentu atau pengguna individu ke aplikasi terkelola di Pusat Identitas IAM. Dengan melakukan ini, Anda dapat menentukan grup untuk dikelola melalui IAM Identity Center. Jika administrator database membuat peran database di Redshift, nama grup di Pusat Identitas IAM memetakan ke nama peran di Redshift. Peran mengontrol izin dalam database. Untuk informasi selengkapnya, lihat [Menetapkan akses pengguna ke aplikasi di konsol Pusat Identitas IAM](#).
4. Setelah Anda mengaktifkan aplikasi, panggil `create-cluster` dan sertakan ARN aplikasi terkelola Redshift dari IAM Identity Center. Melakukan hal ini mengaitkan cluster dengan aplikasi terkelola di IAM Identity Center.

Mengaitkan aplikasi IAM Identity Center dengan cluster atau workgroup yang ada

Jika Anda memiliki cluster atau workgroup yang ingin Anda aktifkan untuk integrasi IAM Identity Center, Anda dapat melakukannya dengan menjalankan perintah SQL. Anda menjalankan perintah berikut untuk mengaktifkan integrasi. Diperlukan administrator database menjalankan kueri dan koneksi antara Redshift dan IAM Identity Center telah diatur. Ketika Anda mengatur `ENABLE`, ini memungkinkan IAM Identity Center untuk menyediakan manajemen identitas untuk cluster atau workgroup.

```

ALTER IDENTITY PROVIDER
<idp_name> | NAMESPACE <namespace> | IAM_ROLE default | 'arn:aws:iam::<AWS account-
id-1>:role/<role-name>' | [DISABLE | ENABLE]

```

Anda dapat menjatuhkan penyedia identitas yang ada. Contoh berikut menunjukkan bagaimana `CASCADE` menghapus pengguna dan peran yang dilampirkan ke penyedia identitas.

```

DROP IDENTITY PROVIDER
<provider_name> [ CASCADE ]

```

Menyiapkan izin pengguna

Administrator mengonfigurasi izin ke berbagai sumber daya, berdasarkan atribut identitas pengguna dan keanggotaan grup, dalam penyedia identitas mereka atau di dalam Pusat Identitas IAM secara langsung. Misalnya, administrator penyedia identitas dapat menambahkan insinyur basis data ke grup yang sesuai dengan peran mereka. Nama grup ini memetakan ke nama peran database Redshift. Peran menyediakan atau membatasi akses ke tabel atau tampilan tertentu di Redshift.

Persona administrator untuk menghubungkan aplikasi

Berikut ini adalah persona yang merupakan kunci untuk menghubungkan aplikasi analitik ke aplikasi terkelola IAM Identity Center untuk Redshift:

- Administrator aplikasi — Membuat aplikasi dan mengonfigurasi layanan mana yang akan memungkinkan pertukaran token identitas. Administrator ini juga menentukan pengguna atau grup mana yang memiliki akses ke aplikasi.
- Administrator data — Mengkonfigurasi akses halus ke data. Pengguna dan grup di Pusat Identitas IAM dapat memetakan ke izin tertentu.

Menghubungkan ke Amazon Redshift dengan IAM Identity Center melalui Amazon QuickSight

Berikut ini menunjukkan cara menggunakan Amazon QuickSight untuk mengautentikasi dengan Redshift saat terhubung dan akses dikelola melalui Pusat Identitas IAM: [Mengotorisasi koneksi dari Amazon QuickSight ke Amazon Redshift cluster](#). Langkah-langkah ini berlaku untuk Amazon Redshift Serverless juga.

Menghubungkan ke Amazon Redshift dengan IAM Identity Center melalui editor kueri Amazon Redshift v2

Setelah menyelesaikan langkah-langkah untuk mengatur koneksi IAM Identity Center dengan Redshift, pengguna dapat mengakses database dan objek yang sesuai dalam database melalui identitas IAM Identity Center, namespace-prefixed. Untuk informasi selengkapnya tentang menghubungkan ke database Redshift dengan login editor kueri v2, lihat [Bekerja dengan editor kueri v2](#).

Memeriksa data melalui AWS Lake Formation

Menggunakan AWS Lake Formation membuatnya lebih mudah untuk mengatur dan mengamankan data lake Anda secara terpusat, dan untuk menyediakan akses data. Mengkonfigurasi propagasi identitas ke Lake Formation melalui IAM Identity Center dan Redshift membuatnya sehingga administrator dapat mengizinkan akses halus ke danau data Amazon S3, berdasarkan grup penyedia identitas organisasi (iDP). Kelompok-kelompok ini dikelola melalui IAM Identity Center. Bagian ini menunjukkan cara mengonfigurasi beberapa kasus penggunaan, kueri dari data lake dan kueri dari berbagi data, yang menunjukkan cara memanfaatkan Pusat Identitas IAM dengan Redshift untuk terhubung ke sumber daya yang diatur oleh Lake Formation.

Menggunakan Pusat Identitas IAM dan koneksi Redshift untuk menanyakan data lake

Langkah-langkah ini mencakup kasus penggunaan di mana Anda menggunakan Pusat Identitas IAM yang terhubung ke Redshift untuk menanyakan data lake yang diatur oleh Lake Formation.

Prasyarat

Prosedur ini memiliki beberapa langkah prasyarat:

1. Pusat Identitas IAM harus disiapkan untuk mendukung otentikasi dan manajemen identitas dengan Redshift. Anda dapat mengaktifkan Pusat Identitas IAM dari konsol dan memilih sumber penyedia identitas (iDP). Setelah ini, sinkronkan satu set pengguna IDP Anda dengan IAM Identity Center. Anda juga harus mengatur koneksi antara IAM Identity Center dan Redshift, mengikuti langkah-langkah yang dijelaskan sebelumnya dalam dokumen ini.
2. Buat cluster Amazon Redshift baru dan aktifkan manajemen identitas melalui IAM Identity Center dalam langkah-langkah konfigurasi.
3. Buat aplikasi Pusat Identitas IAM terkelola untuk Lake Formation dan konfigurasi. Ini mengikuti pengaturan koneksi antara IAM Identity Center dan Redshift. Langkah-langkahnya adalah sebagai berikut:
 - a. Di AWS CLI, gunakan `modify-redshift-idc-application` perintah untuk mengaktifkan integrasi layanan Lake Formation dengan aplikasi yang dikelola Pusat Identitas IAM untuk Redshift. Panggilan ini mencakup `service-integrations` parameter, yang diatur ke nilai string konfigurasi yang memungkinkan otorisasi ke Lake Formation.
 - b. Konfigurasi Lake Formation dengan menggunakan `create-lake-formation-identity-center-configuration` perintah. Ini menciptakan aplikasi Pusat Identitas IAM untuk Lake Formation, yang terlihat di portal IAM Identity Center. Administrator harus mengatur `--cli-input-json` argumen, yang nilainya adalah jalur ke file JSON yang menggunakan

format standar untuk semua panggilan AWS CLI API. Anda harus menyertakan nilai untuk hal-hal berikut:

- `CatalogId`— ID katalog Lake Formation.
- `InstanceArn`— Pusat Identitas IAM misalnya nilai ARN.

Setelah administrator menyelesaikan konfigurasi prasyarat, administrator database dapat membuat skema eksternal untuk tujuan kueri data lake.

1. Administrator membuat skema eksternal - Administrator database Redshift terhubung ke database dan membuat skema eksternal, menggunakan pernyataan SQL berikut:

```
CREATE EXTERNAL SCHEMA if not exists my_external_schema from DATA CATALOG database
'my_lf_integrated_db' catalog_id '12345678901234';
```

Perhatikan bahwa menentukan peran IAM tidak diperlukan dalam kasus ini, karena akses dikelola melalui IAM Identity Center.

2. Administrator memberikan izin — Administrator memberikan penggunaan ke grup Pusat Identitas IAM, yang memberikan izin pada sumber daya Redshift. Hal ini dilakukan dengan menjalankan pernyataan SQL seperti berikut:

```
GRANT USAGE ON SCHEMA "my_external_schema" to "MYC0:sales";
```

Selanjutnya, administrator memberikan izin Lake Formation pada objek, berdasarkan persyaratan untuk organisasi, menggunakan CLI AWS :

```
aws lakeformation grant-permissions ...
```

3. Pengguna menjalankan kueri — Pada titik ini, pengguna Pusat Identitas IAM yang merupakan bagian dari grup penjualan, untuk tujuan ilustrasi, dapat masuk melalui editor kueri v2 ke database Redshift. Kemudian mereka dapat menjalankan kueri yang mengakses tabel dalam skema eksternal, seperti contoh berikut:

```
SELECT * from my_external_schema.table1;
```


Menggunakan Pusat Identitas IAM dan koneksi Redshift untuk terhubung ke datashare

Anda dapat mengakses datashare dari gudang data Redshift yang berbeda saat akses dikelola melalui IAM Identity Center. Untuk melakukan ini, Anda menjalankan kueri untuk menyiapkan database eksternal. Sebelum menyelesaikan langkah-langkah ini, diasumsikan bahwa Anda memiliki koneksi yang diatur antara Redshift dan IAM Identity Center, dan Anda telah membuat AWS Lake Formation aplikasi, seperti yang dijelaskan dalam prosedur sebelumnya.

1. Membuat database eksternal — Administrator membuat database eksternal untuk berbagi data, mereferensikannya melalui ARN nya. Berikut ini adalah contoh yang menunjukkan cara melakukannya:

```
CREATE DATABASE "redshift_external_db" FROM ARN 'arn:aws:glue:us-east-1:123456789012:database/redshift_external_db-iad' WITH NO DATA CATALOG SCHEMA;
```

Dalam kasus penggunaan ini, di mana Anda menggunakan Pusat Identitas IAM dengan Redshift untuk manajemen identitas, peran IAM tidak disertakan.

2. Admin menyiapkan izin — Setelah membuat database, administrator memberikan penggunaan ke grup Pusat Identitas IAM. Ini memberikan izin pada sumber daya Redshift:

```
GRANT USAGE ON DATABASE "my_external_db" to "MYCO:sales";
```

Administrator juga memberikan izin Lake Formation pada objek, menggunakan CLI AWS :

```
aws lakeformation grant-permissions ...
```

3. Pengguna menjalankan kueri — Pengguna dari grup penjualan dapat melakukan kueri tabel di database, berdasarkan izin yang ditetapkan:

```
select * from redshift_external_db.public.employees;
```

Untuk informasi selengkapnya tentang pemberian izin di data lake dan pemberian izin pada pembagian data, lihat [Memberikan izin kepada pengguna dan grup](#). [Untuk informasi selengkapnya tentang pemberian penggunaan skema atau database, lihat GRANT.](#)

Mengintegrasikan aplikasi atau alat Anda dengan OAuth menggunakan penerbit token terpercaya

Anda dapat menambahkan fungsionalitas ke alat klien yang Anda buat untuk terhubung ke Redshift melalui koneksi IAM Identity Center. Jika Anda sudah mengonfigurasi integrasi Redshift ke IAM Identity Center, gunakan properti yang dirinci di bagian ini untuk menyiapkan koneksi.

Plugin otentikasi untuk menghubungkan ke Redshift menggunakan IAM Identity Center

`IdpTokenAuthPlugin` menyediakan properti koneksi dan memfasilitasi otentikasi dengan IAM Identity Center. Ini menerima token web OpenID Connect (OIDC) JSON (JWT) dari penyedia identitas web apa pun yang terhubung dengan IAM Identity Center.

Jika Anda menggunakan driver Amazon Redshift, Anda dapat menggunakan `IdpTokenAuthPlugin` autentikasi ke Redshift dengan IAM Identity Center. Plugin ini menerima OIDC JWT dari penyedia identitas web apa pun yang terhubung dengan IAM Identity Center. Tabel berikut merinci opsi koneksi yang akan digunakan untuk otentikasi yang berhasil.

Driver	Kunci opsi koneksi	Nilai	Catatan
JDBC	<code>plugin_name</code>	<code>com.amazon.redshift.plugin.IdpTokenAuthPlugin</code>	Anda harus memasukkan nama kelas plugin yang sepenuhnya memenuhi syarat saat Anda terhubung.
ODBC	<code>plugin_name</code>	<code>IdpTokenAuthPlugin</code>	
Python	<code>credential_provider</code>	<code>IdpTokenAuthPlugin</code>	Tidak ada <code>plugin_name</code> opsi yang tersedia untuk driver Python. Sebaliknya, gunakan <code>credential_provider</code> .

Plugin ini memiliki opsi koneksi tambahan ini:

- token — OpenID Connect (OIDC) JSON Web Token (JWT) yang disediakan oleh penyedia identitas web yang terhubung dengan IAM Identity Center. Aplikasi Anda harus menghasilkan token ini dengan mengautentikasi pengguna aplikasi Anda dengan penyedia identitas yang terhubung dengan IAM Identity Center.
- token_type — Jenis token yang digunakan untuk. IdpTokenAuthPlugin Anda dapat menentukan nilai untuk opsi berikut:
 - EXT_JWT — Berikan ini jika Anda menggunakan OpenID Connect (OIDC) JSON Web Token (JWT) yang disediakan oleh penyedia identitas berbasis web yang terhubung dengan IAM Identity Center.

Anda harus memasukkan nilai-nilai ini di properti koneksi alat yang Anda buat dan hubungkan. Untuk informasi selengkapnya, lihat dokumentasi opsi koneksi untuk setiap driver masing-masing:

- [Opsi untuk konfigurasi driver JDBC versi 2.1](#)
- [Mengkonfigurasi opsi driver ODBC](#)
- [Opsi konfigurasi untuk konektor Amazon Redshift Python](#)

Memecahkan masalah koneksi dari editor kueri Amazon Redshift v2

Daftar ini merinci kesalahan yang biasanya terjadi dan dapat membantu Anda terhubung ke database Redshift Anda dengan editor kueri v2, menggunakan identitas Pusat Identitas IAM.

- Kesalahan: Masalah Koneksi: Tidak ada informasi sesi pusat identitas yang tersedia. — Ketika kesalahan ini terjadi, periksa pengaturan keamanan dan privasi browser Anda. Pengaturan browser ini, terutama untuk cookie aman, seperti fitur Perlindungan Cookie Total Firefox, dapat mengakibatkan upaya koneksi yang diblokir dari editor kueri Amazon Redshift v2 ke database Redshift. Ikuti langkah-langkah remediasi yang dirinci untuk browser Anda:
 - Firefox — Saat ini, cookie pihak ketiga diblokir secara default. Klik perisai di bilah alamat browser dan alihkan sakelar untuk mematikan perlindungan pelacakan yang disempurnakan untuk editor kueri v2.
 - Mode penyamaran Chrome — Secara default, mode Penyamaran Chrome memblokir cookie pihak ketiga. Klik ikon mata di bilah alamat untuk mengizinkan cookie pihak ketiga untuk editor kueri v2. Setelah Anda mengubah pengaturan untuk mengizinkan cookie, Anda mungkin tidak melihat ikon mata di bilah alamat.

- Safari — Di Mac, buka aplikasi Safari. Pilih Pengaturan, lalu pilih Advanced. Beralih untuk mematikan: Blokir semua cookie.
- Edge — Pilih Pengaturan, lalu pilih Cookie dan izin situs. Kemudian pilih Kelola dan hapus cookie dan data situs dan matikan Blokir cookie pihak ketiga.

Jika Anda mencoba menghubungkan setelah mengubah pengaturan dan terus menerima pesan kesalahan Masalah Koneksi: Tidak ada informasi sesi pusat Identitas yang tersedia, kami sarankan Anda menyegarkan koneksi Anda dengan IAM Identity Center. Untuk melakukan ini, klik kanan instance database Redshift Anda dan pilih Refresh. Jendela baru muncul, yang dapat Anda gunakan untuk mengautentikasi.

- Kesalahan: Masalah koneksi: Sesi pusat identitas kedaluwarsa atau tidak valid. — Setelah integrasi cluster yang disediakan Redshift atau grup kerja Tanpa Server dengan IAM Identity Center, pengguna mungkin menerima kesalahan ini ketika mereka mencoba terhubung ke database Redshift dari editor kueri v2. Ini dapat mengikuti upaya koneksi yang berhasil. Dalam hal ini, kami sarankan Anda mengautentikasi ulang. Untuk melakukan ini, klik kanan instance database Redshift Anda dan pilih Refresh. Jendela baru muncul, yang dapat Anda gunakan untuk mengautentikasi.
- Kesalahan: Cakupan tidak valid. Kredensi pengguna tidak diizinkan untuk terhubung ke Redshift. — Setelah integrasi cluster yang disediakan Redshift atau grup kerja Tanpa Server dengan Pusat Identitas IAM untuk manajemen identitas, pengguna mungkin menerima kesalahan ini ketika mereka mencoba terhubung ke database Redshift dari editor kueri v2. Dalam hal ini, agar editor kueri v2 berhasil menghubungkan dan mengautentikasi pengguna melalui IAM Identity Center untuk mengakses sumber daya yang benar, administrator harus menetapkan pengguna ke aplikasi Redshift IAM Identity Center melalui konsol Redshift. Ini diselesaikan di bawah koneksi IAM Identity Center. Setelah ini, pengguna dapat membuat koneksi yang sukses setelah satu jam, yang merupakan batas caching sesi IAM Identity Center.
- Kesalahan: Database tidak dapat dicantumkan. FATAL: Kueri gagal saat cluster dijeda secara otomatis. — Saat database Amazon Redshift Tanpa Server dalam keadaan idle, tidak memproses beban kerja apa pun, database tersebut dapat tetap dijeda saat Anda terhubung dengan identitas Pusat Identitas IAM. Untuk memperbaiki ini, masuk dengan metode otentikasi lain untuk melanjutkan workgroup Tanpa Server. Kemudian sambungkan ke database dengan identitas IAM Identity Center Anda.
- Kesalahan: Terjadi kesalahan selama upaya untuk berfederasi dengan IAM Identity Center. Administrator Amazon Redshift harus menghapus dan membuat ulang aplikasi IAM Identity Center QEV2, menggunakan konsol Redshift. — Kesalahan ini biasanya terjadi ketika instance aplikasi IAM Identity Center yang terkait dengan editor kueri v2 dihapus. Untuk mengatasinya, administrator

Amazon Redshift harus menghapus dan membuat ulang aplikasi Redshift dan query editor v2 untuk IAM Identity Center. Ini dapat dilakukan pada konsol Redshift atau menggunakan perintah CLI <https://docs.aws.amazon.com/cli/latest/reference/redshift/delete-redshift-idc-application.html>.

Batasan

Keterbatasan ini berlaku:

- Menggunakan Pusat Identitas IAM dengan driver Redshift — Saat Anda menggunakan `IdpTokenAuthPlugin`, tersedia melalui driver Redshift saat ini, aplikasi klien harus menghasilkan token otentikasi. Namun, perhatikan bahwa AWS IAM Identity Center saat ini tidak mendukung pembuatan token akses untuk Redshift. Dengan demikian, menggunakan token akses Pusat Identitas IAM tidak didukung. Saat ini dimungkinkan untuk digunakan `IdpTokenAuthPlugin` untuk terhubung dengan database Amazon Redshift melalui penyedia identitas web eksternal, seperti Okta, PingOne atau Microsoft Entra ID (Azure AD), yang terintegrasi dengan IAM Identity Center. Dalam hal ini, klien bertanggung jawab untuk menghasilkan OpenID Connect (OIDC) JSON Web Token (JWT) dari penyedia identitas web dan memasoknya sebagai input ke driver. `IdpTokenAuthPlugin` Plugin dijelaskan di bagian sebelumnya. Anda juga dapat terhubung menggunakan editor kueri v2, jika Anda ingin menggunakan otorisasi dan otentikasi IAM Identity Center secara langsung.
- Tidak ada dukungan untuk VPC yang disempurnakan — VPC yang disempurnakan tidak didukung saat Anda mengonfigurasi propagasi identitas tepercaya Redshift dengan IAM Identity Center. Untuk informasi selengkapnya tentang VPC yang disempurnakan, lihat Perutean [VPC yang Ditingkatkan di Amazon Redshift](#).
- Caching Pusat Identitas IAM - Pusat Identitas IAM menyimpan informasi sesi cache. Ini dapat menyebabkan masalah akses yang tidak dapat diprediksi saat Anda mencoba terhubung ke database Redshift Anda melalui editor kueri Redshift v2. Ini karena sesi Pusat Identitas IAM terkait di editor kueri v2 tetap valid, bahkan dalam kasus di mana pengguna database keluar dari AWS konsol. Cache kedaluwarsa setelah satu jam, yang biasanya memperbaiki masalah apa pun.

Menggunakan peran terkait layanan untuk Amazon Redshift

[Amazon Redshift menggunakan peran terkait layanan AWS Identity and Access Management \(IAM\)](#).

Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Amazon Redshift.

Peran terkait layanan telah ditentukan sebelumnya oleh Amazon Redshift dan menyertakan semua

izin yang diperlukan layanan untuk memanggil AWS layanan atas nama kluster Amazon Redshift Anda.

Peran terkait layanan membuat pengaturan Amazon Redshift lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Peran tersebut ditautkan ke kasus penggunaan Amazon Redshift dan memiliki izin yang telah ditentukan sebelumnya. Hanya Amazon Redshift yang dapat mengambil peran tersebut, dan hanya peran terkait layanan yang dapat menggunakan kebijakan izin yang telah ditentukan sebelumnya. Amazon Redshift membuat peran terkait layanan di akun Anda saat pertama kali membuat kluster atau titik akhir VPC yang dikelola RedShift. Anda dapat menghapus peran terkait layanan hanya setelah menghapus semua kluster Amazon Redshift atau titik akhir VPC yang dikelola RedShift di akun Anda. Ini melindungi sumber daya Amazon Redshift karena Anda tidak dapat secara tidak sengaja menghapus izin yang diperlukan untuk mengakses sumber daya.

Amazon Redshift mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat [AWS Wilayah dan Titik Akhir](#).

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [Layanan AWS yang berfungsi dengan IAM](#) lalu cari layanan yang menampilkan Ya pada kolom Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Amazon Redshift

Amazon Redshift menggunakan peran terkait layanan bernama — Memungkinkan AWSServiceRoleForRedshiftAmazon Redshift memanggil layanan atas nama Anda. AWS Peran terkait layanan ini dilampirkan ke kebijakan terkelola berikut ini: AmazonRedshiftServiceLinkedRolePolicy. Untuk pembaruan kebijakan ini, lihat kebijakan yang [AWS dikelola \(telah ditentukan\) untuk Amazon Redshift](#).

Peran AWSServiceRoleForRedshift terkait layanan hanya percaya **redshift.amazonaws.com** untuk mengambil peran.

Kebijakan izin peran AWSServiceRoleForRedshift terkait layanan memungkinkan Amazon Redshift menyelesaikan hal berikut di semua sumber daya terkait:

- `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`

Izin untuk sumber daya jaringan

Izin berikut memungkinkan tindakan di Amazon EC2 untuk pembuatan dan pengelolaan aturan grup keamanan. Grup dan aturan keamanan ini secara khusus dikaitkan dengan tag `aws:RequestTag/Redshift` sumber daya Amazon Redshift. Ini membatasi ruang lingkup izin untuk sumber daya Amazon Redshift tertentu.

- `ec2:CreateSecurityGroup`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

- `ec2:ModifySecurityGroupRules`
- `ec2>DeleteSecurityGroup`

Tindakan untuk pencatatan audit

Tindakan yang tercantum dengan logs awalan berkaitan dengan audit logging dan fitur terkait. Secara khusus, pembuatan dan pengelolaan grup log dan aliran log.

- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogStreams`
- `logs:GetLogEvents`

JSON berikut menunjukkan tindakan dan cakupan sumber daya, ke Amazon Redshift, untuk pencatatan audit.

```
[
  {
    "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:*"
    ]
  }
]

```

Untuk informasi selengkapnya tentang peran terkait layanan dan tujuannya AWS, lihat [Menggunakan peran terkait layanan](#). Untuk informasi selengkapnya tentang tindakan tertentu dan sumber daya IAM lainnya untuk Amazon Redshift, [lihat Tindakan, sumber daya, dan kunci kondisi untuk Amazon Redshift](#).

Tindakan untuk mengelola kredensi admin dengan AWS Secrets Manager

Tindakan yang tercantum dengan `secretsmanager` awalan berkaitan dengan penggunaan Amazon Redshift untuk mengelola kredensial admin Anda. Tindakan ini memungkinkan Amazon Redshift digunakan AWS Secrets Manager untuk membuat dan mengelola rahasia kredensi admin Anda.

JSON berikut menunjukkan tindakan dan cakupan sumber daya, ke Amazon Redshift, untuk mengelola kredensi admin dengan AWS Secrets Manager

```

[
  {
    "Effect": "Allow",
    "Action": [
      "secretsmanager:DescribeSecret",
      "secretsmanager>DeleteSecret",
      "secretsmanager:PutSecretValue",
      "secretsmanager:UpdateSecret",
      "secretsmanager:UpdateSecretVersionStage",
      "secretsmanager:RotateSecret"
    ],
    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:redshift!*"
    ],
    "Condition": {
      "StringEquals": {
        "secretsmanager:ResourceTag/aws:secretsmanager:owningService":
"redshift"
      }
    }
  },
  {

```

```

    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetRandomPassword"
    ],
    "Resource": "*"
}
]

```

Untuk mengizinkan entitas IAM membuat peran terkait AWSServiceRoleForRedshift layanan

```

{
  "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"}}
}

```

Untuk mengizinkan entitas IAM menghapus peran terkait AWSServiceRoleForRedshift layanan

Tambahkan pernyataan kebijakan berikut ini ke izin untuk entitas IAM:

```

{
  "Effect": "Allow",
  "Action": [
    "iam>DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource": "arn:aws:iam::<AWS-account-ID>:role/aws-service-role/redshift.amazonaws.com/AWSServiceRoleForRedshift",
  "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}

```

Atau, Anda dapat menggunakan kebijakan AWS terkelola untuk [menyediakan akses penuh](#) ke Amazon Redshift.

Membuat peran terkait layanan untuk Amazon Redshift

Anda tidak perlu membuat peran AWSServiceRoleForRedshift terkait layanan secara manual. Amazon Redshift menciptakan peran terkait layanan untuk Anda. Jika peran

AWSServiceRoleForRedshift terkait layanan telah dihapus dari akun Anda, Amazon Redshift akan membuat peran tersebut saat Anda meluncurkan kluster Amazon Redshift baru.

Important

Jika Anda menggunakan layanan Amazon Redshift sebelum 18 September 2017, ketika mulai mendukung peran terkait layanan, maka Amazon Redshift membuat peran di akun Anda. AWSServiceRoleForRedshift Untuk mempelajari lebih lanjut, lihat [Peran baru muncul di akun IAM saya](#).

Mengedit peran terkait layanan untuk Amazon Redshift

Amazon Redshift tidak memungkinkan Anda mengedit peran terkait AWSServiceRoleForRedshift layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit deskripsi peran menggunakan konsol IAM, AWS Command Line Interface (AWS CLI), atau IAM API. Untuk informasi selengkapnya, lihat [Memodifikasi peran](#) dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Amazon Redshift

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif.

Sebelum Anda dapat menghapus peran terkait layanan untuk akun, Anda harus mematikan dan menghapus kluster apa pun di akun tersebut. Untuk informasi selengkapnya, lihat [Mematikan dan menghapus cluster](#).

Anda dapat menggunakan konsol IAM, API IAM AWS CLI, atau IAM untuk menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat [Menghapus peran tertaut layanan](#) dalam Panduan Pengguna IAM.

Menggunakan otentikasi IAM untuk menghasilkan kredensi pengguna basis data

Anda dapat membuat kredensial database sementara berdasarkan izin yang diberikan melalui kebijakan izin AWS Identity and Access Management (IAM) untuk mengelola akses yang dimiliki pengguna ke database Amazon Redshift Anda.

Umumnya, pengguna database Amazon Redshift masuk ke database dengan memberikan nama pengguna dan kata sandi database. Namun, Anda tidak perlu mempertahankan nama pengguna dan kata sandi di database Amazon Redshift Anda. Sebagai alternatif, Anda dapat mengonfigurasi sistem Anda untuk mengizinkan pengguna membuat kredensial pengguna dan masuk ke database berdasarkan kredensial IAM mereka.

Untuk informasi selengkapnya, lihat [Penyedia Identitas dan Federasi](#) di Panduan Pengguna IAM.

Topik

- [Gambaran Umum](#)
- [Membuat kredensial IAM sementara](#)
- [Opsi untuk memberikan kredensial IAM](#)

Gambaran Umum

Amazon Redshift menyediakan operasi [GetClusterCredentials](#) API untuk menghasilkan kredensial pengguna database sementara. Anda dapat mengonfigurasi klien SQL Anda dengan driver Amazon Redshift JDBC atau ODBC yang mengelola proses pemanggilan operasi. `GetClusterCredentials` Mereka melakukannya dengan mengambil kredensial pengguna database, dan membuat koneksi antara klien SQL Anda dan database Amazon Redshift Anda. Anda juga dapat menggunakan aplikasi database Anda untuk memanggil `GetClusterCredentials` operasi secara terprogram, mengambil kredensial pengguna database, dan terhubung ke database.

Jika Anda sudah mengelola identitas pengguna di luar AWS, Anda dapat menggunakan penyedia identitas (IDP) yang sesuai dengan Security Assertion Markup Language (SAML) 2.0 untuk mengelola akses ke sumber daya Amazon Redshift. Anda mengonfigurasi IDP Anda untuk mengizinkan pengguna federasi Anda mengakses peran IAM. Dengan peran IAM tersebut, Anda dapat menghasilkan kredensial database sementara dan masuk ke database Amazon Redshift.

Klien SQL Anda memerlukan izin untuk memanggil `GetClusterCredentials` operasi untuk Anda. Anda mengelola izin tersebut dengan membuat peran IAM dan melampirkan kebijakan izin IAM yang memberikan atau membatasi akses ke operasi dan tindakan terkait. `GetClusterCredentials` Sebagai praktik terbaik, kami merekomendasikan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).

Kebijakan ini juga memberikan atau membatasi akses ke sumber daya tertentu, seperti kluster Amazon Redshift, database, nama pengguna database, dan nama grup pengguna.

Note

Sebaiknya gunakan driver Amazon Redshift JDBC atau ODBC untuk mengelola proses panggilan `GetClusterCredentials` operasi dan masuk ke database. Untuk mempermudah, kami berasumsi bahwa Anda menggunakan klien SQL dengan driver JDBC atau ODBC di seluruh topik ini.

Untuk detail spesifik dan contoh penggunaan `GetClusterCredentials` operasi atau perintah `get-cluster-credentials` CLI paralel, lihat [GetClusterCredentials](#) dan [get-cluster-credentials](#)

Untuk mengelola otentikasi dan otorisasi secara terpusat, Amazon Redshift mendukung otentikasi database dengan IAM, memungkinkan otentikasi pengguna melalui federasi perusahaan. Alih-alih membuat pengguna, Anda dapat menggunakan identitas yang ada dari AWS Directory Service, direktori pengguna perusahaan Anda, atau penyedia identitas web. Ini dikenal sebagai pengguna federasi. AWS menetapkan peran untuk pengguna federasi ketika akses diminta melalui iDP.

Untuk menyediakan akses gabungan ke aplikasi pengguna atau klien di organisasi Anda untuk memanggil operasi Amazon Redshift API, Anda juga dapat menggunakan driver JDBC atau ODBC dengan dukungan SAMP 2.0 untuk meminta autentikasi dari IDP organisasi Anda. Dalam hal ini, pengguna organisasi Anda tidak memiliki akses langsung ke Amazon Redshift.

Membuat kredensial IAM sementara

Di bagian ini, Anda dapat menemukan cara mengonfigurasi sistem Anda untuk menghasilkan kredensial pengguna basis data berbasis IAM sementara dan masuk ke database Anda menggunakan kredensial baru.

Pada tingkat tinggi, proses mengalir sebagai berikut:

1. [Langkah 1: Buat peran IAM untuk akses masuk tunggal IAM](#)

(Opsional) Anda dapat mengautentikasi pengguna untuk mengakses database Amazon Redshift dengan mengintegrasikan autentikasi IAM dan penyedia identitas pihak ketiga (iDP).

2. [Langkah 2: Konfigurasi pernyataan SAMP untuk IDP Anda](#)

(Opsional) Untuk menggunakan autentikasi IAM menggunakan iDP, Anda perlu menentukan aturan klaim dalam aplikasi iDP yang memetakan pengguna atau grup di organisasi Anda

ke peran IAM. Secara opsional, Anda dapat menyertakan elemen atribut untuk mengatur `GetClusterCredentials` parameter.

3. [Langkah 3: Buat peran IAM dengan izin untuk memanggil `GetClusterCredentials`](#)

Aplikasi klien SQL Anda mengasumsikan pengguna saat memanggil operasi.

`GetClusterCredentials` Jika Anda membuat peran IAM untuk akses penyedia identitas, Anda dapat menambahkan izin yang diperlukan ke peran tersebut.

4. [Langkah 4: Buat basis data pengguna dan grup basis data](#)

(Opsional) Secara default, `GetClusterCredentials` mengembalikan kredensi membuat pengguna baru jika nama pengguna tidak ada. Anda juga dapat memilih untuk menentukan grup pengguna yang bergabung dengan pengguna saat masuk. Secara default, pengguna database bergabung dengan grup PUBLIC.

5. [Langkah 5: Konfigurasi koneksi JDBC atau ODBC untuk menggunakan kredensial IAM](#)

Untuk terhubung ke database Amazon Redshift, Anda mengonfigurasi klien SQL untuk menggunakan driver Amazon Redshift JDBC atau ODBC.

Langkah 1: Buat peran IAM untuk akses masuk tunggal IAM

Jika Anda tidak menggunakan penyedia identitas untuk akses masuk tunggal, Anda dapat melewati langkah ini.

Jika Anda sudah mengelola identitas pengguna di luar AWS, Anda dapat mengautentikasi pengguna untuk mengakses database Amazon Redshift dengan mengintegrasikan autentikasi IAM dan penyedia identitas SAML-2.0 pihak ketiga (iDP).

Untuk informasi selengkapnya, lihat [Penyedia Identitas dan Federasi](#) di Panduan Pengguna IAM.

Sebelum Anda dapat menggunakan autentikasi Amazon Redshift IDP, buat penyedia identitas SAMP. AWS Anda membuat iDP di konsol IAM untuk menginformasikan tentang iDP AWS dan konfigurasinya. Melakukan hal ini membangun kepercayaan antara AWS akun Anda dan IDP.

Untuk langkah-langkah membuat peran, lihat [Membuat Peran untuk Federasi SAMP 2.0 \(Konsol\)](#) di Panduan Pengguna IAM.

Langkah 2: Konfigurasi pernyataan SAMP untuk IDP Anda

Setelah membuat peran IAM, Anda menentukan aturan klaim di aplikasi iDP untuk memetakan pengguna atau grup di organisasi Anda ke peran IAM. Untuk informasi selengkapnya, lihat [Mengonfigurasi Pernyataan SAMP untuk Respons Otentikasi](#) di Panduan Pengguna IAM.

Jika Anda memilih untuk menggunakan `GetClusterCredentials` parameter opsional `DbUser`, `AutoCreate`, dan `DbGroups`, Anda memiliki dua opsi. Anda dapat mengatur nilai untuk parameter dengan koneksi JDBC atau ODBC Anda, atau Anda dapat mengatur nilai dengan menambahkan elemen atribut SAMP ke IDP Anda. Untuk informasi tentang parameter `DbUser`, `AutoCreate` dan `DbGroups`, lihat [Langkah 5: Konfigurasi koneksi JDBC atau ODBC untuk menggunakan kredensial IAM](#).

Note

Jika Anda menggunakan variabel kebijakan IAM `IAM${redshift:DbUser}`, seperti yang dijelaskan dalam [Kebijakan sumber daya untuk GetClusterCredentials](#) nilai `for DbUser` diganti dengan nilai yang diambil oleh konteks permintaan operasi API. Driver Amazon Redshift menggunakan nilai untuk `DbUser` variabel yang disediakan oleh URL koneksi, bukan nilai yang diberikan sebagai atribut SAMP.

Untuk membantu mengamankan konfigurasi ini, sebaiknya gunakan kondisi dalam kebijakan IAM untuk memvalidasi `DbUser` nilai dengan menggunakan `RoleSessionName` Anda dapat menemukan contoh cara menyetel kondisi menggunakan kebijakan IAM di [Contoh kebijakan untuk menggunakan GetClusterCredentials](#).

Untuk mengkonfigurasi IDP Anda untuk mengatur, dan `DbGroups` parameter `DbUserAutoCreate`, sertakan elemen-elemen berikut: `Attribute`

- `Attribute` Elemen dengan Name atribut disetel ke "https://redshift.amazon.com/SAML/Attributes/DbUser"

Atur `AttributeValue` elemen ke nama pengguna yang akan terhubung ke database Amazon Redshift.

Nilai dalam `AttributeValue` elemen harus huruf kecil, dimulai dengan huruf, hanya berisi karakter alfanumerik, garis bawah ('_'), tanda plus ('+'), titik ('.'), at ('@'), atau tanda hubung ('-'), dan kurang dari 128 karakter. Biasanya, nama pengguna adalah ID pengguna (misalnya,

bobsmith) atau alamat email (misalnya bobsmith@example.com). Nilai tidak dapat menyertakan spasi (misalnya, nama tampilan pengguna seperti Bob Smith).

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbUser">
  <AttributeValue>user-name</AttributeValue>
</Attribute>
```

- Elemen Atribut dengan atribut Name disetel ke "https://redshift.amazon.com/SAML/Attributes/AutoCreate"

Tetapkan AttributeValue elemen ke true untuk membuat pengguna database baru jika tidak ada. Setel AttributeValue ke false untuk menentukan bahwa pengguna database harus ada di database Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/AutoCreate">
  <AttributeValue>true</AttributeValue>
</Attribute>
```

- AttributeElemen dengan Name atribut diatur untuk disetel ke "https://redshift.amazon.com/SAML/Attributes/DbGroups"

Elemen ini mengandung satu atau lebih AttributeValue elemen. Tetapkan setiap AttributeValue elemen ke nama grup database yang DbUser bergabung selama durasi sesi saat menghubungkan ke database Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbGroups">
  <AttributeValue>group1</AttributeValue>
  <AttributeValue>group2</AttributeValue>
  <AttributeValue>group3</AttributeValue>
</Attribute>
```

Langkah 3: Buat peran IAM dengan izin untuk memanggil GetClusterCredentials

Klien SQL Anda memerlukan otorisasi untuk memanggil GetClusterCredentials operasi atas nama Anda. Untuk memberikan otorisasi tersebut, Anda membuat pengguna atau peran dan melampirkan kebijakan yang memberikan izin yang diperlukan.

Untuk membuat peran IAM dengan izin untuk memanggil `GetClusterCredentials`

1. Menggunakan layanan IAM, buat pengguna atau peran. Anda juga dapat menggunakan pengguna atau peran yang ada. Misalnya, jika Anda membuat peran IAM untuk akses penyedia identitas, Anda dapat melampirkan kebijakan IAM yang diperlukan ke peran tersebut.
2. Lampirkan kebijakan izin dengan izin untuk memanggil `redshift:GetClusterCredentials` operasi. Bergantung pada parameter opsional yang Anda tentukan, Anda juga dapat mengizinkan atau membatasi tindakan dan sumber daya tambahan dalam kebijakan Anda:
 - Untuk mengizinkan klien SQL Anda mengambil ID cluster, AWS Region, dan port, sertakan izin untuk memanggil `redshift:DescribeClusters` operasi dengan sumber daya cluster Redshift.
 - Jika Anda menggunakan `AutoCreate` opsi, sertakan izin untuk menelepon `redshift:CreateClusterUser` dengan `dbuser` sumber daya. Nama Sumber Daya Amazon (ARN) berikut menentukan Amazon Redshift. `dbuser` Ganti *regionaccount-id*, dan *cluster-name* dengan nilai untuk AWS Wilayah, akun, dan klaster Anda. Untuk *dbuser-name*, tentukan nama pengguna yang akan digunakan untuk masuk ke database cluster.

```
arn:aws:redshift:region:account-id:dbuser:cluster-name/dbuser-name
```

- (Opsional) Tambahkan ARN yang menentukan `dbname` resource Amazon Redshift dalam format berikut. Ganti *regionaccount-id*, dan *cluster-name* dengan nilai untuk AWS Wilayah, akun, dan klaster Anda. Untuk *database-name*, tentukan nama database tempat pengguna akan masuk.

```
arn:aws:redshift:region:account-id:dbname:cluster-name/database-name
```

- Jika Anda menggunakan `DbGroups` opsi, sertakan izin untuk memanggil `redshift:JoinGroup` operasi dengan `dbgroup` sumber daya Amazon Redshift dalam format berikut. Ganti *regionaccount-id*, dan *cluster-name* dengan nilai untuk AWS Wilayah, akun, dan klaster Anda. Untuk *dbgroup-name*, tentukan nama grup pengguna yang bergabung dengan pengguna saat login.

```
arn:aws:redshift:region:account-id:dbgroup:cluster-name/dbgroup-name
```

Untuk informasi selengkapnya dan contoh tambahan, lihat [Kebijakan sumber daya untuk GetClusterCredentials](#).

Contoh berikut menunjukkan kebijakan yang memungkinkan peran IAM untuk memanggil GetClusterCredentials operasi. Menentukan resource Amazon dbuser Redshift memberikan akses peran ke temp_creds_user nama pengguna database pada kluster bernama.

examplecluster

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
temp_creds_user"
  }
}
```

Anda dapat menggunakan wildcard (*) untuk mengganti semua, atau sebagian, nama cluster, nama pengguna, dan nama grup database. Contoh berikut memungkinkan nama pengguna apa pun yang dimulai temp_ dengan cluster apa pun di akun yang ditentukan.

Important

Pernyataan dalam contoh berikut menentukan karakter wildcard (*) sebagai bagian dari nilai sumber daya sehingga kebijakan mengizinkan sumber daya apa pun yang dimulai dengan karakter yang ditentukan. Menggunakan karakter wildcard dalam kebijakan IAM Anda mungkin terlalu permisif. Sebagai praktik terbaik, kami sarankan untuk menggunakan kebijakan paling ketat yang layak untuk aplikasi bisnis Anda.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:*/temp_*"
  }
}
```

Contoh berikut menunjukkan kebijakan yang memungkinkan peran IAM untuk memanggil `GetClusterCredentials` operasi dengan opsi untuk secara otomatis membuat pengguna baru dan menentukan grup yang bergabung dengan pengguna saat login. `"Resource": "*"` Klausula memberikan akses peran ke sumber daya apa pun, termasuk cluster, pengguna database, atau grup pengguna.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "redshift:GetClusterCredentials",
      "redshift:CreateClusterUser",
      "redshift:JoinGroup"
    ],
    "Resource": "*"
  }
}
```

Untuk informasi selengkapnya, lihat [sintaks Amazon Redshift ARN](#).

Langkah 4: Buat basis data pengguna dan grup basis data

Secara opsional, Anda dapat membuat pengguna database yang Anda gunakan untuk masuk ke database cluster. Jika Anda membuat kredensial pengguna sementara untuk pengguna yang sudah ada, Anda dapat menonaktifkan kata sandi pengguna untuk memaksa pengguna masuk dengan kata sandi sementara. Atau, Anda dapat menggunakan opsi `GetClusterCredentials Autocreate` untuk secara otomatis membuat pengguna database baru.

Anda dapat membuat grup pengguna database dengan izin yang Anda inginkan agar pengguna database IAM bergabung saat login. Saat Anda memanggil `GetClusterCredentials` operasi, Anda dapat menentukan daftar nama grup pengguna yang bergabung dengan pengguna baru saat login. Keanggotaan grup ini hanya berlaku untuk sesi yang dibuat menggunakan kredensial yang dihasilkan dengan permintaan yang diberikan.

Untuk membuat pengguna basis data dan grup basis data

1. [Masuk ke database Amazon Redshift Anda dan buat pengguna database menggunakan `CREATE USER` atau ubah pengguna yang ada menggunakan `ALTER USER`.](#)

2. Secara opsional, tentukan opsi DISABLE PASSWORD untuk mencegah pengguna menggunakan kata sandi. Ketika kata sandi pengguna dinonaktifkan, pengguna dapat masuk hanya menggunakan kredensi sementara. Jika kata sandi tidak dinonaktifkan, pengguna dapat masuk dengan kata sandi atau menggunakan kredensial sementara. Anda tidak dapat menonaktifkan kata sandi untuk pengguna super.

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses terprogram, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses terprogram?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. <ul style="list-style-type: none"> • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat otentikasi Pusat Identitas IAM di Panduan Referensi AWS SDK dan Alat.

Pegguna mana yang membutuhkan akses terprogram?	Untuk	Oleh
IAM	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk dalam Menggunakan kredensial sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredensial jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. <ul style="list-style-type: none"> • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensial pengguna IAM di Panduan Pengguna. AWS Command Line Interface • Untuk AWS SDK dan alat bantu, lihat Mengautentikasi menggunakan kredensial jangka panjang di Panduan Referensi AWS SDK dan Alat. • Untuk AWS API, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Contoh berikut membuat pengguna dengan password dinonaktifkan.

```
create user temp_creds_user password disable;
```

Contoh berikut menonaktifkan password untuk pengguna yang sudah ada.

```
alter user temp_creds_user password disable;
```

3. Buat grup pengguna database menggunakan [CREATE GROUP](#).
4. Gunakan perintah [GRANT](#) untuk menentukan hak akses untuk grup.

Langkah 5: Konfigurasikan koneksi JDBC atau ODBC untuk menggunakan kredensial IAM

Anda dapat mengonfigurasi klien SQL Anda dengan driver Amazon Redshift JDBC atau ODBC. Driver ini mengelola proses pembuatan kredensial pengguna database dan membuat koneksi antara klien SQL Anda dan database Amazon Redshift Anda.

Jika Anda menggunakan penyedia identitas untuk otentikasi, tentukan nama plugin penyedia kredensi. Driver Amazon Redshift JDBC dan ODBC menyertakan plugin untuk penyedia identitas berbasis SAML berikut:

- Microsoft Active Directory Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure AD

Untuk langkah-langkah mengatur Microsoft Azure AD sebagai penyedia identitas, lihat [Menyiapkan otentikasi masuk tunggal JDBC atau ODBC dengan Microsoft Azure AD](#).

Untuk mengkonfigurasi koneksi JDBC untuk menggunakan kredensial IAM

1. Unduh driver Amazon Redshift JDBC terbaru dari halaman. [Mengkonfigurasi koneksi untuk driver JDBC versi 2.1 untuk Amazon Redshift](#)
2. Buat URL JDBC dengan opsi kredensi IAM dalam salah satu format berikut. Untuk menggunakan autentikasi IAM, tambahkan `iam:` ke URL Amazon Redshift JDBC `jdbc:redshift:` berikut seperti yang ditunjukkan pada contoh berikut.

```
jdbc:redshift:iam://
```

Tambahkan `cluster-name`, `region`, dan `account-id`. Driver JDBC menggunakan informasi akun IAM dan nama cluster Anda untuk mengambil ID cluster dan Region. AWS Untuk melakukannya, pengguna atau peran Anda harus memiliki izin untuk memanggil

`redshift:DescribeClusters` operasi dengan cluster yang ditentukan. Jika pengguna atau peran Anda tidak memiliki izin untuk memanggil `redshift:DescribeClusters` operasi, sertakan ID cluster, AWS Wilayah, dan port seperti yang ditunjukkan pada contoh berikut. Nomor port adalah opsional.

```
jdbc:redshift:iam://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev
```

3. Tambahkan opsi JDBC untuk memberikan kredensial IAM. Anda menggunakan kombinasi opsi JDBC yang berbeda untuk memberikan kredensial IAM. Untuk detailnya, lihat [Opsi JDBC dan ODBC untuk Membuat Kredensi Pengguna Database](#).

URL berikut menentukan AccessKey ID dan SecretAccessKey untuk pengguna.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
AccessKeyId=AKIAIOSFODNN7EXAMPLE&SecretAccessKey=wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY
```

Contoh berikut menentukan profil bernama yang berisi kredensial IAM.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?Profile=user2
```

4. Tambahkan opsi JDBC yang digunakan driver JDBC untuk memanggil operasi `API.GetClusterCredentials`. Jangan sertakan opsi ini jika Anda memanggil operasi `API.GetClusterCredentials` secara terprogram.

Contoh berikut mencakup opsi `JDBCGetClusterCredentials`.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
plugin_name=com.amazon.redshift.plugin.AzureCredentialsProvider&UID=user&PWD=password&idp_t
```

Untuk mengonfigurasi koneksi ODBC untuk menggunakan kredensial IAM

Dalam prosedur berikut, Anda dapat menemukan langkah-langkah hanya untuk mengkonfigurasi otentikasi IAM. Untuk langkah-langkah menggunakan otentikasi standar, menggunakan nama pengguna dan kata sandi database, lihat [Mengkonfigurasi koneksi ODBC](#).

1. Instal dan konfigurasi driver Amazon Redshift ODBC terbaru untuk sistem operasi Anda. Untuk informasi lebih lanjut, lihat [Mengkonfigurasi koneksi ODBC](#) halaman.

⚠ Important

Driver Amazon Redshift ODBC harus versi 1.3.6.1000 atau yang lebih baru.

- Ikuti langkah-langkah untuk sistem operasi Anda untuk mengonfigurasi pengaturan koneksi.

Untuk informasi selengkapnya, lihat salah satu dari berikut ini:

- [Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#)
- [Gunakan pengelola driver ODBC untuk mengonfigurasi driver di sistem operasi Linux dan macOS X](#)

- Pada sistem operasi Microsoft Windows, akses jendela Pengaturan DSN Driver Amazon Redshift ODBC.

- Di bawah Pengaturan Koneksi, masukkan informasi berikut:

- Nama Sumber Data
- Server (opsional)
- Port (opsional)
- Basis Data

Jika pengguna atau peran Anda memiliki izin untuk memanggil `redshift:DescribeClusters` operasi, hanya Nama Sumber Data dan Database yang diperlukan. Amazon Redshift menggunakan `ClusterId` dan Wilayah untuk mendapatkan server dan port dengan memanggil operasi `DescribeCluster`

Jika pengguna atau peran Anda tidak memiliki izin untuk memanggil `redshift:DescribeClusters` operasi, tentukan Server dan Port.

- Di bawah Otentikasi, pilih nilai untuk Jenis Auth.

Untuk setiap jenis otentikasi, masukkan nilai seperti yang tercantum berikut:

AWS Profil

Masukkan informasi berikut:

- ClusterID
- Wilayah

- Nama profil

Masukkan nama profil dalam file AWS konfigurasi yang berisi nilai untuk opsi koneksi ODBC. Untuk informasi selengkapnya, lihat [Menggunakan Profil Konfigurasi](#).

(Opsional) Berikan detail untuk opsi yang digunakan driver ODBC untuk memanggil operasi `GetClusterCredentials` API:

- DbUser
- Pengguna AutoCreate
- DbGroups

Untuk informasi selengkapnya, lihat [Opsi JDBC dan ODBC untuk Membuat Kredensi Pengguna Database](#).

Kredensi IAM

Masukkan informasi berikut:

- ClusterID
- Wilayah
- AccessKeyID dan SecretAccessKey

ID kunci akses dan kunci akses rahasia untuk peran IAM atau pengguna yang dikonfigurasi untuk otentikasi database IAM.

- SessionToken

SessionToken diperlukan untuk peran IAM dengan kredensi sementara. Untuk informasi selengkapnya, lihat [Kredensial Keamanan Sementara](#).

Berikan detail untuk opsi yang digunakan driver ODBC untuk memanggil operasi `GetClusterCredentials` API:

- DbUser(Diperlukan)
- Pengguna AutoCreate (opsional)
- DbGroups(opsional)

Untuk informasi selengkapnya, lihat [Opsi JDBC dan ODBC untuk Membuat Kredensi Pengguna Database](#).

Penyedia Identitas: AD FS

Untuk Otentikasi Terintegrasi Windows dengan AD FS, biarkan Pengguna dan Kata Sandi kosong.

Berikan detail IDP:

- IdP Host

Nama host penyedia identitas perusahaan. Nama ini tidak boleh menyertakan garis miring (/).

- IDP Port (opsional)

Port yang digunakan oleh penyedia identitas. Default-nya adalah 443.

- Peran yang Diutamakan

Nama Sumber Daya Amazon (ARN) untuk peran IAM dari `AttributeValue` elemen multi-nilai untuk `Role` atribut dalam pernyataan SAMP. Untuk menemukan nilai yang sesuai untuk peran yang diinginkan, bekerjalah dengan administrator IDP Anda. Untuk informasi selengkapnya, lihat [Konfigurasi pernyataan SAMP untuk IDP Anda](#).

(Opsional) Berikan detail untuk opsi yang digunakan driver ODBC untuk memanggil operasi `GetClusterCredentials` API:

- DbUser
- Pengguna AutoCreate
- DbGroups

Untuk informasi selengkapnya, lihat [Opsi JDBC dan ODBC untuk Membuat Kredensi Pengguna Database](#).

Penyedia Identitas: PingFederate

Untuk Pengguna dan Kata Sandi, masukkan nama pengguna dan kata sandi IDP Anda.

Berikan detail IDP:

- IdP Host

Nama host penyedia identitas perusahaan. Nama ini tidak boleh menyertakan garis miring (/).

- IDP Port (opsional)

Port yang digunakan oleh penyedia identitas. Default-nya adalah 443.

- Peran yang Diutamakan

Nama Sumber Daya Amazon (ARN) untuk peran IAM dari `AttributeValue` elemen multi-nilai untuk `Role` atribut dalam pernyataan SAMP. Untuk menemukan nilai yang sesuai untuk peran yang diinginkan, bekerjalah dengan administrator IDP Anda. Untuk informasi selengkapnya, lihat [Konfigurasi pernyataan SAMP untuk IDP Anda](#).

(Opsional) Berikan detail untuk opsi yang digunakan driver ODBC untuk memanggil operasi `GetClusterCredentials` API:

- `DbUser`
- Pengguna `AutoCreate`
- `DbGroups`

Untuk informasi selengkapnya, lihat [Opsi JDBC dan ODBC untuk Membuat Kredensi Pengguna Database](#).

Penyedia Identitas: Okta

Untuk Pengguna dan Kata Sandi, masukkan nama pengguna dan kata sandi IDP Anda.

Berikan detail IDP:

- IDP Host

Nama host penyedia identitas perusahaan. Nama ini tidak boleh menyertakan garis miring (/).

- Pelabuhan IDP

Nilai ini tidak digunakan oleh Okta.

- Peran yang Diutamakan

Nama Sumber Daya Amazon (ARN) untuk peran IAM dari `AttributeValue` elemen untuk `Role` atribut dalam pernyataan SAMP. Untuk menemukan nilai yang sesuai

untuk peran yang diinginkan, bekerjalah dengan administrator iDP Anda. Untuk informasi selengkapnya, lihat [Konfigurasi pernyataan SAMP untuk IDP Anda](#).

- ID Aplikasi Okta

ID untuk aplikasi Okta. Nilai untuk ID Aplikasi mengikuti “amazon_aws” di tautan penyematan aplikasi Okta. Bekerja dengan administrator iDP Anda untuk mendapatkan nilai ini.

(Opsional) Berikan detail untuk opsi yang digunakan driver ODBC untuk memanggil operasi `GetClusterCredentials` API:

- DbUser
- Pengguna AutoCreate
- DbGroups

Untuk informasi selengkapnya, lihat [Opsi JDBC dan ODBC untuk Membuat Kredensi Pengguna Database](#).

Penyedia Identitas: Azure AD

Untuk Pengguna dan Kata Sandi, masukkan nama pengguna dan kata sandi IDP Anda.

Untuk ID Cluster dan Region, masukkan ID cluster dan AWS Region klaster Amazon Redshift Anda.

Untuk Database, masukkan database yang Anda buat untuk cluster Amazon Redshift Anda.

Berikan detail IDP:

- Penyewa iDP

Penyewa digunakan untuk Azure AD.

- Rahasia Klien Azure

Rahasia klien dari aplikasi perusahaan Amazon Redshift di Azure.

- ID Klien Azure

ID klien (ID aplikasi) dari aplikasi perusahaan Amazon Redshift di Azure.

(Opsional) Berikan detail untuk opsi yang digunakan driver ODBC untuk memanggil operasi `GetClusterCredentials` API:

- DbUser
- Pengguna AutoCreate
- DbGroups

Untuk informasi selengkapnya, lihat [Opsi JDBC dan ODBC untuk Membuat Kredensi Pengguna Database](#).

Opsinya untuk memberikan kredensial IAM

Untuk memberikan kredensial IAM untuk koneksi JDBC atau ODBC, pilih salah satu opsi berikut.

- AWS profil

Sebagai alternatif untuk memberikan nilai kredensial dalam bentuk pengaturan JDBC atau ODBC, Anda dapat menempatkan nilai dalam profil bernama. Untuk informasi selengkapnya, lihat [Menggunakan Profil Konfigurasi](#).

- Kredensial IAM

Berikan nilai untuk `AccessKey ID`, `SecretAccessKey`, dan, secara opsional, `SessionToken` dalam bentuk pengaturan JDBC atau ODBC. `SessionToken` diperlukan hanya untuk peran IAM dengan kredensial sementara. Untuk informasi selengkapnya, lihat [Opsi JDBC dan ODBC untuk menyediakan kredensial IAM](#).

- Federasi penyedia identitas

Saat Anda menggunakan federasi penyedia identitas untuk mengaktifkan pengguna dari penyedia identitas untuk mengautentikasi ke Amazon Redshift, tentukan nama plugin penyedia kredensial. Untuk informasi selengkapnya, lihat [Menggunakan plugin penyedia kredensial](#).

Driver Amazon Redshift JDBC dan ODBC menyertakan plugin untuk penyedia kredensial federasi identitas berbasis SAMP berikut:

- Layanan Federasi Identitas Aktif Microsoft (AD FS)
- PingOne
- Okta
- Microsoft Azure Active Directory (Azure AD)

Anda dapat memberikan nama plugin dan nilai terkait dalam bentuk pengaturan JDBC atau ODBC atau dengan menggunakan profil. Lihat informasi yang lebih lengkap di [Opsi untuk konfigurasi driver JDBC versi 2.1](#) dan [Konfigurasi opsi driver ODBC](#).

Untuk informasi selengkapnya, lihat [Konfigurasi koneksi JDBC atau ODBC untuk menggunakan kredensial IAM](#).

Menggunakan Profil Konfigurasi

Anda dapat menyediakan opsi dan `GetClusterCredentials` opsi kredensial IAM sebagai pengaturan dalam profil bernama di file konfigurasi Anda AWS. Untuk memberikan nama profil, gunakan opsi `Profil JDBC`. Konfigurasi disimpan dalam file bernama `config` atau file bernama `credentials` dalam folder bernama `.aws` di direktori home Anda.

Untuk plugin penyedia kredensial berbasis SAMP yang disertakan dengan driver Amazon Redshift JDBC atau ODBC, Anda dapat menggunakan pengaturan yang dijelaskan sebelumnya. [Menggunakan plugin penyedia kredensial](#) Jika `plugin_name` tidak digunakan, opsi lain diabaikan.

Contoh berikut menunjukkan file `~/.aws/credentials` dengan dua profil.

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY

[user2]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
session_token=AQoDYXdzEPT//////////
wEXAMPLEtc764bNrC9SAPBSM22wD0k4x4HIZ8j4FZTwdQWLwsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTf1fKD8YUuwthAx7
qkPpKPi/kMcGd
QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5V5XDvp75YU
9HFv1Rd8Tx6q6fE8YQcHNvXakiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fP0Ln9FX9KSYvKTr4rvx3iSI1TJabIQwj2ICCR/oLxBA==
```

Untuk menggunakan kredensial `user2` sebagai contoh, tentukan `Profile=user2` di URL JDBC.

Untuk informasi selengkapnya tentang penggunaan profil, lihat [Pengaturan konfigurasi dan file kredensial](#) di Panduan AWS Command Line Interface Pengguna.

Untuk informasi selengkapnya tentang penggunaan profil untuk driver JDBC, lihat [Menentukan profil](#)

Untuk informasi selengkapnya tentang penggunaan profil untuk driver ODBC, lihat [Mengkonfigurasi otentikasi](#).

Opsi JDBC dan ODBC untuk menyediakan kredensial IAM

Tabel berikut mencantumkan opsi JDBC dan ODBC untuk menyediakan kredensial IAM.

Opsi	Deskripsi
Iam	Untuk digunakan hanya dalam string koneksi ODBC. Setel ke 1 untuk menggunakan otentikasi IAM.
AccessKey ID	ID kunci akses dan kunci akses rahasia untuk peran IAM atau pengguna yang dikonfigurasi untuk otentikasi database IAM. <code>SessionToken</code> diperlukan hanya untuk peran IAM dengan kredensial sementara. <code>SessionToken</code> tidak digunakan untuk pengguna. Untuk informasi selengkapnya, lihat Kredensial Keamanan Sementara .
SecretAccessKey	
SessionToken	
plugin_name	Nama kelas yang sepenuhnya memenuhi syarat yang mengimplementasikan penyedia kredensial. Driver Amazon Redshift JDBC menyertakan plugin penyedia kredensial berbasis SAMP. Jika Anda menyediakan <code>plugin_name</code> , Anda juga dapat memberikan opsi terkait lainnya. Untuk informasi selengkapnya, lihat Menggunakan plugin penyedia kredensial .
Profile	Nama profil dalam file AWS kredensial atau konfigurasi yang berisi nilai untuk opsi koneksi JDBC. Untuk informasi selengkapnya, lihat Menggunakan Profil Konfigurasi .

Menggunakan plugin penyedia kredensial

Amazon Redshift menggunakan plugin penyedia kredensial untuk autentikasi masuk tunggal.

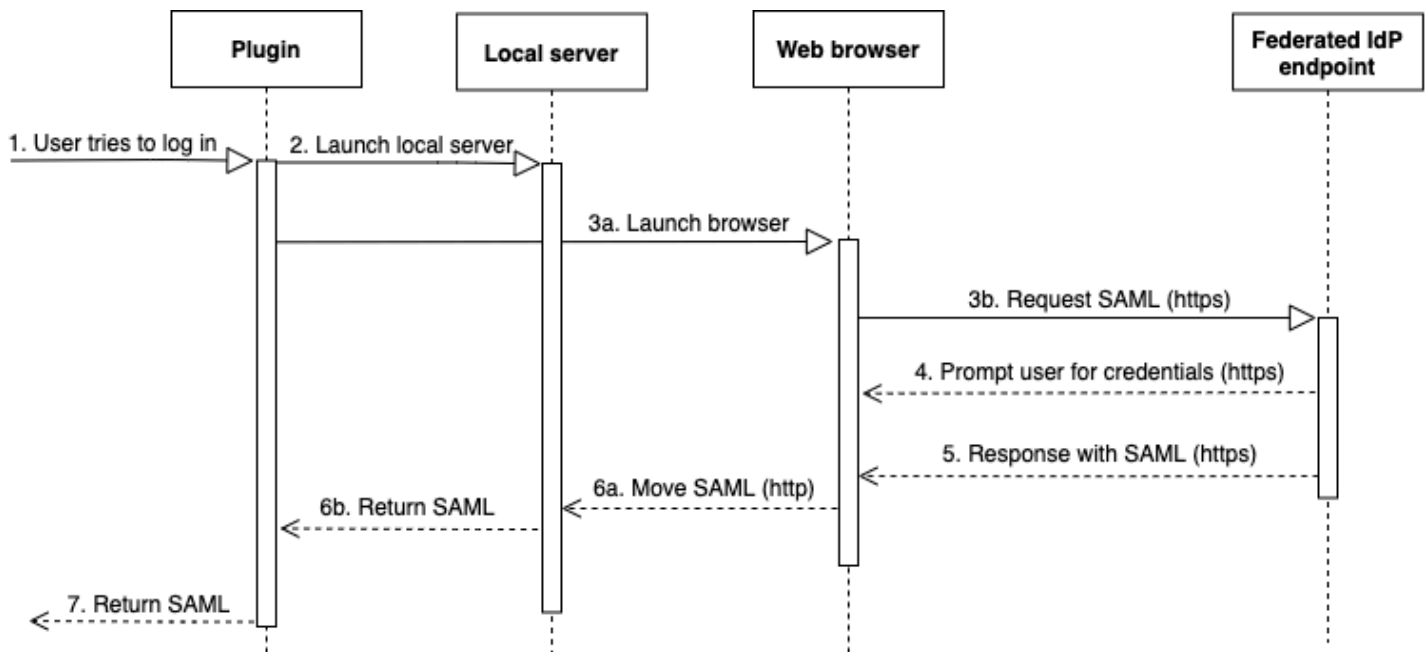
Untuk mendukung otentikasi masuk tunggal, Amazon Redshift menyediakan plugin Azure AD untuk Microsoft Azure Active Directory. Untuk informasi tentang cara mengkonfigurasi plugin ini, lihat [Menyiapkan otentikasi masuk tunggal JDBC atau ODBC dengan Microsoft Azure AD](#).

Menyiapkan otentikasi multi-faktor

Menyiapkan otentikasi multi-faktor

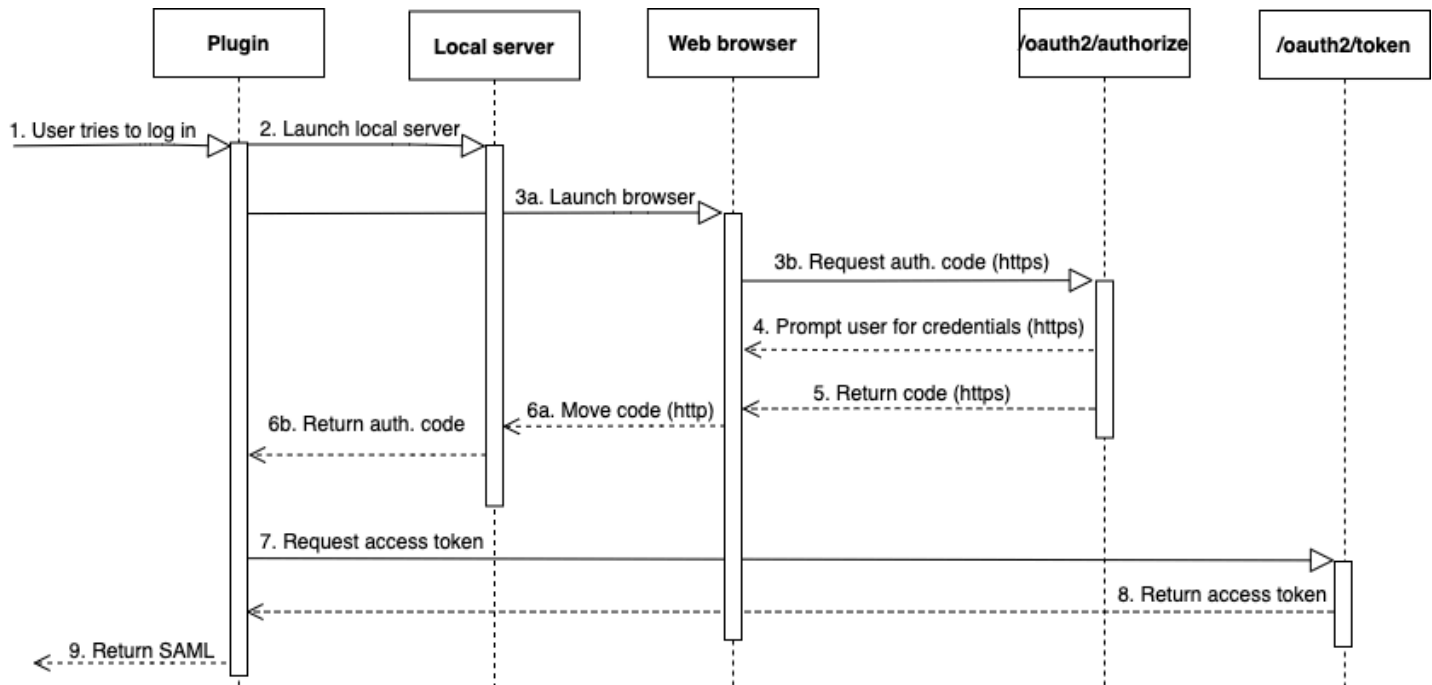
Untuk mendukung otentikasi multi-faktor (MFA), Amazon Redshift menyediakan plugin berbasis browser. Gunakan plugin SAMP browser untuk Okta PingOne, dan plugin Azure AD browser untuk Microsoft Azure Active Directory.

Dengan plugin SALL browser, otentikasi SAFL mengalir seperti ini:



1. Seorang pengguna mencoba masuk.
2. Plugin meluncurkan server lokal untuk mendengarkan koneksi masuk di localhost.
3. Plugin ini meluncurkan browser web untuk meminta respons SAMP melalui HTTPS dari titik akhir penyedia identitas federasi URL login masuk tunggal yang ditentukan.
4. Browser web mengikuti tautan dan meminta pengguna untuk memasukkan kredensial.
5. Setelah pengguna mengautentikasi dan memberikan persetujuan, titik akhir penyedia identitas federasi mengembalikan respons SAMP melalui HTTPS ke URI yang ditunjukkan oleh `redirect_uri`.
6. Browser web memindahkan pesan respons dengan respons SAMP ke yang ditunjukkan `redirect_uri`.
7. Server lokal menerima koneksi masuk dan plugin mengambil respons SAMP dan meneruskannya ke Amazon Redshift.

Dengan plugin browser Azure AD, otentikasi SAMP mengalir seperti ini:



1. Seorang pengguna mencoba masuk.
2. Plugin meluncurkan server lokal untuk mendengarkan koneksi masuk di localhost.
3. Plugin meluncurkan browser web untuk meminta kode otorisasi dari titik akhir Azure AD. `oauth2/authorize`
4. Browser web mengikuti tautan yang dihasilkan melalui HTTPS dan meminta pengguna untuk memasukkan kredensial. Tautan dihasilkan menggunakan properti konfigurasi, seperti `tenant` dan `client_id`.
5. Setelah pengguna mengotentikasi dan memberikan persetujuan, `oauth2/authorize` titik akhir Azure AD mengembalikan dan mengirimkan respons melalui HTTPS dengan kode otorisasi ke yang ditunjukkan `redirect_uri`
6. Browser web memindahkan pesan respons dengan respons SAMP ke yang ditunjukkan `redirect_uri`.
7. Server lokal menerima koneksi masuk dan permintaan plugin dan mengambil kode otorisasi dan mengirimkan permintaan POST ke titik akhir Azure AD. `oauth2/token`
8. `oauth2/token` titik akhir Azure AD mengembalikan respons dengan token akses ke yang ditunjukkan `redirect_uri`
9. Plugin mengambil respons SAMP dan meneruskannya ke Amazon Redshift.

Lihat bagian berikut:

- Microsoft Active Directory Federation Services (AD FS)

Untuk informasi selengkapnya, lihat [Menyiapkan otentikasi Single Sign-on JDBC atau ODBC dengan AD FS](#).

- PingOne (Ping)

Ping hanya didukung dengan Adaptor PingOne iDP yang telah ditentukan menggunakan otentikasi Formulir.

Untuk informasi selengkapnya, lihat [Menyiapkan otentikasi masuk tunggal JDBC atau ODBC dengan Ping Identity](#).

- Okta

Okta hanya didukung untuk aplikasi yang disediakan Okta yang digunakan dengan AWS Management Console

Untuk informasi selengkapnya, lihat [Menyiapkan otentikasi Single Sign-on JDBC atau ODBC dengan Okta](#).

- Direktori Aktif Microsoft Azure

Untuk informasi selengkapnya, lihat [Menyiapkan otentikasi masuk tunggal JDBC atau ODBC dengan Microsoft Azure AD](#).

Mengkonfigurasi opsi plugin

Mengkonfigurasi opsi plugin

Untuk menggunakan plugin penyedia kredensial berbasis SAML, tentukan opsi berikut menggunakan opsi JDBC atau ODBC atau dalam profil bernama. Jika `plugin_name` tidak ditentukan, opsi lain diabaikan.

Opsi	Deskripsi
<code>plugin_name</code>	Untuk JDBC, nama kelas yang mengimplementasikan penyedia kredensial. Tentukan satu dari yang berikut ini: <ul style="list-style-type: none"> • Untuk Layanan Federasi Direktori Aktif

Opsi	Deskripsi
	<pre data-bbox="337 210 1507 289">com.amazon.redshift.plugin.AdfsCredentialsProvider</pre> <ul data-bbox="305 304 500 336" style="list-style-type: none"> • Untuk Okta <pre data-bbox="337 373 1507 453">com.amazon.redshift.plugin.OktaCredentialsProvider</pre> <ul data-bbox="305 468 625 499" style="list-style-type: none"> • Untuk PingFederate <pre data-bbox="337 537 1507 617">com.amazon.redshift.plugin.PingCredentialsProvider</pre> <ul data-bbox="305 632 885 663" style="list-style-type: none"> • Untuk Microsoft Azure Active Directory <pre data-bbox="337 701 1507 781">com.amazon.redshift.plugin.AzureCredentialsProvider</pre> <ul data-bbox="305 795 597 827" style="list-style-type: none"> • Untuk SAMP MFA <pre data-bbox="337 865 1507 945">com.amazon.redshift.plugin.BrowserSamlCredentialsProvider</pre> <ul data-bbox="305 959 1291 991" style="list-style-type: none"> • Untuk Microsoft Azure Active Directory masuk tunggal dengan MFA <pre data-bbox="337 1029 1507 1108">com.amazon.redshift.plugin.BrowserAzureCredentialsProvider</pre> <p data-bbox="305 1186 998 1218">Untuk ODBC, tentukan salah satu dari berikut ini:</p> <ul data-bbox="305 1270 1404 1638" style="list-style-type: none"> • Untuk Layanan Federasi Direktori Aktif: <code>adfs</code> • Untuk Okta: <code>okta</code> • Untuk PingFederate: <code>ping</code> • Untuk Microsoft Azure Active Directory: <code>azure</code> • Untuk SAMP MFA: <code>browser saml</code> • Untuk sistem masuk tunggal Microsoft Azure Active Directory dengan MFA: <code>browser azure ad</code>
<code>idp_host</code>	<p data-bbox="305 1711 1485 1837">Nama host penyedia identitas perusahaan. Nama ini tidak boleh menyertakan garis miring (<code>/</code>). Untuk penyedia identitas Okta, nilai untuk <code>idp_host</code> harus diakhiri dengan <code>.okta.com</code> .</p>

Opsi	Deskripsi
<code>idp_port</code>	Port yang digunakan oleh penyedia identitas. Default-nya adalah 443. Port ini diabaikan untuk Okta.
<code>preferred_role</code>	Peran Amazon Resource Name (ARN) dari <code>AttributeValue</code> elemen untuk <code>Role</code> atribut dalam pernyataan SAMP. Untuk menemukan nilai yang sesuai untuk peran yang diinginkan, bekerjalah dengan administrator iDP Anda. Untuk informasi selengkapnya, lihat Konfigurasi pernyataan SAMP untuk IDP Anda .
<code>user</code>	Nama pengguna perusahaan, termasuk domain bila berlaku. Misalnya, untuk Active Directory, nama domain diperlukan dalam format <code>domain\username</code> .
<code>password</code>	Kata sandi pengguna perusahaan. Kami menyarankan untuk tidak menggunakan opsi ini. Sebagai gantinya, gunakan klien SQL Anda untuk memasok kata sandi.
<code>app_id</code>	ID untuk aplikasi Okta. Hanya digunakan dengan Okta. Nilai untuk <code>app_id</code> mengikuti <code>amazon_aws</code> di tautan embed aplikasi Okta. Untuk mendapatkan nilai ini, bekerja dengan administrator iDP Anda. Berikut ini adalah contoh link embed aplikasi: <code>https://example.okta.com/home/amazon_aws/0oa2hylwrpM8UGehd1t7/272</code>
<code>idp_tenant</code>	Penyewa yang digunakan untuk Azure AD. Digunakan hanya dengan Azure.
<code>client_id</code>	ID klien untuk aplikasi perusahaan Amazon Redshift di Azure AD. Digunakan hanya dengan Azure.

Menyiapkan otentikasi masuk tunggal JDBC atau ODBC dengan Microsoft Azure AD

Anda dapat menggunakan Microsoft Azure AD sebagai penyedia identitas (iDP) untuk mengakses kluster Amazon Redshift Anda. Berikut ini, Anda dapat menemukan prosedur yang menjelaskan cara mengatur hubungan kepercayaan untuk tujuan ini. Untuk informasi selengkapnya tentang mengonfigurasi AWS sebagai penyedia layanan untuk iDP, [lihat Mengonfigurasi IDP SAMP 2.0 Anda dengan Kepercayaan Pihak yang Mengandalkan dan Menambahkan Klaim](#) di Panduan Pengguna IAM.

Note

Untuk menggunakan Azure AD dengan JDBC, driver Amazon Redshift JDBC harus versi 1.2.37.1061 atau yang lebih baru. Untuk menggunakan Azure AD dengan ODBC, driver Amazon Redshift ODBC harus versi 1.4.10.1000 atau yang lebih baru.

Tonton video berikut untuk mempelajari cara menggabungkan akses Amazon Redshift dengan sistem masuk tunggal Microsoft Azure AD: [Menggabungkan akses Amazon Redshift dengan sistem masuk tunggal Microsoft Azure AD](#).

Untuk mengatur Azure AD dan AWS akun Anda agar saling percaya

1. Buat atau gunakan kluster Amazon Redshift yang ada agar pengguna Azure AD dapat terhubung. Untuk mengkonfigurasi koneksi, properti tertentu dari cluster ini diperlukan, seperti pengidentifikasi cluster. Untuk informasi selengkapnya, lihat [Membuat Cluster](#).
2. Siapkan Direktori Aktif Azure, grup, pengguna yang digunakan AWS di portal Microsoft Azure.
3. Tambahkan Amazon Redshift sebagai aplikasi perusahaan di portal Microsoft Azure untuk digunakan untuk masuk tunggal ke AWS Konsol dan login gabungan ke Amazon Redshift. Pilih aplikasi Enterprise.
4. Pilih +Aplikasi baru. Halaman Tambahkan aplikasi muncul.
5. Cari **AWS** di bidang pencarian.
6. Pilih Amazon Web Services (AWS) dan pilih Tambah. Ini menciptakan AWS aplikasi.
7. Di bawah Kelola, pilih Single sign-on.
8. Pilih SAML. Halaman Amazon Web Services (AWS) | Masuk berbasis SAML muncul.
9. Pilih Ya untuk melanjutkan ke halaman Mengatur Single Sign-On dengan SAMP. Halaman ini menampilkan daftar atribut terkait sistem masuk tunggal yang telah dikonfigurasi sebelumnya.
10. Untuk Konfigurasi SAMP Dasar, pilih ikon edit dan pilih Simpan.
11. Saat Anda mengonfigurasi lebih dari satu aplikasi, berikan nilai pengenalan. Misalnya, masukkan **<https://signin.aws.amazon.com/saml#2>**. Perhatikan bahwa dari aplikasi kedua dan seterusnya, gunakan format ini dengan tanda # untuk menentukan nilai SPN yang unik.
12. Di bagian Atribut Pengguna dan Klaim, pilih ikon edit.

Secara default, Unique User Identifier (UID), Peran RoleSessionName, dan SessionDuration klaim sudah dikonfigurasi sebelumnya.

13. Pilih + Tambahkan klaim baru untuk menambahkan klaim bagi pengguna database.

Untuk Nama, masukkan **DbUser**.

Untuk Namespace, masukkan **https://redshift.amazon.com/SAML/Attributes**.

Untuk Sumber, pilih Atribut.

Untuk atribut Source, pilih user.userprincipalname. Lalu, pilih Simpan.

14. Pilih + Tambahkan klaim baru untuk menambahkan klaim AutoCreate.

Untuk Nama, masukkan **AutoCreate**.

Untuk Namespace, masukkan **https://redshift.amazon.com/SAML/Attributes**.

Untuk Sumber, pilih Atribut.

Untuk atribut Source, pilih "true". Lalu, pilih Simpan.

Di sini, *123456789012* adalah AWS akun Anda, *AzureSSO* adalah peran IAM yang Anda buat, dan *AzureADProvider* merupakan penyedia IAM.

Nama klaim	Nilai
Pengenal pengguna unik (ID nama)	user.userprincipalname
https://aws.amazon.com/SAML/Attributes/SessionDuration	"900"
https://aws.amazon.com/SAML/Attributes/Role	<i>arn:aws:iam:: 123456789012: peran/azuresso, arn:aws:iam:: 123456789012: saml-provider/ azuReadProvider</i>
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.userprincipalname
https://redshift.amazon.com/SAML/Attributes/ AutoCreate	"benar"

Nama klaim	Nilai
<code>https://redshift.amazon.com/SAML/Attributes/DbGroups</code>	<code>user.assignedroles</code>
<code>https://redshift.amazon.com/SAML/Attributes/DbUser</code>	<code>user.userprincipalname</code>

15. Di bawah Pendaftaran Aplikasi > ***your-application-name*** > Otentikasi, tambahkan Aplikasi Seluler Dan Desktop. Tentukan URL sebagai `http://localhost/redshift/`.
16. Di bagian Sertifikat Penandatanganan SAMP, pilih Unduh untuk mengunduh dan menyimpan file XHTML metadata federasi untuk digunakan saat Anda membuat penyedia identitas SAMP IAM. File ini digunakan untuk membuat identitas federasi masuk tunggal.
17. Buat penyedia identitas SAMP IAM di konsol IAM. Dokumen metadata yang Anda berikan adalah file XML metadata federasi yang Anda simpan saat menyiapkan Aplikasi Azure Enterprise. Untuk langkah-langkah mendetail, lihat [Membuat dan Mengelola Penyedia Identitas IAM \(Konsol\)](#) di Panduan Pengguna IAM.
18. Buat peran IAM untuk federasi SAML 2.0 di konsol IAM. Untuk langkah-langkah mendetail, lihat [Membuat Peran untuk SAMP](#) di Panduan Pengguna IAM.
19. Buat kebijakan IAM yang dapat Anda lampirkan ke peran IAM yang Anda buat untuk federasi SAMP 2.0 di konsol IAM. Untuk langkah-langkah mendetail, lihat [Membuat Kebijakan IAM \(Konsol\)](#) di Panduan Pengguna IAM.

Ubah kebijakan berikut (dalam format JSON) untuk lingkungan Anda:

- Gantikan AWS Region cluster Anda untuk ***us-west-1***.
- Ganti AWS akun Anda untuk ***123456789012***.
- Gantikan pengenal klaster Anda (atau * untuk semua cluster) untuk ***cluster-identifier***
- Gantikan database Anda (atau * untuk semua database) untuk ***dev***.
- Gantikan pengenal unik peran IAM Anda. ***AROAJ2UCCR6DPCEXAMPLE***
- Gantikan domain email penyewa atau perusahaan Anda. ***example.com***
- Gantikan grup database yang Anda rencanakan untuk menetapkan pengguna. ***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": "*"
      }
    ]
  }
}

```

Kebijakan ini memberikan izin sebagai berikut:

- Bagian pertama memberikan izin ke operasi `GetClusterCredentials` API untuk mendapatkan kredensial sementara untuk klaster yang ditentukan. Dalam contoh ini, sumber daya adalah `cluster-identifier` dengan database `dev`, dalam akun `123456789012`, dan di AWS Wilayah `us-west-1`. `${redshift:DbUser}` Klausula ini hanya memungkinkan pengguna yang cocok dengan `DbUser` nilai yang ditentukan dalam Azure AD untuk terhubung.
- Klausul kondisi memberlakukan bahwa hanya pengguna tertentu yang mendapatkan kredensial sementara. Ini adalah pengguna di bawah peran yang ditentukan oleh ID unik peran `AROAJ2UCCR6DPCEXAMPLE` di akun IAM yang diidentifikasi oleh alamat email di domain email perusahaan Anda. Untuk informasi selengkapnya tentang ID unik, lihat [ID Unik](#) di Panduan Pengguna IAM.

Penyiapan Anda dengan iDP Anda (dalam hal ini, Azure AD) menentukan bagaimana klausa kondisi ditulis. Jika email karyawan Anda `johndoe@example.com`, atur terlebih dahulu `${redshift:DbUser}` ke bidang super yang cocok dengan nama pengguna karyawan `johndoe`. Kemudian, untuk membuat kondisi ini berfungsi, atur `RoleSessionName` bidang AWS SAMP ke bidang super yang cocok dengan email `johndoe@example.com` karyawan. Saat Anda mengambil pendekatan ini, pertimbangkan hal berikut:

- Jika Anda mengatur `${redshift:DbUser}` untuk menjadi email karyawan, maka hapus `@example.com` dalam contoh JSON untuk mencocokkan `RoleSessionName`.
- Jika Anda menetapkan `RoleSessionId` untuk menjadi hanya nama pengguna karyawan, maka hapus `@example.com` dalam contoh untuk mencocokkan `RoleSessionName`.
- Dalam contoh JSON, `${redshift:DbUser}` dan `RoleSessionName` keduanya diatur ke email karyawan. Contoh ini JSON menggunakan nama `@example.com` pengguna database Amazon Redshift untuk menandatangani pengguna untuk mengakses cluster.
- Bagian kedua memberikan izin untuk membuat `dbuser` nama di cluster yang ditentukan. Dalam contoh ini JSON, ini membatasi pembuatan untuk `${redshift:DbUser}`
- Bagian ketiga memberikan izin untuk menentukan pengguna mana `dbgroup` yang dapat bergabung. Dalam contoh ini JSON, pengguna dapat bergabung dengan `my_dbgroup` grup dalam cluster yang ditentukan.
- Bagian keempat memberikan izin untuk tindakan yang dapat dilakukan pengguna pada semua sumber daya. Dalam contoh ini JSON, memungkinkan pengguna untuk memanggil `redshift:DescribeClusters` untuk mendapatkan informasi cluster seperti titik akhir cluster, AWS Region, dan port. Ini juga memungkinkan pengguna untuk menelepon `iam:ListRoles` untuk memeriksa peran mana yang dapat diasumsikan pengguna.

Untuk mengatur JDBC untuk otentikasi ke Microsoft Azure AD

- Konfigurasi klien database Anda untuk terhubung ke cluster Anda melalui JDBC menggunakan sistem masuk tunggal Azure AD Anda.

Anda dapat menggunakan klien apa pun yang menggunakan driver JDBC untuk terhubung menggunakan sistem masuk tunggal Azure AD atau menggunakan bahasa seperti Java untuk terhubung menggunakan skrip. Untuk informasi instalasi dan konfigurasi, lihat [Mengkonfigurasi koneksi untuk driver JDBC versi 2.1 untuk Amazon Redshift](#).

Misalnya, Anda dapat menggunakan SqlWorkBench/J sebagai klien. Saat Anda mengkonfigurasi SQLWorkBench/J, URL database Anda menggunakan format berikut.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Jika Anda menggunakan SqlWorkBench/J sebagai klien, ambil langkah-langkah berikut:

- a. Mulai SQL Workbench/J. Pada halaman Select Connection Profile, tambahkan Profil Grup yang disebut. **AzureAuth**
- b. Untuk Profil Koneksi, masukkan **Azure**.
- c. Pilih Kelola Driver, dan pilih Amazon Redshift. Pilih ikon Open Folder di sebelah Library, lalu pilih file JDBC .jar yang sesuai.
- d. Pada halaman Pilih Profil Koneksi, tambahkan informasi ke profil koneksi sebagai berikut:
 - Untuk Pengguna, masukkan nama pengguna Microsoft Azure Anda. Ini adalah nama pengguna akun Microsoft Azure yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke cluster yang Anda coba autentikasi.
 - Untuk Kata Sandi, masukkan kata sandi Microsoft Azure Anda.
 - Untuk Driver, pilih Amazon Redshift (com.amazon.redshift.jdbc.driver).
 - Untuk URL, masukkan ***jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name***.
- e. Pilih Extended Properties untuk menambahkan informasi tambahan ke properti koneksi, seperti yang dijelaskan berikut.

Untuk konfigurasi masuk tunggal Azure AD, tambahkan informasi tambahan sebagai berikut:

- Untuk `plugin_name`, masukkan. **`com.amazon.redshift.plugin.AzureCredentialsProvider`** Nilai ini menentukan driver untuk menggunakan Azure AD Single Sign-On sebagai metode otentikasi.
- Untuk `idp_tenant`, masukkan. ***your-idp-tenant*** Hanya digunakan untuk Microsoft Azure AD. Ini adalah nama penyewa perusahaan Anda yang dikonfigurasi pada Azure AD. Nilai ini dapat berupa nama penyewa atau ID unik penyewa dengan tanda hubung.
- Untuk `client_secret`, masukkan. ***your-azure-redshift-application-client-secret*** Hanya digunakan untuk Microsoft Azure AD. Ini adalah rahasia klien Anda dari aplikasi Amazon Redshift yang Anda buat saat mengatur konfigurasi Azure Single Sign-On Anda. Ini hanya berlaku untuk `com.amazon.redshift.plugin.AzureCredentialsProvider` plugin.
- Untuk `client_id`, masukkan. ***your-azure-redshift-application-client-id*** Hanya digunakan untuk Microsoft Azure AD. Ini adalah ID klien (dengan tanda hubung) dari aplikasi Amazon Redshift yang Anda buat saat mengatur konfigurasi Azure Single Sign-On Anda.

Untuk sistem masuk tunggal Azure AD dengan konfigurasi MFA, tambahkan informasi tambahan ke properti koneksi sebagai berikut:

- Untuk `plugin_name`, masukkan. **`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`** Nilai ini menentukan driver untuk menggunakan sistem masuk tunggal Azure AD dengan MFA sebagai metode otentikasi.
- Untuk `idp_tenant`, masukkan. ***your-idp-tenant*** Hanya digunakan untuk Microsoft Azure AD. Ini adalah nama penyewa perusahaan Anda yang dikonfigurasi pada Azure AD. Nilai ini dapat berupa nama penyewa atau ID unik penyewa dengan tanda hubung.
- Untuk `client_id`, masukkan. ***your-azure-redshift-application-client-id*** Opsi ini hanya digunakan untuk Microsoft Azure AD. Ini adalah ID klien (dengan tanda hubung) dari aplikasi Amazon Redshift yang Anda buat saat mengatur sistem masuk tunggal Azure AD Anda dengan konfigurasi MFA.
- Untuk `listen_port`, masukkan. ***your-listen-port*** Ini adalah port yang didengarkan oleh server lokal. Defaultnya adalah 7890.
- Untuk `idp_response_timeout`, masukkan. ***the-number-of-seconds*** Ini adalah jumlah detik untuk menunggu sebelum waktu habis ketika server iDP mengirim kembali respons.

Jumlah minimum detik harus 10. Jika membuat koneksi membutuhkan waktu lebih lama dari ambang ini, maka koneksi dibatalkan.

Untuk mengatur ODBC untuk otentikasi ke Microsoft Azure AD

- Konfigurasi klien database Anda untuk terhubung ke cluster Anda melalui ODBC menggunakan sistem masuk tunggal Azure AD Anda.

Amazon Redshift menyediakan driver ODBC untuk sistem operasi Linux, Windows, dan macOS. Sebelum Anda menginstal driver ODBC, tentukan apakah alat klien SQL Anda 32-bit atau 64-bit. Instal driver ODBC yang sesuai dengan persyaratan alat klien SQL Anda.

Juga instal dan konfigurasi driver Amazon Redshift ODBC terbaru untuk sistem operasi Anda sebagai berikut:

- Untuk Windows, lihat [Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#).
- Untuk macOS, lihat [Instal driver Amazon Redshift ODBC di macOS X](#)
- Untuk Linux, lihat [Instal driver Amazon Redshift ODBC di Linux](#).

Di Windows, di halaman Pengaturan DSN Driver Amazon Redshift ODBC, di bawah Pengaturan Koneksi, masukkan informasi berikut:

- Untuk Nama Sumber Data, masukkan ***your-DSN***. Ini menentukan nama sumber data yang digunakan sebagai nama profil ODBC.
- Untuk tipe Auth untuk konfigurasi masuk tunggal Azure AD, pilih **Identity Provider: Azure AD**. Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi menggunakan sistem masuk tunggal Azure.
- Untuk tipe Auth untuk sistem masuk tunggal Azure AD dengan konfigurasi MFA, pilih **Identity Provider: Browser Azure AD**. Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi menggunakan Azure single sign-on dengan MFA.
- Untuk ID Cluster, masukkan ***your-cluster-identifier***.
- Untuk Wilayah, masukkan ***your-cluster-region***.
- Untuk Database, masukkan ***your-database-name***.
- Untuk Pengguna, masukkan ***your-azure-username***. Ini adalah nama pengguna untuk akun Microsoft Azure yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke cluster

yang Anda coba autentikasi. Gunakan ini hanya untuk Jenis Auth adalah Penyedia Identitas: Azure AD.

- Untuk Kata Sandi, masukkan ***your-azure-password***. Gunakan ini hanya untuk Jenis Auth adalah Penyedia Identitas: Azure AD.
- Untuk IDP Tenant, masukkan. ***your-idp-tenant*** Ini adalah nama penyewa perusahaan Anda yang dikonfigurasi di IDP (Azure) Anda. Nilai ini dapat berupa nama penyewa atau ID unik penyewa dengan tanda hubung.
- Untuk Rahasia Klien Azure, masukkan ***your-azure-redshift-application-client-secret***. Ini adalah rahasia klien dari aplikasi Amazon Redshift yang Anda buat saat mengatur konfigurasi masuk tunggal Azure Anda.
- Untuk ID Klien Azure, masukkan ***your-azure-redshift-application-client-id***. Ini adalah ID klien (dengan tanda hubung) dari aplikasi Amazon Redshift yang Anda buat saat mengatur konfigurasi masuk tunggal Azure Anda.
- Untuk Listen Port, masukkan ***your-listen-port***. Ini adalah port mendengarkan default yang didengarkan oleh server lokal. Defaultnya adalah 7890. Ini hanya berlaku untuk plugin Browser Azure AD.
- Untuk Response Timeout, masukkan ***the-number-of-seconds***. Ini adalah jumlah detik untuk menunggu sebelum waktu habis ketika server iDP mengirim kembali respons. Jumlah minimum detik harus 10. Jika membuat koneksi membutuhkan waktu lebih lama dari ambang ini, maka koneksi dibatalkan. Opsi ini hanya berlaku untuk plugin Browser Azure AD.

Di macOS dan Linux, edit `odbc.ini` file sebagai berikut:

 Note

Semua entri tidak peka huruf besar/kecil.

- Untuk clusterid, masukkan. ***your-cluster-identifier*** Ini adalah nama cluster Amazon Redshift yang dibuat.
- Untuk wilayah, masukkan ***your-cluster-region***. Ini adalah AWS Wilayah cluster Amazon Redshift yang dibuat.
- Untuk database, masukkan ***your-database-name***. Ini adalah nama database yang Anda coba akses di cluster Amazon Redshift.
- Untuk lokal, masukkan ***en-us***. Ini adalah bahasa yang menampilkan pesan kesalahan

- Untuk `iam`, masukkan **1**. Nilai ini menentukan driver untuk mengautentikasi menggunakan kredensial IAM.
- Untuk `plugin_name` untuk konfigurasi masuk tunggal Azure AD, masukkan **AzureAD**. Ini menentukan driver untuk menggunakan Azure Single Sign-On sebagai metode otentikasi.
- Untuk `plugin_name` untuk sistem masuk tunggal Azure AD dengan konfigurasi MFA, masukkan **BrowserAzureAD**. Ini menentukan driver untuk menggunakan Azure Single Sign-On dengan MFA sebagai metode otentikasi.
- Untuk `uid`, masukkan ***your-azure-username***. Ini adalah nama pengguna akun Microsoft Azure yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke cluster yang Anda coba autentikasi. Gunakan ini hanya untuk `plugin_name` adalah `AzuRead`.
- Untuk `pwd`, masukkan ***your-azure-password***. Gunakan ini hanya untuk `plugin_name` adalah `AzuRead`.
- Untuk `idp_tenant`, masukkan ***your-idp-tenant***. Ini adalah nama penyewa perusahaan Anda yang dikonfigurasi di IDP (Azure) Anda. Nilai ini dapat berupa nama penyewa atau ID unik penyewa dengan tanda hubung.
- Untuk `client_secret`, masukkan ***your-azure-redshift-application-client-secret***. Ini adalah rahasia klien dari aplikasi Amazon Redshift yang Anda buat saat mengatur konfigurasi masuk tunggal Azure Anda.
- Untuk `client_id`, masukkan ***your-azure-redshift-application-client-id***. Ini adalah ID klien (dengan tanda hubung) dari aplikasi Amazon Redshift yang Anda buat saat mengatur konfigurasi masuk tunggal Azure Anda.
- Untuk `listen_port`, masukkan ***your-listen-port***. Ini adalah port yang didengarkan oleh server lokal. Defaultnya adalah 7890. Ini berlaku untuk plugin Browser Azure AD.
- Untuk `idp_response_timeout`, masukkan ***the-number-of-seconds***. Ini adalah periode waktu yang ditentukan dalam hitungan detik untuk menunggu respons dari Azure. Opsi ini berlaku untuk plugin Browser Azure AD.

Di macOS dan Linux, edit juga pengaturan profil untuk menambahkan ekspor berikut.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Untuk memecahkan masalah dengan plugin Browser Azure AD

1. Untuk menggunakan plugin Browser Azure AD, Anda harus mengatur URL balasan yang ditentukan dalam permintaan agar sesuai dengan URL balasan yang dikonfigurasi untuk aplikasi Anda.

Arahkan ke halaman Siapkan Single Sign-On dengan SAMP di portal Microsoft Azure. Kemudian periksa URL Balas diatur ke `http://localhost/redshift/`.

2. Jika Anda mendapatkan kesalahan penyewa IDP, verifikasi bahwa nama IDP Tenant cocok dengan nama domain yang awalnya Anda gunakan untuk mengatur Direktori Aktif di Microsoft Azure.

Di Windows, navigasikan ke bagian Pengaturan Koneksi di halaman Pengaturan Amazon Redshift ODBC DSN. Kemudian periksa nama penyewa perusahaan Anda yang dikonfigurasi di IDP (Azure) cocok dengan nama domain yang awalnya Anda gunakan untuk mengatur Direktori Aktif di Microsoft Azure.

Di macOS dan Linux, temukan file `odbc.ini`. Kemudian periksa nama penyewa perusahaan Anda yang dikonfigurasi di IDP (Azure) cocok dengan nama domain yang awalnya Anda gunakan untuk mengatur Direktori Aktif di Microsoft Azure.

3. Jika Anda mendapatkan kesalahan bahwa URL balasan yang ditentukan dalam permintaan tidak cocok dengan URL balasan yang dikonfigurasi untuk aplikasi Anda, verifikasi bahwa URI Pengalihan sama dengan URL balasan.

Arahkan ke halaman pendaftaran Aplikasi aplikasi Anda di portal Microsoft Azure. Kemudian periksa URI Redirect cocok dengan URL balasan.

4. Jika Anda mendapatkan respons tak terduga: kesalahan tidak sah, verifikasi bahwa Anda telah menyelesaikan konfigurasi aplikasi Seluler dan desktop.

Arahkan ke halaman pendaftaran Aplikasi aplikasi Anda di portal Microsoft Azure. Kemudian navigasikan ke Otentikasi dan periksa apakah Anda mengonfigurasi aplikasi Seluler dan desktop untuk menggunakan `http://localhost/redshift/` sebagai URI pengalihan.

Menyiapkan otentikasi Single Sign-on JDBC atau ODBC dengan AD FS

Anda dapat menggunakan AD FS sebagai penyedia identitas (iDP) untuk mengakses kluster Amazon Redshift Anda. Berikut ini, Anda dapat menemukan prosedur yang menjelaskan cara mengatur hubungan kepercayaan untuk tujuan ini. Untuk informasi selengkapnya tentang mengonfigurasi

AWS sebagai penyedia layanan untuk AD FS, lihat [Mengonfigurasi IDP SAMP 2.0 Anda dengan Kepercayaan Pihak yang Mengandalkan dan Menambahkan Klaim](#) di Panduan Pengguna IAM.

Untuk mengatur AD FS dan AWS akun Anda agar saling percaya

1. Buat atau gunakan klaster Amazon Redshift yang ada agar pengguna AD FS dapat terhubung. Untuk mengkonfigurasi koneksi, properti tertentu dari cluster ini diperlukan, seperti pengidentifikasi cluster. Untuk informasi selengkapnya, lihat [Membuat Cluster](#).
2. Siapkan AD FS untuk mengontrol akses Amazon Redshift di Konsol Manajemen Microsoft:
 1. Pilih ADFS 2.0, lalu pilih Add Relying Party Trust. Pada halaman Add Relying Party Trust Wizard, pilih Mulai.
 2. Pada halaman Pilih Sumber Data, pilih Impor data tentang pihak yang mengandalkan yang dipublikasikan secara online atau di jaringan lokal.
 3. Untuk alamat metadata Federasi (nama host atau URL), masukkan. **https://signin.aws.amazon.com/saml-metadata.xml** File XHTML metadata adalah dokumen metadata SAMP standar yang menggambarkan sebagai pihak yang mengandalkan. AWS
 4. Pada halaman Tentukan Nama Tampilan, masukkan nilai untuk Nama tampilan.
 5. Pada halaman Pilih Aturan Otorisasi Penerbitan, pilih aturan otorisasi penerbitan untuk mengizinkan atau menolak semua pengguna mengakses pihak yang bergantung ini.
 6. Pada halaman Siap Tambah Kepercayaan, tinjau pengaturan Anda.
 7. Pada halaman Selesai, pilih Buka dialog Edit Aturan Klaim untuk kepercayaan pihak yang mengandalkan ini saat wizard ditutup.
 8. Pada menu konteks (klik kanan), pilih Mengandalkan Perwalian Partai.
 9. Untuk pihak yang Anda andalkan, buka menu konteks (klik kanan) dan pilih Edit Aturan Klaim. Pada halaman Edit Aturan Klaim, pilih Tambah Aturan.
 10. Untuk templat aturan Klaim, pilih Ubah Klaim Masuk, lalu pada Nameld halaman Edit Aturan —, lakukan hal berikut:
 - Untuk nama aturan Klaim, masukkan Nameld.
 - Untuk Nama klaim masuk, pilih Nama Akun Windows.
 - Untuk Nama klaim keluar, pilih ID Nama.
 - Untuk format ID nama keluar, pilih Persistent Identifier.
 - Pilih Lewati semua nilai klaim.

11 Pada halaman Edit Aturan Klaim, pilih Tambah Aturan. Pada halaman Pilih Templat Aturan, untuk templat aturan Klaim, pilih Kirim Atribut LDAP sebagai Klaim.

12 Pada halaman Configure Rule, lakukan hal berikut:

- Untuk nama aturan Klaim, masukkan RoleSessionName.
- Untuk toko Atribut, pilih Active Directory.
- Untuk Atribut LDAP, pilih Alamat Email.
- Untuk Jenis Klaim Keluar, pilih `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.

13 Pada halaman Edit Aturan Klaim, pilih Tambah Aturan. Pada halaman Pilih Templat Aturan, untuk templat aturan Klaim, pilih Kirim Klaim Menggunakan Aturan Kustom.

14 Pada halaman Aturan Edit — Dapatkan Grup IKLAN, untuk nama aturan Klaim, masukkan Dapatkan Grup IKLAN.

15 Untuk aturan Kustom, masukkan yang berikut ini.

```
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 Pada halaman Edit Aturan Klaim, pilih Tambah Aturan. Pada halaman Pilih Templat Aturan, untuk templat aturan Klaim, pilih Kirim Klaim Menggunakan Aturan Kustom.

17 Pada halaman Edit Aturan — Peran, untuk nama aturan Klaim, ketik Peran.

18 Untuk aturan Kustom, masukkan yang berikut ini.

```
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-"));
```

Perhatikan ARN dari penyedia SAMP dan peran yang harus diasumsikan. Dalam contoh ini, `arn:aws:iam:123456789012:saml-provider/ADFS` adalah ARN dari penyedia SAMP dan merupakan ARN `arn:aws:iam:123456789012:role/ADFS-` dari peran tersebut.

3. Pastikan Anda telah mengunduh `federationmetadata.xml` file tersebut. Periksa apakah isi dokumen tidak memiliki karakter yang tidak valid. Ini adalah file metadata yang Anda gunakan saat mengonfigurasi hubungan kepercayaan. AWS
4. Buat penyedia identitas SALL IAM di konsol IAM. Dokumen metadata. yang Anda berikan adalah file XHTML metadata federasi yang Anda simpan saat Anda menyiapkan Aplikasi Azure Enterprise. Untuk langkah-langkah mendetail, lihat [Membuat dan Mengelola Penyedia Identitas IAM \(Konsol\)](#) di Panduan Pengguna IAM.
5. Buat peran IAM untuk federasi SAFL 2.0 di konsol IAM. Untuk langkah-langkah mendetail, lihat [Membuat Peran untuk SAMP](#) di Panduan Pengguna IAM.
6. Buat kebijakan IAM yang dapat Anda lampirkan ke peran IAM yang Anda buat untuk federasi SAMP 2.0 di konsol IAM. Untuk langkah-langkah mendetail, lihat [Membuat Kebijakan IAM \(Konsol\)](#) di Panduan Pengguna IAM. Untuk contoh Azure AD, lihat [Menyiapkan otentikasi masuk tunggal JDBC atau ODBC dengan Microsoft Azure AD](#).

Untuk mengatur JDBC untuk otentikasi ke AD FS

- Konfigurasi klien database Anda untuk terhubung ke cluster Anda melalui JDBC menggunakan sistem masuk tunggal AD FS.

Anda dapat menggunakan klien apa pun yang menggunakan driver JDBC untuk terhubung menggunakan sistem masuk tunggal AD FS atau menggunakan bahasa seperti Java untuk terhubung menggunakan skrip. Untuk informasi instalasi dan konfigurasi, lihat [Mengkonfigurasi koneksi untuk driver JDBC versi 2.1 untuk Amazon Redshift](#).

Misalnya, Anda dapat menggunakan SqlWorkBench/J sebagai klien. Saat Anda mengkonfigurasi SQLWorkBench/J, URL database Anda menggunakan format berikut.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Jika Anda menggunakan SqlWorkBench/J sebagai klien, ambil langkah-langkah berikut:

- a. Mulai SQL Workbench/J. Di halaman Pilih Profil Koneksi, tambahkan Grup Profil, misalnya, **ADFS**
- b. Untuk Profil Koneksi, masukkan nama profil koneksi Anda, misalnya **ADFS**.
- c. Pilih Kelola Driver, dan pilih Amazon Redshift. Pilih ikon Open Folder di sebelah Library, lalu pilih file JDBC .jar yang sesuai.

- d. Pada halaman Pilih Profil Koneksi, tambahkan informasi ke profil koneksi sebagai berikut:
 - Untuk Pengguna, masukkan nama pengguna AD FS Anda. Ini adalah nama pengguna akun yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke cluster yang Anda coba autentikasi.
 - Untuk Kata Sandi, masukkan kata sandi AD FS Anda.
 - Untuk Driver, pilih Amazon Redshift (com.amazon.redshift.jdbc.driver).
 - Untuk URL, masukkan **`jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name`**.
- e. Pilih Extended Properties. Untuk plugin_name, masukkan **`com.amazon.redshift.plugin.AdfsCredentialsProvider`** Nilai ini menentukan driver untuk menggunakan sistem masuk tunggal AD FS sebagai metode otentikasi.

Untuk mengatur ODBC untuk otentikasi ke AD FS

- Konfigurasi klien database Anda untuk terhubung ke kluster Anda melalui ODBC menggunakan sistem masuk tunggal AD FS.

Amazon Redshift menyediakan driver ODBC untuk sistem operasi Linux, Windows, dan macOS. Sebelum Anda menginstal driver ODBC, tentukan apakah alat klien SQL Anda 32-bit atau 64-bit. Instal driver ODBC yang sesuai dengan persyaratan alat klien SQL Anda.

Juga instal dan konfigurasi driver Amazon Redshift ODBC terbaru untuk sistem operasi Anda sebagai berikut:


- Untuk Windows, lihat [Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#).
- Untuk macOS, lihat [Instal driver Amazon Redshift ODBC di macOS X](#)
- Untuk Linux, lihat [Instal driver Amazon Redshift ODBC di Linux](#).

Di Windows, di halaman Pengaturan DSN Driver Amazon Redshift ODBC, di bawah Pengaturan Koneksi, masukkan informasi berikut:

- Untuk Nama Sumber Data, masukkan **`your-DSN`**. Ini menentukan nama sumber data yang digunakan sebagai nama profil ODBC.

- Untuk jenis Auth, pilih Penyedia Identitas: SAMP. Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi menggunakan sistem masuk tunggal AD FS.
- Untuk ID Cluster, masukkan *your-cluster-identifier*.
- Untuk Wilayah, masukkan *your-cluster-region*.
- Untuk Database, masukkan *your-database-name*.
- Untuk Pengguna, masukkan *your-adfs-username*. Ini adalah nama pengguna untuk akun AD FS yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke kluster yang Anda coba autentikasi. Gunakan ini hanya untuk jenis Auth adalah Penyedia Identitas: SAMP.
- Untuk Kata Sandi, masukkan *your-adfs-password*. Gunakan ini hanya untuk jenis Auth adalah Penyedia Identitas: SAMP.

Di macOS dan Linux, edit `odbc.ini` file sebagai berikut:

 Note

Semua entri tidak peka huruf besar/kecil.

- Untuk clusterid, masukkan. *your-cluster-identifier* Ini adalah nama cluster Amazon Redshift yang dibuat.
- Untuk wilayah, masukkan *your-cluster-region*. Ini adalah AWS Wilayah cluster Amazon Redshift yang dibuat.
- Untuk database, masukkan *your-database-name*. Ini adalah nama database yang Anda coba akses di cluster Amazon Redshift.
- Untuk lokal, masukkan `en-us`. Ini adalah bahasa yang menampilkan pesan kesalahan.
- Untuk iam, masukkan `1`. Nilai ini menentukan driver untuk mengautentikasi menggunakan kredensial IAM.
- Untuk plugin_name, lakukan salah satu hal berikut:
 - Untuk proses masuk tunggal AD FS dengan konfigurasi MFA, masukkan. **BrowserSAML** Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi ke AD FS.
 - Untuk konfigurasi masuk tunggal AD FS, masukkan. **ADFS** Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi menggunakan sistem masuk tunggal Azure AD.

- Untuk uid, masukkan ***your-adfs-username***. Ini adalah nama pengguna akun Microsoft Azure yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke cluster yang Anda coba autentikasi. Gunakan ini hanya untuk plugin_name adalah ADFS.
- Untuk pwd, masukkan ***your-adfs-password***. Gunakan ini hanya untuk plugin_name adalah ADFS.

Di macOS dan Linux, edit juga pengaturan profil untuk menambahkan ekspor berikut.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Menyiapkan otentikasi masuk tunggal JDBC atau ODBC dengan Ping Identity

Anda dapat menggunakan Ping Identity sebagai penyedia identitas (iDP) untuk mengakses kluster Amazon Redshift Anda. Berikut ini, Anda dapat menemukan prosedur yang menjelaskan cara mengatur hubungan kepercayaan untuk tujuan ini menggunakan PingOne portal. Untuk informasi selengkapnya tentang mengonfigurasi AWS sebagai penyedia layanan untuk Identitas Ping, lihat [Mengonfigurasi IDP SAMP 2.0 Anda dengan Kepercayaan Pihak yang Mengandalkan dan Menambahkan Klaim](#) di Panduan Pengguna IAM.

Untuk mengatur Identitas Ping dan AWS akun Anda agar saling percaya

1. Buat atau gunakan kluster Amazon Redshift yang ada agar pengguna Identitas Ping Anda dapat terhubung. Untuk mengkonfigurasi koneksi, properti tertentu dari cluster ini diperlukan, seperti pengidentifikasi cluster. Untuk informasi selengkapnya, lihat [Membuat Cluster](#).
2. Tambahkan Amazon Redshift sebagai aplikasi SAMP baru di portal. PingOne Untuk langkah-langkah rinci, lihat [dokumentasi Ping Identity](#).
 1. Pergi ke Aplikasi Saya.
 2. Di bawah Add Application, pilih New SAMP Application.
 3. Untuk Nama Aplikasi, masukkan **Amazon Redshift**.
 4. Untuk Protocol Version, pilih SAMP v2.0.
 5. Untuk Kategori, pilih ***your-application-category***.

6. Untuk Assertion Consumer Service (ACS), ketik. ***your-redshift-local-host-url*** Ini adalah host dan port lokal yang dialihkan oleh pernyataan SAMP.
7. Untuk ID Entitas, masukkan `urn:amazon:webservices`.
8. Untuk Menandatangani, pilih Tanda Pernyataan.
9. Di bagian Pemetaan Atribut SSO, buat klaim seperti yang ditunjukkan pada tabel berikut.

Atribut aplikasi	Atribut jembatan identitas dari nilai literal
<code>https://aws.amazon.com/SAML/Attributes/Role</code>	<i>arn:aws:iam:: 123456789012: peran/ping, arn:aws:iam:: 123456789012: saml-provider/PingProvider</i>
<code>https://aws.amazon.com/SAML/Attributes/RoleSessionName</code>	Email
<code>https://redshift.amazon.com/SAML/Attributes/AutoCreate</code>	“benar”
<code>https://redshift.amazon.com/SAML/Attributes/DbUser</code>	Email
<code>https://redshift.amazon.com/SAML/Attributes/DbGroups</code>	Grup dalam atribut “DbGroups” berisi awalan @directory. Untuk menghapus ini, di jembatan Identity, masukkan memberOf. Di Function, pilih ExtractByRegularExpression. Dalam Ekspresi, masukkan <code>(.*) [\ @] (? :.*).</code>

3. Untuk Akses Grup, siapkan akses grup berikut, jika diperlukan:
 - `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. Tinjau pengaturan Anda dan buat perubahan, jika perlu.
5. Gunakan URL Initiate Single Sign-On (SSO) sebagai URL login untuk plugin Browser SAMP.

6. Buat penyedia identitas SALL IAM di konsol IAM. Dokumen metadata yang Anda berikan adalah file XML metadata federasi yang Anda simpan saat Anda mengatur Ping Identity. Untuk langkah-langkah mendetail, lihat [Membuat dan Mengelola Penyedia Identitas IAM \(Konsol\)](#) di Panduan Pengguna IAM.
7. Buat peran IAM untuk federasi SAFL 2.0 di konsol IAM. Untuk langkah-langkah mendetail, lihat [Membuat Peran untuk SAMP](#) di Panduan Pengguna IAM.
8. Buat kebijakan IAM yang dapat Anda lampirkan ke peran IAM yang Anda buat untuk federasi SAMP 2.0 di konsol IAM. Untuk langkah-langkah mendetail, lihat [Membuat Kebijakan IAM \(Konsol\)](#) di Panduan Pengguna IAM. Untuk contoh Azure AD, lihat [Menyiapkan otentikasi masuk tunggal JDBC atau ODBC dengan Microsoft Azure AD](#).

Untuk mengatur JDBC untuk otentikasi ke Ping Identity

- Konfigurasi klien database Anda untuk terhubung ke cluster Anda melalui JDBC menggunakan sistem masuk tunggal Ping Identity.

Anda dapat menggunakan klien apa pun yang menggunakan driver JDBC untuk terhubung menggunakan sistem masuk tunggal Ping Identity atau menggunakan bahasa seperti Java untuk terhubung menggunakan skrip. Untuk informasi instalasi dan konfigurasi, lihat [Mengkonfigurasi koneksi untuk driver JDBC versi 2.1 untuk Amazon Redshift](#).

Misalnya, Anda dapat menggunakan SqlWorkBench/J sebagai klien. Saat Anda mengkonfigurasi SQLWorkBench/J, URL database Anda menggunakan format berikut.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Jika Anda menggunakan SqlWorkBench/J sebagai klien, ambil langkah-langkah berikut:

- a. Mulai SQL Workbench/J. Di halaman Pilih Profil Koneksi, tambahkan Grup Profil, misalnya, **Ping**
- b. Untuk Profil Koneksi *your-connection-profile-name*, masukkan, misalnya **Ping**.
- c. Pilih Kelola Driver, dan pilih Amazon Redshift. Pilih ikon Open Folder di sebelah Library, lalu pilih file JDBC .jar yang sesuai.
- d. Pada halaman Pilih Profil Koneksi, tambahkan informasi ke profil koneksi sebagai berikut:

- Untuk Pengguna, masukkan nama PingOne pengguna Anda. Ini adalah nama pengguna PingOne akun yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke cluster yang Anda coba autentikasi.
 - Untuk Kata Sandi, masukkan PingOne kata sandi Anda.
 - Untuk Driver, pilih Amazon Redshift (`com.amazon.redshift.jdbc.driver`).
 - Untuk URL, masukkan **`jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name`**.
- e. Pilih Extended Properties dan lakukan salah satu hal berikut:
- Untuk `login_url`, masukkan **`your-ping-ss0-login-url`**. Nilai ini menentukan URL untuk menggunakan sistem masuk tunggal sebagai otentikasi untuk masuk.
 - Untuk Ping Identity, untuk `plugin_name`, masukkan **`com.amazon.redshift.plugin.PingCredentialsProvider`**. Nilai ini menentukan driver untuk menggunakan Ping Identity single sign-on sebagai metode otentikasi.
 - Untuk Ping Identity dengan sistem masuk tunggal, untuk `plugin_name`, masukkan **`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`**. Nilai ini menentukan driver untuk menggunakan Ping Identity PingOne dengan single sign-on sebagai metode otentikasi.

Untuk mengatur ODBC untuk otentikasi ke Ping Identity

- Konfigurasi klien database Anda untuk terhubung ke cluster Anda melalui ODBC menggunakan sistem masuk PingOne tunggal Ping Identity.

Amazon Redshift menyediakan driver ODBC untuk sistem operasi Linux, Windows, dan macOS. Sebelum Anda menginstal driver ODBC, tentukan apakah alat klien SQL Anda 32-bit atau 64-bit. Instal driver ODBC yang sesuai dengan persyaratan alat klien SQL Anda.

Juga instal dan konfigurasi driver Amazon Redshift ODBC terbaru untuk sistem operasi Anda sebagai berikut:

- Untuk Windows, lihat [Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#).
- Untuk macOS, lihat [Instal driver Amazon Redshift ODBC di macOS X](#)
- Untuk Linux, lihat [Instal driver Amazon Redshift ODBC di Linux](#).

Di Windows, di halaman Pengaturan DSN Driver Amazon Redshift ODBC, di bawah Pengaturan Koneksi, masukkan informasi berikut:

- Untuk Nama Sumber Data, masukkan ***your-DSN***. Ini menentukan nama sumber data yang digunakan sebagai nama profil ODBC.
- Untuk jenis Auth, lakukan salah satu hal berikut:
 - Untuk konfigurasi Ping Identity, pilih Identity Provider: Ping Federate. Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi menggunakan sistem masuk tunggal Ping Identity.
 - Untuk Ping Identity dengan konfigurasi masuk tunggal, pilih Penyedia Identitas: Browser SALL. Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi menggunakan Ping Identity dengan sistem masuk tunggal.
- Untuk ID Cluster, masukkan ***your-cluster-identifier***.
- Untuk Wilayah, masukkan ***your-cluster-region***.
- Untuk Database, masukkan ***your-database-name***.
- Untuk Pengguna, masukkan ***your-ping-username***. Ini adalah nama pengguna untuk PingOne akun yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke kluster yang Anda coba autentikasi. Gunakan ini hanya untuk jenis Auth adalah Penyedia Identitas: PingFederate.
- Untuk Kata Sandi, masukkan ***your-ping-password***. Gunakan ini hanya untuk jenis Auth adalah Penyedia Identitas: PingFederate.
- Untuk Listen Port, masukkan ***your-listen-port***. Ini adalah port yang didengarkan oleh server lokal. Defaultnya adalah 7890. Ini hanya berlaku untuk plugin Browser SAMP.
- Untuk Response Timeout, masukkan ***the-number-of-seconds***. Ini adalah jumlah detik untuk menunggu sebelum waktu habis ketika server iDP mengirim kembali respons. Jumlah minimum detik harus 10. Jika membuat koneksi membutuhkan waktu lebih lama dari ambang ini, maka koneksi dibatalkan. Ini hanya berlaku untuk plugin Browser SAMP.
- Untuk URL Login, masukkan ***your-login-url***. Ini hanya berlaku untuk plugin Browser SAMP.

Di macOS dan Linux, edit `odbc.ini` file sebagai berikut:

 Note

Semua entri tidak peka huruf besar/kecil.

- Untuk clusterid, masukkan. ***your-cluster-identifier*** Ini adalah nama cluster Amazon Redshift yang dibuat.
- Untuk wilayah, masukkan ***your-cluster-region***. Ini adalah AWS Wilayah cluster Amazon Redshift yang dibuat.
- Untuk database, masukkan ***your-database-name***. Ini adalah nama database yang Anda coba akses di cluster Amazon Redshift.
- Untuk lokal, masukkan ***en-us***. Ini adalah bahasa yang menampilkan pesan kesalahan.
- Untuk iam, masukkan ***1***. Nilai ini menentukan driver untuk mengautentikasi menggunakan kredensial IAM.
- Untuk plugin_name, lakukan salah satu hal berikut:
 - Untuk konfigurasi Ping Identity, masukkan ***BrowserSAML***. Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi ke Ping Identity.
 - Untuk Ping Identity dengan konfigurasi masuk tunggal, masukkan. ***Ping*** Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi menggunakan Ping Identity dengan sistem masuk tunggal.
- Untuk uid, masukkan ***your-ping-username***. Ini adalah nama pengguna akun Microsoft Azure yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke cluster yang Anda coba autentikasi. Gunakan ini hanya untuk plugin_name adalah Ping.
- Untuk pwd, masukkan. ***your-ping-password*** Gunakan ini hanya untuk plugin_name adalah Ping.
- Untuk login_url, masukkan. ***your-login-url*** Ini adalah Initiate single sign-on URL yang mengembalikan SAML Response. Ini hanya berlaku untuk plugin Browser SAMP.
- Untuk idp_response_timeout, masukkan. ***the-number-of-seconds*** Ini adalah periode waktu yang ditentukan dalam hitungan detik untuk menunggu respons dari PingOne Identity. Ini hanya berlaku untuk plugin Browser SAMP.
- Untuk listen_port, masukkan. ***your-listen-port*** Ini adalah port yang didengarkan oleh server lokal. Defaultnya adalah 7890. Ini hanya berlaku untuk plugin Browser SAMP.

Di macOS dan Linux, edit juga pengaturan profil untuk menambahkan ekspor berikut.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Menyiapkan otentikasi Single Sign-on JDBC atau ODBC dengan Okta

Anda dapat menggunakan Okta sebagai penyedia identitas (iDP) untuk mengakses kluster Amazon Redshift Anda. Berikut ini, Anda dapat menemukan prosedur yang menjelaskan cara mengatur hubungan kepercayaan untuk tujuan ini. Untuk informasi selengkapnya tentang mengonfigurasi AWS sebagai penyedia layanan untuk Okta, lihat [Mengonfigurasi IDP SAMP 2.0 Anda dengan Kepercayaan Pihak yang Mengandalkan dan Menambahkan](#) Klaim di Panduan Pengguna IAM.

Untuk mengatur Okta dan AWS akun Anda agar saling percaya

1. Buat atau gunakan kluster Amazon Redshift yang ada agar pengguna Okta dapat terhubung. Untuk mengkonfigurasi koneksi, properti tertentu dari cluster ini diperlukan, seperti pengidentifikasi cluster. Untuk informasi selengkapnya, lihat [Membuat Cluster](#).
2. Tambahkan Amazon Redshift sebagai aplikasi baru di portal Okta. Untuk langkah-langkah rinci, lihat [dokumentasi Okta](#).
 - Pilih Tambahkan Aplikasi.
 - Di bawah Tambahkan Aplikasi, pilih Buat Aplikasi Baru.
 - Pada halaman Create a New Add Application Integration, untuk Platform, pilih Web.
 - Untuk metode Sign on, pilih SAFL v2.0.
 - Pada halaman Pengaturan Umum, untuk nama Aplikasi, masukkan ***your-redshift-saml-sso-name***. Ini adalah nama aplikasi Anda.
 - Pada halaman Pengaturan SAMP, untuk Single sign on URL, masukkan ***your-redshift-local-host-url***. Ini adalah host dan port lokal yang dialihkan oleh pernyataan SAMP, misalnya. `http://localhost:7890/redshift/`
3. Gunakan tanda tunggal pada nilai URL sebagai URL Penerima dan URL Tujuan.
4. Untuk Menandatangani, pilih Tanda Pernyataan.

5. Untuk URI Audiens (SP Entity ID), masukkan **urn:amazon:webservices** klaim, seperti yang ditunjukkan pada tabel berikut.
6. Di bagian Pengaturan Lanjut, untuk ID Penerbit SAMP, masukkan ***your-Identity-Provider-Issuer-ID***, yang dapat Anda temukan di bagian Lihat Petunjuk Pengaturan.
7. Di bagian Pernyataan Atribut, buat klaim seperti yang ditunjukkan pada tabel berikut.

Nama klaim	Nilai
https://aws.amazon.com/SAML/Attributes/Role	<i>arn:aws:iam:: 123456789012: peran/Okta, arn:aws:iam:: 123456789012: saml-provider/Okta</i>
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.email
https://redshift.amazon.com/SAML/Attributes/AutoCreate	“benar”
https://redshift.amazon.com/SAML/Attributes/DbUser	user.email

8. Di bagian App Embed Link, temukan URL yang dapat Anda gunakan sebagai URL login untuk plugin Browser SAMP.
9. Buat penyedia identitas SALL IAM di konsol IAM. Dokumen metadata yang Anda berikan adalah file XML metadata federasi yang Anda simpan saat Anda mengatur Okta. Untuk langkah-langkah mendetail, lihat [Membuat dan Mengelola Penyedia Identitas IAM \(Konsol\)](#) di Panduan Pengguna IAM.
10. Buat peran IAM untuk federasi SAFL 2.0 di konsol IAM. Untuk langkah-langkah mendetail, lihat [Membuat Peran untuk SAMP](#) di Panduan Pengguna IAM.
11. Buat kebijakan IAM yang dapat Anda lampirkan ke peran IAM yang Anda buat untuk federasi SAMP 2.0 di konsol IAM. Untuk langkah-langkah mendetail, lihat [Membuat Kebijakan IAM \(Konsol\)](#) di Panduan Pengguna IAM. Untuk contoh Azure AD, lihat [Menyiapkan otentikasi masuk tunggal JDBC atau ODBC dengan Microsoft Azure AD](#).

Untuk mengatur JDBC untuk otentikasi ke Okta

- Konfigurasi klien database Anda untuk terhubung ke cluster Anda melalui JDBC menggunakan sistem masuk tunggal Okta.

Anda dapat menggunakan klien apa pun yang menggunakan driver JDBC untuk terhubung menggunakan sistem masuk tunggal Okta atau menggunakan bahasa seperti Java untuk terhubung menggunakan skrip. Untuk informasi instalasi dan konfigurasi, lihat [Mengkonfigurasi koneksi untuk driver JDBC versi 2.1 untuk Amazon Redshift](#).

Misalnya, Anda dapat menggunakan SqlWorkBench/J sebagai klien. Saat Anda mengkonfigurasi SQLWorkBench/J, URL database Anda menggunakan format berikut.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Jika Anda menggunakan SqlWorkBench/J sebagai klien, ambil langkah-langkah berikut:

- a. Mulai SQL Workbench/J. Di halaman Pilih Profil Koneksi, tambahkan Grup Profil, misalnya, **Okta**
- b. Untuk Profil Koneksi ***your-connection-profile-name***, masukkan, misalnya **Okta**.
- c. Pilih Kelola Driver, dan pilih Amazon Redshift. Pilih ikon Open Folder di sebelah Library, lalu pilih file JDBC .jar yang sesuai.
- d. Pada halaman Pilih Profil Koneksi, tambahkan informasi ke profil koneksi sebagai berikut:
 - Untuk Pengguna, masukkan nama pengguna Okta Anda. Ini adalah nama pengguna akun Okta yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke cluster yang Anda coba autentikasi.
 - Untuk Kata Sandi, masukkan kata sandi Okta Anda.
 - Untuk Driver, pilih Amazon Redshift (com.amazon.redshift.jdbc.driver).
 - Untuk URL, masukkan ***jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name***.
- e. Pilih Extended Properties dan lakukan salah satu hal berikut:
 - Untuk login_url, masukkan. ***your-okta-sso-login-url*** Nilai ini menentukan URL untuk menggunakan sistem masuk tunggal sebagai otentikasi untuk masuk ke Okta.

- Untuk sistem masuk tunggal Okta, untuk plugin_name, masukkan. **com.amazon.redshift.plugin.OktaCredentialsProvider** Nilai ini menentukan driver untuk menggunakan Okta single sign-on sebagai metode otentikasi.
- Untuk sistem masuk tunggal Okta dengan MFA, untuk plugin_name, masukkan. **com.amazon.redshift.plugin.BrowserSamlCredentialsProvider** Nilai ini menentukan driver untuk menggunakan Okta single sign-on dengan MFA sebagai metode otentikasi.

Untuk mengatur ODBC untuk otentikasi ke Okta

- Konfigurasi klien database Anda untuk terhubung ke cluster Anda melalui ODBC menggunakan sistem masuk tunggal Okta.

Amazon Redshift menyediakan driver ODBC untuk sistem operasi Linux, Windows, dan macOS. Sebelum Anda menginstal driver ODBC, tentukan apakah alat klien SQL Anda 32-bit atau 64-bit. Instal driver ODBC yang sesuai dengan persyaratan alat klien SQL Anda.

Juga instal dan konfigurasi driver Amazon Redshift ODBC terbaru untuk sistem operasi Anda sebagai berikut:


- Untuk Windows, lihat [Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows](#).
- Untuk macOS, lihat. [Instal driver Amazon Redshift ODBC di macOS X](#)
- Untuk Linux, lihat [Instal driver Amazon Redshift ODBC di Linux](#).

Di Windows, di halaman Pengaturan DSN Driver Amazon Redshift ODBC, di bawah Pengaturan Koneksi, masukkan informasi berikut:

- Untuk Nama Sumber Data, masukkan **your-DSN**. Ini menentukan nama sumber data yang digunakan sebagai nama profil ODBC.
- Untuk jenis Auth, lakukan salah satu hal berikut:
 - Untuk konfigurasi masuk tunggal Okta, pilih. **Identity Provider: Okta** Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi menggunakan Okta single sign-on.

- Untuk sistem masuk tunggal Okta dengan konfigurasi MFA, pilih. **Identity Provider: Browser SAML** Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi menggunakan Okta single sign-on dengan MFA.
- Untuk ID Cluster, masukkan *your-cluster-identifier*.
- Untuk Wilayah, masukkan *your-cluster-region*.
- Untuk Database, masukkan *your-database-name*.
- Untuk Pengguna, masukkan *your-okta-username*. Ini adalah nama pengguna untuk akun Okta yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke cluster yang Anda coba autentikasi. Gunakan ini hanya untuk jenis Auth adalah Penyedia Identitas: Okta.
- Untuk Kata Sandi, masukkan *your-okta-password*. Gunakan ini hanya untuk jenis Auth adalah Penyedia Identitas: Okta.

Di macOS dan Linux, edit `odbc.ini` file sebagai berikut:

 Note

Semua entri tidak peka huruf besar/kecil.

- Untuk clusterid, masukkan. *your-cluster-identifier* Ini adalah nama cluster Amazon Redshift yang dibuat.
- Untuk wilayah, masukkan *your-cluster-region*. Ini adalah AWS Wilayah cluster Amazon Redshift yang dibuat.
- Untuk database, masukkan *your-database-name*. Ini adalah nama database yang Anda coba akses di cluster Amazon Redshift.
- Untuk lokal, masukkan `en-us`. Ini adalah bahasa yang menampilkan pesan kesalahan.
- Untuk iam, masukkan `1`. Nilai ini menentukan driver untuk mengautentikasi menggunakan kredensial IAM.
- Untuk plugin_name, lakukan salah satu hal berikut:
 - Untuk sistem masuk tunggal Okta dengan konfigurasi MFA, masukkan. **BrowserSAML** Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi ke Okta single sign-on dengan MFA.
 - Untuk konfigurasi masuk tunggal Okta, masukkan. **Okta** Ini adalah metode otentikasi yang digunakan driver ODBC untuk mengautentikasi menggunakan Okta single sign-on.

- Untuk uid, masukkan ***your-okta-username***. Ini adalah nama pengguna akun Okta yang Anda gunakan untuk sistem masuk tunggal yang memiliki izin ke cluster yang Anda coba autentikasi. Gunakan ini hanya untuk plugin_name adalah Okta.
- Untuk pwd, masukkan. ***your-okta-password*** Gunakan ini hanya untuk plugin_name adalah Okta.
- Untuk login_url, masukkan. ***your-login-url*** Ini adalah Initiate single sign-on URL yang mengembalikan SAML Response. Ini hanya berlaku untuk plugin Browser SAMP.
- Untuk idp_response_timeout, masukkan. ***the-number-of-seconds*** Ini adalah periode waktu yang ditentukan dalam hitungan detik untuk menunggu respons dari PingOne. Ini hanya berlaku untuk plugin Browser SAMP.
- Untuk listen_port, masukkan. ***your-listen-port*** Ini adalah port yang didengarkan oleh server lokal. Defaultnya adalah 7890. Ini hanya berlaku untuk plugin Browser SAMP.

Di macOS dan Linux, edit juga pengaturan profil untuk menambahkan ekspor berikut.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Opsi JDBC dan ODBC untuk Membuat Kredensi Pengguna Database

Untuk menggunakan driver Amazon Redshift JDBC atau ODBC untuk membuat kredensial pengguna database, berikan nama pengguna database sebagai opsi JDBC atau ODBC. Secara opsional, Anda dapat meminta driver membuat pengguna database baru jika tidak ada, dan Anda dapat menentukan daftar grup pengguna database yang bergabung dengan pengguna saat login.

Jika Anda menggunakan penyedia identitas (iDP), bekerjalah dengan administrator iDP Anda untuk menentukan nilai yang benar untuk opsi ini. Administrator iDP Anda juga dapat mengonfigurasi iDP Anda untuk menyediakan opsi ini, dalam hal ini Anda tidak perlu menyediakannya sebagai opsi JDBC atau ODBC. Untuk informasi selengkapnya, lihat [Konfigurasi pernyataan SAMP untuk iDP Anda](#).

Note

Jika Anda menggunakan variabel kebijakan IAM `IAM${redshift:DbUser}`, seperti yang dijelaskan dalam [Kebijakan sumber daya untuk GetClusterCredentials](#) nilai `for DbUser` diganti dengan nilai yang diambil oleh konteks permintaan operasi API. Driver Amazon

Redshift menggunakan nilai untuk `DbUser` variabel yang disediakan oleh URL koneksi, bukan nilai yang diberikan sebagai atribut `SAMP`.

Untuk membantu mengamankan konfigurasi ini, kami sarankan Anda menggunakan kondisi dalam kebijakan IAM untuk memvalidasi `DbUser` nilai dengan `RoleSessionName` Anda dapat menemukan contoh cara menyetel kondisi menggunakan kebijakan IAM di [Contoh kebijakan untuk menggunakan `GetClusterCredentials`](#).

Tabel berikut mencantumkan opsi untuk membuat kredensi pengguna database.

Opsi	Deskripsi
<code>DbUser</code>	Nama pengguna database. Jika pengguna bernama <code>DbUser</code> ada dalam database, kredensi pengguna sementara memiliki izin yang sama dengan pengguna yang ada. Jika <code>DbUser</code> tidak ada dalam database dan <code>AutoCreate</code> benar, nama pengguna baru <code>DbUser</code> dibuat. Secara opsional, nonaktifkan kata sandi untuk pengguna yang ada. Untuk informasi selengkapnya, lihat ALTER_USER
<code>AutoCreate</code>	Tentukan <code>true</code> untuk membuat pengguna database dengan nama yang ditentukan untuk <code>DbUser</code> jika tidak ada. Default-nya adalah salah.
<code>DbGroups</code>	Daftar yang dibatasi koma dari nama-nama dari satu atau lebih kelompok database yang ada yang bergabung dengan pengguna database untuk sesi saat ini. Secara default, pengguna baru hanya ditambahkan ke PUBLIK.

Membuat kredensi database untuk identitas IAM menggunakan Amazon Redshift CLI atau API

Untuk menghasilkan kredensial pengguna database sementara secara terprogram, Amazon Redshift menyediakan [get-cluster-credentials](#) perintah untuk AWS Command Line Interface (AWS CLI) dan operasi API. [GetClusterCredentials](#) Atau Anda dapat mengonfigurasi klien SQL Anda dengan driver Amazon Redshift JDBC atau ODBC yang mengelola proses pemanggilan `GetClusterCredentials` operasi, mengambil kredensi pengguna database, dan membuat koneksi antara klien SQL Anda dan database Amazon Redshift Anda. Untuk informasi selengkapnya, lihat [Opsi JDBC dan ODBC untuk Membuat Kredensi Pengguna Database](#).

Note

Sebaiknya gunakan driver Amazon Redshift JDBC atau ODBC untuk menghasilkan kredensi pengguna database.

Di bagian ini, Anda dapat menemukan langkah-langkah untuk memanggil `GetClusterCredentials` operasi atau `get-cluster-credentials` perintah secara terprogram, mengambil kredensi pengguna database, dan terhubung ke database.

Untuk menghasilkan dan menggunakan kredensial basis data sementara

1. Membuat atau memodifikasi pengguna atau peran dengan izin yang diperlukan. Untuk informasi selengkapnya tentang izin IAM, lihat [Buat peran IAM dengan izin untuk memanggil `GetClusterCredentials`](#)
2. Sebagai pengguna atau peran yang Anda otorisasi pada langkah sebelumnya, jalankan perintah `get-cluster-credentials` CLI atau panggil operasi `GetClusterCredentials` API dan berikan nilai-nilai berikut:
 - Cluster identifier — Nama cluster yang berisi database.
 - Nama pengguna database — Nama pengguna database yang sudah ada atau baru.
 - Jika pengguna tidak ada dalam database dan `AutoCreate` benar, pengguna baru dibuat dengan `PASSWORD` dinonaktifkan.
 - Jika pengguna tidak ada, dan `AutoCreate` salah, permintaan gagal.
 - Untuk contoh ini, nama pengguna database adalah `temp_creds_user`.
 - `Autocreate` — (Opsional) Buat pengguna baru jika nama pengguna database tidak ada.
 - Nama basis data — (Opsional) Nama database yang diizinkan pengguna untuk masuk. Jika nama database tidak ditentukan, pengguna dapat masuk ke database cluster apa pun.
 - Grup basis data — (Opsional) Daftar grup pengguna database yang ada. Setelah login berhasil, pengguna database ditambahkan ke grup pengguna yang ditentukan. Jika tidak ada grup yang ditentukan, pengguna hanya memiliki izin `PUBLIK`. Nama grup pengguna harus cocok dengan ARN sumber daya `dbgroup` yang ditentukan dalam kebijakan IAM yang dilampirkan pada pengguna atau peran.
 - Waktu kedaluwarsa — (Opsional) Waktu, dalam hitungan detik, hingga kredensial sementara kedaluwarsa. Anda dapat menentukan nilai antara 900 detik (15 menit) dan 3600 detik (60 menit). Defaultnya adalah 900 detik.

3. Amazon Redshift memverifikasi bahwa pengguna memiliki izin untuk memanggil `GetClusterCredentials` operasi dengan sumber daya yang ditentukan.
4. Amazon Redshift mengembalikan kata sandi sementara dan nama pengguna database.

Contoh berikut menggunakan Amazon Redshift CLI untuk menghasilkan kredensial database sementara untuk pengguna yang sudah ada bernama `temp_creds_user`

```
aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user temp_creds_user --db-name exampledb --duration-seconds 3600
```

Hasilnya adalah sebagai berikut.

```
{
  "DbUser": "IAM:temp_creds_user",
  "Expiration": "2016-12-08T21:12:53Z",
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM80yxpDHwXVPyJYBDm/
ggX2Eeaq6P3DgTzgPg=="
}
```

Contoh berikut menggunakan Amazon Redshift CLI dengan `autocreate` untuk menghasilkan kredensial database sementara untuk pengguna baru dan menambahkan pengguna ke grup `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
```

Hasilnya adalah sebagai berikut.

```
{
  "DbUser": "IAMA:temp_creds_user:example_group",
  "Expiration": "2016-12-08T21:12:53Z",
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM80yxpDHwXVPyJYBDm/
ggX2Eeaq6P3DgTzgPg=="
}
```

5. Buat koneksi otentikasi Secure Socket Layer (SSL) dengan cluster Amazon Redshift dan kirim permintaan login dengan nama pengguna dan kata sandi dari respons.

GetClusterCredentials Sertakan IAMA: awalan IAM: atau dengan nama pengguna, misalnya IAM:temp_creds_user atauIAMA:temp_creds_user.

Important

Konfigurasi klien SQL Anda untuk memerlukan SSL. Jika tidak, jika klien SQL Anda secara otomatis mencoba terhubung dengan SSL, itu dapat kembali ke non-SSL jika ada jenis kegagalan. Dalam hal ini, upaya koneksi pertama mungkin gagal karena kredensialnya kedaluwarsa atau tidak valid, maka upaya koneksi kedua gagal karena koneksi tidak SSL. Jika itu terjadi, pesan kesalahan pertama mungkin terlewatkan. Untuk informasi selengkapnya tentang menghubungkan ke kluster menggunakan SSL, lihat [Mengkonfigurasi opsi keamanan untuk koneksi](#).

6. Jika koneksi tidak menggunakan SSL, upaya koneksi gagal.
7. Cluster mengirimkan authentication permintaan ke klien SQL.
8. Klien SQL kemudian mengirimkan kata sandi sementara ke cluster.
9. Jika kata sandi valid dan belum kedaluwarsa, cluster menyelesaikan koneksi.

Mengotorisasi Amazon Redshift untuk mengakses layanan AWS lain atas nama Anda

Beberapa fitur Amazon Redshift memerlukan Amazon Redshift untuk mengakses layanan AWS lain atas nama Anda. Misalnya, perintah [COPY](#) dan [UNLOAD](#) dapat memuat atau membongkar data ke cluster Amazon Redshift menggunakan bucket Amazon S3. Perintah [CREATE EXTERNAL FUNCTION](#) dapat memanggil fungsi AWS Lambda menggunakan fungsi yang ditentukan pengguna Lambda skalar (UDF). Amazon Redshift Spectrum dapat menggunakan katalog data di Amazon AWS Glue Athena atau. Agar kluster Amazon Redshift bertindak atas nama Anda, Anda memberikan kredensi keamanan ke kluster Anda. Metode yang lebih disukai untuk menyediakan kredensial keamanan adalah dengan menentukan peran AWS Identity and Access Management (IAM). Untuk COPY dan UNLOAD, Anda dapat memberikan kredensi sementara.

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. <ul style="list-style-type: none"> • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat otentikasi Pusat Identitas IAM di Panduan Referensi AWS SDK dan Alat.
IAM	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk dalam Menggunakan kredensial sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredensial jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. <ul style="list-style-type: none"> • Untuk mengetahui AWS CLI, lihat Mengotentikasi menggunakan kredensial pengguna IAM di Panduan Pengguna. AWS Command Line Interface

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
		<ul style="list-style-type: none"> • Untuk AWS SDK dan alat bantu, lihat Mengautentikasi menggunakan kredensial jangka panjang di Panduan Referensi AWS SDK dan Alat. • Untuk AWS API, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Berikut ini, cari tahu cara membuat peran IAM dengan izin yang sesuai untuk mengakses layanan lain AWS . Anda juga perlu mengaitkan peran dengan klaster Anda dan menentukan Nama Sumber Daya Amazon (ARN) peran saat menjalankan perintah Amazon Redshift. Untuk informasi selengkapnya, lihat [Mengotorisasi operasi COPY, UNLOAD, CREATE EXTERNAL FUNCTION, dan CREATE EXTERNAL SCHEMA menggunakan peran IAM](#).

Selain itu, pengguna super dapat memberikan hak istimewa ASSUMEROLE kepada pengguna dan grup tertentu untuk menyediakan akses ke peran untuk operasi COPY dan UNLOAD. Untuk selengkapnya, lihat [GRANT](#) di Panduan Pengembang Database Amazon Redshift.

Membuat peran IAM untuk memungkinkan klaster Amazon Redshift Anda mengakses layanan AWS

Untuk membuat peran IAM untuk mengizinkan klaster Amazon Redshift Anda berkomunikasi dengan layanan AWS lain atas nama Anda, lakukan langkah-langkah berikut. Nilai yang digunakan di bagian ini adalah contoh, Anda dapat memilih nilai berdasarkan kebutuhan Anda.

Untuk membuat peran IAM untuk memungkinkan Amazon Redshift mengakses layanan AWS

1. Buka [konsol IAM](#).
2. Di panel navigasi, pilih Peran.
3. Pilih Buat peran.

4. Pilih AWS layanan, lalu pilih Redshift.
5. Di bawah Pilih kasus penggunaan Anda, pilih Redshift - Customizable dan kemudian pilih Next: Permissions. Halaman kebijakan izin lampirkan akan muncul.
6. Untuk akses ke Amazon S3 menggunakan COPY, sebagai contoh, Anda dapat menggunakan **AmazonS3ReadOnlyAccess** dan menambahkan. Untuk akses ke Amazon S3 menggunakan COPY atau UNLOAD, sebaiknya Anda membuat kebijakan terkelola yang membatasi akses ke bucket dan awalan yang diinginkan. Untuk operasi baca dan tulis, kami sarankan untuk menerapkan hak istimewa paling sedikit dan membatasi hanya bucket Amazon S3 dan awalan kunci yang diperlukan Amazon Redshift.


Untuk akses untuk memanggil fungsi Lambda untuk perintah CREATE EXTERNAL FUNCTION, tambahkan. **AWSLambdaRole**

Untuk Redshift Spectrum, selain akses Amazon S3, tambahkan atau.

AWSGlueConsoleFullAccess AmazonAthenaFullAccess

Pilih Berikutnya: Penandaan.

7. Halaman Tambahkan penandaan akan muncul. Anda dapat menambahkan tanda secara opsional. Pilih Berikutnya: Tinjau.
8. Untuk nama Peran, ketikkan nama untuk peran Anda, misalnya **RedshiftCopyUnload**. Pilih Buat peran.
9. Peran baru tersedia untuk semua pengguna di cluster yang menggunakan peran tersebut. Untuk membatasi akses hanya ke pengguna tertentu pada cluster tertentu, atau ke cluster di wilayah tertentu, edit hubungan kepercayaan untuk peran tersebut. Untuk informasi selengkapnya, lihat [Membatasi akses ke peran IAM](#).
10. Kaitkan peran dengan cluster Anda. Anda dapat mengaitkan peran IAM dengan klaster saat membuat klaster, atau menambahkan peran tersebut ke klaster yang ada. Untuk informasi selengkapnya, lihat [Mengaitkan peran IAM dengan cluster](#).

 Note

Untuk membatasi akses ke data tertentu, gunakan peran IAM yang memberikan hak istimewa paling sedikit yang diperlukan.

Membatasi akses ke peran IAM

Secara default, peran IAM yang tersedia untuk kluster Amazon Redshift tersedia untuk semua pengguna di cluster tersebut. Anda dapat memilih untuk membatasi peran IAM ke pengguna database Amazon Redshift tertentu pada kluster tertentu atau ke wilayah tertentu.

Untuk mengizinkan hanya pengguna database tertentu untuk menggunakan peran IAM, lakukan langkah-langkah berikut.

Untuk mengidentifikasi pengguna database tertentu dengan akses ke peran IAM

1. Identifikasi Nama Sumber Daya Amazon (ARN) untuk pengguna database di kluster Amazon Redshift Anda. ARN untuk pengguna database dalam format:
`arn:aws:redshift:region:account-id:dbuser:cluster-name/user-name`

Untuk Amazon Redshift Tanpa Server gunakan format ARN berikut.

`arn:aws:redshift:region:account-id:dbuser:workgroup-name/user-name`

2. Buka [konsol IAM](#).
3. Di panel navigasi, pilih Peran.
4. Pilih peran IAM yang ingin Anda batasi untuk pengguna database Amazon Redshift tertentu.
5. Pilih tab Trust Relationships, lalu pilih Edit Trust Relationship. Peran IAM baru yang memungkinkan Amazon Redshift mengakses layanan AWS lain atas nama Anda memiliki hubungan kepercayaan sebagai berikut:

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

6. Tambahkan kondisi ke bagian `sts:AssumeRole` tindakan dari hubungan kepercayaan yang membatasi `sts:ExternalId` bidang ke nilai yang Anda tentukan. Sertakan ARN untuk setiap

pengguna database yang ingin Anda berikan akses ke peran tersebut. ID eksternal dapat berupa string unik apa pun.

Misalnya, hubungan kepercayaan berikut menetapkan bahwa hanya pengguna database `user1` dan `user2` di kluster `my-cluster` di wilayah yang `us-west-2` memiliki izin untuk menggunakan peran IAM ini.

```
{
  "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. Pilih Perbarui Kebijakan Kepercayaan.

Membatasi peran IAM ke Wilayah AWS

Anda dapat membatasi peran IAM agar hanya dapat diakses di Wilayah tertentu AWS . Secara default, peran IAM untuk Amazon Redshift tidak dibatasi untuk wilayah tunggal mana pun.

Untuk membatasi penggunaan peran IAM berdasarkan wilayah, lakukan langkah-langkah berikut.

Untuk mengidentifikasi wilayah yang diizinkan untuk peran IAM

1. Buka [konsol IAM](https://console.aws.amazon.com/) di <https://console.aws.amazon.com/>.
2. Di panel navigasi, pilih Peran.
3. Pilih peran yang ingin Anda ubah dengan wilayah tertentu.

- Pilih tab Trust Relationships dan kemudian pilih Edit Trust Relationship. Peran IAM baru yang memungkinkan Amazon Redshift mengakses layanan AWS lain atas nama Anda memiliki hubungan kepercayaan sebagai berikut:

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

- Ubah Service daftar untuk daftar wilayah tertentu yang ingin Anda izinkan penggunaan peran tersebut. Principal Setiap wilayah dalam Service daftar harus dalam format berikut: `redshift.region.amazonaws.com`.

Misalnya, hubungan kepercayaan yang diedit berikut mengizinkan penggunaan peran IAM di `us-east-1` dan `us-west-2` wilayah saja.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.us-east-1.amazonaws.com",
          "redshift.us-west-2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- Pilih Perbarui Kebijakan Kepercayaan

Merantai peran IAM di Amazon Redshift

Saat Anda melampirkan peran ke kluster, kluster Anda dapat mengambil peran tersebut untuk mengakses Amazon S3, Amazon Athena AWS Glue, AWS Lambda dan atas nama Anda. Jika peran yang dilampirkan ke kluster Anda tidak memiliki akses ke sumber daya yang diperlukan, Anda dapat merantai peran lain, mungkin milik akun lain. Cluster Anda kemudian sementara mengasumsikan peran berantai untuk mengakses data. Anda juga dapat memberikan akses lintas akun dengan merantai peran. Setiap peran dalam rantai mengasumsikan peran berikutnya dalam rantai, sampai cluster mengambil peran di akhir rantai. Jumlah maksimum peran IAM yang dapat Anda kaitkan tunduk pada kuota. Untuk informasi selengkapnya, lihat kuota “Peran IAM cluster untuk Amazon Redshift untuk mengakses layanan AWS lain” di [Kuota untuk objek Amazon Redshift](#)

Misalnya, Perusahaan A ingin mengakses data dalam bucket Amazon S3 milik Perusahaan B. Perusahaan A menciptakan peran AWS layanan untuk Amazon Redshift RoleA bernama dan menempelkannya ke kluster mereka. Perusahaan B membuat peran bernama RoleB yang diizinkan untuk mengakses data di bucket Perusahaan B. Untuk mengakses data dalam bucket B Perusahaan, Perusahaan A menjalankan perintah COPY menggunakan iam_role parameter yang berantai RoleA dan RoleB. Selama operasi COPY, untuk RoleA sementara mengasumsikan RoleB untuk mengakses bucket Amazon S3.

Untuk peran rantai, Anda membangun hubungan kepercayaan antara peran. Peran yang mengasumsikan peran lain (misalnya, RoleA) harus memiliki kebijakan izin yang memungkinkannya mengambil peran berantai berikutnya (misalnya, RoleB). Pada gilirannya, peran yang meneruskan izin (RoleB) harus memiliki kebijakan kepercayaan yang memungkinkannya meneruskan izinnya ke peran berantai sebelumnya (RoleA). Untuk informasi selengkapnya, lihat [Menggunakan peran IAM](#) di Panduan Pengguna IAM.

Peran pertama dalam rantai harus menjadi peran yang melekat pada cluster. Peran pertama, dan setiap peran berikutnya yang mengambil peran berikutnya dalam rantai, harus memiliki kebijakan yang mencakup pernyataan tertentu. Pernyataan ini memiliki Allow efek pada sts:AssumeRole tindakan dan Nama Sumber Daya Amazon (ARN) dari peran berikutnya dalam suatu Resource elemen. Dalam contoh kami, RoleA memiliki kebijakan izin berikut yang memungkinkannya untuk berasumsi RoleB, dimiliki oleh AWS akun 210987654321.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1487639602000",
```

```

        "Effect": "Allow",
        "Action": [
            "sts:AssumeRole"
        ],
        "Resource": "arn:aws:iam::210987654321:role/RoleB"
    }
]
}

```

Peran yang beralih ke peran lain harus membangun hubungan kepercayaan dengan peran yang mengambil peran atau dengan AWS akun yang memiliki peran tersebut. Dalam contoh kami, RoleB memiliki kebijakan kepercayaan berikut untuk membangun hubungan kepercayaan dengan RoleA.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::role/RoleA"
      }
    }
  ]
}

```

Kebijakan kepercayaan berikut menetapkan hubungan kepercayaan dengan pemilik RoleA, AWS akun123456789012.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}

```

Note

Untuk membatasi otorisasi rantai peran untuk pengguna tertentu, tentukan kondisi. Untuk informasi selengkapnya, lihat [Membatasi akses ke peran IAM](#).

Saat menjalankan perintah UNLOAD, COPY, CREATE EXTERNAL FUNCTION, atau CREATE EXTERNAL SCHEMA, Anda merantai peran dengan menyertakan daftar ARN peran yang dipisahkan koma dalam parameter. `iam_role` Berikut ini menunjukkan sintaks untuk peran rantai dalam parameter. `iam_role`

```
unload ('select * from venue limit 10')
to 's3://acmedata/redshift/venue_pipe_'
IAM_ROLE 'arn:aws:iam::<aws-account-id-1>:role/<role-name-1>[,arn:aws:iam::<aws-
account-id-2>:role/<role-name-2>][,...]';
```

Note

Seluruh rantai peran tertutup dalam tanda kutip tunggal dan tidak boleh berisi spasi.

Dalam contoh berikut, `RoleA` dilampirkan ke cluster milik AWS akun123456789012. `RoleB`, yang termasuk dalam akun210987654321, memiliki izin untuk mengakses bucket bernama `s3://companyb/redshift/`. Contoh rantai berikut `RoleA` dan `RoleB` untuk MEMBONGKAR data ke bucket `s3://companyb/redshift/`.

```
unload ('select * from venue limit 10')
to 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

Contoh berikut menggunakan perintah COPY untuk memuat data yang diturunkan dalam contoh sebelumnya.

```
copy venue
from 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

Dalam contoh berikut, CREATE EXTERNAL SCHEMA menggunakan peran berantai untuk mengambil peran. `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';
```

Dalam contoh berikut, CREATE EXTERNAL FUNCTION menggunakan peran berantai untuk mengambil peranRoleB.

```
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';
```

Informasi tambahan

Untuk informasi lebih lanjut, lihat juga [Mengotorisasi operasi COPY, UNLOAD, CREATE EXTERNAL FUNCTION, dan CREATE EXTERNAL SCHEMA menggunakan peran IAM](#).

Mengotorisasi operasi COPY, UNLOAD, CREATE EXTERNAL FUNCTION, dan CREATE EXTERNAL SCHEMA menggunakan peran IAM

Anda dapat menggunakan perintah [COPY](#) untuk memuat (atau mengimpor) data ke Amazon Redshift dan perintah [UNLOAD](#) untuk membongkar (atau mengeksport) data dari Amazon Redshift. Anda dapat menggunakan perintah CREATE EXTERNAL FUNCTION untuk membuat fungsi yang ditentukan pengguna yang memanggil fungsi dari AWS Lambda

Saat menggunakan Amazon Redshift Spectrum, Anda menggunakan perintah [CREATE EXTERNAL SCHEMA](#) untuk menentukan lokasi bucket Amazon S3 yang berisi data Anda. Saat menjalankan perintah COPY, UNLOAD, atau CREATE EXTERNAL SCHEMA, Anda memberikan kredensi keamanan. Kredensi ini mengizinkan kluster Amazon Redshift Anda untuk membaca atau menulis data ke dan dari tujuan target Anda, seperti bucket Amazon S3.

Saat menjalankan CREATE EXTERNAL FUNCTION, Anda memberikan kredensi keamanan menggunakan parameter peran IAM. Kredensi ini mengizinkan kluster Amazon Redshift Anda untuk menjalankan fungsi Lambda. AWS Lambda Metode yang lebih disukai untuk menyediakan kredensial keamanan adalah dengan menentukan peran AWS Identity and Access Management (IAM). Untuk COPY dan UNLOAD, Anda dapat memberikan kredensi sementara. Untuk informasi tentang membuat peran IAM, lihat [Mengotorisasi Amazon Redshift untuk mengakses layanan AWS lain atas nama Anda](#).

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. <ul style="list-style-type: none"> • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat otentikasi Pusat Identitas IAM di Panduan Referensi AWS SDK dan Alat.
IAM	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk dalam Menggunakan kredensial sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredensial jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. <ul style="list-style-type: none"> • Untuk mengetahui AWS CLI, lihat Mengotentikasi

Pegguna mana yang membutuhkan akses programatis?	Untuk	Oleh
		<p>menggunakan kredensial pengguna IAM di Panduan Pengguna.AWS Command Line Interface</p> <ul style="list-style-type: none"> • Untuk AWS SDK dan alat bantu, lihat Mengautentikasi menggunakan kredensial jangka panjang di Panduan Referensi AWS SDK dan Alat. • Untuk AWS API, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Langkah-langkah untuk menggunakan peran IAM adalah sebagai berikut:

- Buat peran IAM untuk digunakan dengan kluster Amazon Redshift Anda.
- Kaitkan peran IAM dengan cluster.
- Sertakan ARN peran IAM saat Anda memanggil perintah COPY, UNLOAD, CREATE EXTERNAL SCHEMA, atau CREATE EXTERNAL FUNCTION.

Dalam topik ini, Anda mempelajari cara mengaitkan peran IAM dengan cluster Amazon Redshift.

Mengaitkan peran IAM dengan cluster

Setelah Anda membuat peran IAM yang mengizinkan Amazon Redshift untuk mengakses layanan AWS lain untuk Anda, Anda harus mengaitkan peran tersebut dengan kluster Amazon Redshift. Anda harus melakukan ini sebelum Anda dapat menggunakan peran untuk memuat atau membongkar data.

Izin diperlukan untuk mengaitkan peran IAM dengan kluster

Untuk mengaitkan peran IAM dengan kluster, pengguna harus memiliki `iam:PassRole` izin untuk peran IAM tersebut. Izin ini memungkinkan administrator untuk membatasi peran IAM mana yang dapat dikaitkan pengguna dengan kluster Amazon Redshift. Sebagai praktik terbaik, sebaiknya lampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).

Contoh berikut menunjukkan kebijakan IAM yang dapat dilampirkan ke pengguna yang memungkinkan pengguna untuk mengambil tindakan ini:

- Dapatkan detail untuk semua cluster Amazon Redshift yang dimiliki oleh akun pengguna tersebut.
- Kaitkan salah satu dari tiga peran IAM dengan salah satu dari dua cluster Amazon Redshift.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "redshift:DescribeClusters",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "redshift:ModifyClusterIamRoles",
        "redshift:CreateCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-cluster",
        "arn:aws:redshift:us-east-1:123456789012:cluster:my-second-redshift-
cluster"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::123456789012:role/MyRedshiftRole",
        "arn:aws:iam::123456789012:role/SecondRedshiftRole",
        "arn:aws:iam::123456789012:role/ThirdRedshiftRole"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

Setelah pengguna memiliki izin yang sesuai, pengguna tersebut dapat mengaitkan peran IAM dengan kluster Amazon Redshift. Peran IAM kemudian siap digunakan dengan perintah COPY atau UNLOAD atau perintah Amazon Redshift lainnya.

Untuk informasi selengkapnya tentang kebijakan IAM, lihat [Ringkasan kebijakan IAM](#) di Panduan Pengguna IAM.

Mengelola asosiasi peran IAM dengan cluster

Anda dapat mengaitkan peran IAM dengan kluster Amazon Redshift saat membuat kluster. Atau Anda dapat memodifikasi kluster yang ada dan menambahkan atau menghapus satu atau beberapa asosiasi peran IAM.

Ketahui hal-hal berikut:

- Jumlah maksimum peran IAM yang dapat Anda kaitkan tunduk pada kuota.
- Peran IAM dapat dikaitkan dengan beberapa cluster Amazon Redshift.
- Peran IAM dapat dikaitkan dengan cluster Amazon Redshift hanya jika peran IAM dan cluster dimiliki oleh akun yang sama. AWS

Menggunakan konsol untuk mengelola asosiasi peran IAM

Anda dapat mengelola asosiasi peran IAM untuk kluster dengan konsol menggunakan prosedur berikut.

Untuk mengelola asosiasi peran IAM

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, lalu pilih cluster yang ingin Anda perbarui.
3. Untuk Tindakan, pilih Kelola peran IAM untuk menampilkan daftar peran IAM saat ini yang terkait dengan cluster.
4. Pada halaman Kelola peran IAM, pilih peran IAM yang tersedia untuk ditambahkan, lalu pilih Tambahkan peran IAM.

5. Pilih Selesai untuk menyimpan perubahan Anda.

Menggunakan AWS CLI untuk mengelola asosiasi peran IAM

Anda dapat mengelola asosiasi peran IAM untuk kluster AWS CLI dengan menggunakan pendekatan berikut.

Mengaitkan peran IAM dengan cluster menggunakan AWS CLI

Untuk mengaitkan peran IAM dengan cluster saat cluster dibuat, tentukan Amazon Resource Name (ARN) peran IAM untuk parameter `--iam-role-arns` perintah `create-cluster`. Jumlah maksimum peran IAM yang dapat Anda tambahkan saat memanggil `create-cluster` perintah tunduk pada kuota.

Mengaitkan dan memisahkan peran IAM dengan kluster Amazon Redshift adalah proses asinkron. Anda bisa mendapatkan status semua asosiasi kluster peran IAM dengan memanggil `describe-clusters` perintah.

Contoh berikut mengaitkan dua peran IAM dengan cluster yang baru dibuat bernama `my-redshift-cluster`

```
aws redshift create-cluster \  
  --cluster-identifier "my-redshift-cluster" \  
  --node-type "ra3.4xlarge" \  
  --number-of-nodes 16 \  
  --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftCopyUnload" \  
                  "arn:aws:iam::123456789012:role/SecondRedshiftRole"
```

Untuk mengaitkan peran IAM dengan kluster Amazon Redshift yang ada, tentukan Nama Sumber Daya Amazon (ARN) peran IAM untuk `--add-iam-roles` parameter perintah `modify-cluster-iam-roles`. Jumlah maksimum peran IAM yang dapat Anda tambahkan saat memanggil `modify-cluster-iam-roles` perintah tunduk pada kuota.

Contoh berikut mengaitkan peran IAM dengan cluster yang ada bernama `my-redshift-cluster`

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier "my-redshift-cluster" \  
  --add-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Memutuskan peran IAM dari cluster menggunakan AWS CLI

Untuk memisahkan peran IAM dari cluster, tentukan ARN dari peran IAM untuk parameter perintah. `--remove-iam-roles modify-cluster-iam-roles modify-cluster-iam-roles` Jumlah maksimum peran IAM yang dapat Anda hapus saat memanggil `modify-cluster-iam-roles` perintah tunduk pada kuota.

Contoh berikut menghapus asosiasi untuk peran IAM untuk 123456789012 AWS akun dari cluster bernama `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \
  --cluster-identifier "my-redshift-cluster" \
  --remove-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Membuat daftar asosiasi peran IAM untuk klaster menggunakan AWS CLI

Untuk mencantumkan semua peran IAM yang terkait dengan cluster Amazon Redshift, dan status asosiasi peran IAM, panggil perintah. `describe-clusters` ARN untuk setiap peran IAM yang terkait dengan cluster dikembalikan dalam `IamRoles` daftar seperti yang ditunjukkan pada contoh output berikut.

Peran yang telah dikaitkan dengan cluster menunjukkan status `in-sync`. Peran yang sedang dalam proses dikaitkan dengan cluster menunjukkan status `adding`. Peran yang sedang dipisah dari cluster menunjukkan status `removing`.

```
{
  "Clusters": [
    {
      "ClusterIdentifier": "my-redshift-cluster",
      "NodeType": "ra3.4xlarge",
      "NumberOfNodes": 16,
      "IamRoles": [
        {
          "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",
          "IamRoleApplyStatus": "in-sync"
        },
        {
          "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
          "IamRoleApplyStatus": "in-sync"
        }
      ]
    }
  ],
}
```

```
    ...
  },
  {
    "ClusterIdentifier": "my-second-redshift-cluster",
    "NodeType": "ra3.4xlarge",
    "NumberOfNodes": 10,
    "IamRoles": [
      {
        "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",
        "IamRoleApplyStatus": "in-sync"
      },
      {
        "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
        "IamRoleApplyStatus": "in-sync"
      },
      {
        "IamRoleArn": "arn:aws:iam::123456789012:role/ThirdRedshiftRole",
        "IamRoleApplyStatus": "in-sync"
      }
    ],
    ...
  }
]
```

Untuk informasi selengkapnya tentang penggunaan AWS CLI, lihat [Panduan AWS CLI Pengguna](#).

Membuat peran IAM sebagai default untuk Amazon Redshift

Saat Anda membuat peran IAM melalui konsol Redshift, Amazon Redshift secara terprogram membuat peran dalam peran Akun AWS Anda dan secara otomatis melampirkan kebijakan terkelola yang ada padanya. AWS Pendekatan ini berarti Anda dapat tetap berada di dalam konsol Redshift dan tidak perlu beralih ke konsol IAM untuk pembuatan peran. Untuk kontrol izin yang lebih terperinci untuk peran IAM yang ada yang dibuat di konsol Amazon Redshift, Anda dapat melampirkan kebijakan terkelola yang disesuaikan ke peran IAM.

Ikhtisar peran IAM yang dibuat di konsol

Saat Anda menggunakan konsol Amazon Redshift untuk membuat peran IAM, Amazon Redshift melacak semua peran IAM yang dibuat melalui konsol. Amazon Redshift memilih sebelumnya peran IAM default terbaru untuk membuat semua cluster baru dan memulihkan cluster dari snapshot.

Anda dapat membuat peran IAM melalui konsol yang memiliki kebijakan dengan izin untuk menjalankan perintah SQL. Perintah-perintah ini termasuk COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL, atau CREATE LIBRARY. Secara opsional, Anda bisa mendapatkan kontrol yang lebih terperinci atas akses pengguna ke AWS sumber daya Anda dengan membuat dan melampirkan kebijakan khusus ke peran IAM.

Saat Anda membuat peran IAM dan mengaturnya sebagai default untuk kluster menggunakan konsol, Anda tidak perlu memberikan Nama Sumber Daya Amazon (ARN) peran IAM untuk melakukan autentikasi dan otorisasi.

Menggunakan peran IAM yang dibuat di konsol

Peran IAM yang Anda buat melalui konsol untuk kluster Anda memiliki kebijakan `AmazonRedshiftAllCommandsFullAccess` terkelola yang dilampirkan secara otomatis. Peran IAM ini memungkinkan Amazon Redshift untuk menyalin, membongkar, menanyakan, dan menganalisis data AWS untuk sumber daya di akun IAM Anda. Kebijakan terkelola menyediakan akses ke operasi [COPY](#), [UNLOAD](#), [CREATE EXTERNAL FUNCTION](#), [CREATE EXTERNAL SCHEMA](#), [CREATE MODEL](#), dan [CREATE LIBRARY](#). Kebijakan ini juga memberikan izin untuk menjalankan pernyataan SELECT untuk AWS layanan terkait, seperti Amazon S3, Amazon Logs, CloudWatch SageMaker Amazon, dan AWS Glue

Perintah CREATE EXTERNAL FUNCTION, CREATE EXTERNAL SCHEMA, CREATE MODEL, dan CREATE LIBRARY memiliki default kata kunci. Untuk kata kunci ini untuk perintah ini, Amazon Redshift menggunakan peran IAM yang ditetapkan sebagai default dan terkait dengan cluster saat perintah berjalan. Anda dapat menjalankan perintah [DEFAULT_IAM_ROLE untuk memeriksa peran IAM](#) default saat ini yang dilampirkan ke cluster.

Untuk mengontrol hak akses peran IAM yang dibuat dan ditetapkan sebagai default untuk kluster Redshift Anda, gunakan hak istimewa ASSUMEROLE. Kontrol akses ini berlaku untuk pengguna database dan grup ketika mereka menjalankan perintah seperti yang tercantum sebelumnya. Setelah Anda memberikan hak istimewa ASSUMEROLE kepada pengguna atau grup untuk peran IAM, pengguna atau grup dapat mengambil peran tersebut saat menjalankan perintah ini. Dengan menggunakan hak istimewa ASSUMEROLE, Anda dapat memberikan akses ke perintah yang sesuai sesuai kebutuhan.

Menggunakan konsol Amazon Redshift, Anda dapat melakukan hal berikut:

- [Membuat peran IAM sebagai default](#)

- [Menghapus peran IAM dari klaster Anda](#)
- [Mengaitkan peran IAM dengan klaster Anda](#)
- [Menyetel peran IAM sebagai default](#)
- [Membuat peran IAM tidak lagi default untuk klaster Anda](#)

Izin kebijakan AmazonRedshiftAllCommandsFullAccess terkelola

Contoh berikut menunjukkan izin dalam kebijakan AmazonRedshiftAllCommandsFullAccess terkelola yang mengizinkan tindakan tertentu untuk peran IAM yang ditetapkan sebagai default untuk klaster Anda. Peran IAM dengan kebijakan izin yang dilampirkan mengotorisasi apa yang dapat dan tidak dapat dilakukan oleh pengguna atau grup. Dengan izin ini, Anda dapat menjalankan perintah COPY dari Amazon S3, menjalankan UNLOAD, dan menggunakan perintah CREATE MODEL.

```
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3>DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
    ],
    "Resource": [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3:::*redshift*",
        "arn:aws:s3:::*redshift/*"
    ]
}
```

Contoh berikut menunjukkan izin dalam kebijakan AmazonRedshiftAllCommandsFullAccess terkelola yang mengizinkan tindakan tertentu untuk peran IAM yang ditetapkan sebagai default untuk kluster. Peran IAM dengan kebijakan izin yang dilampirkan mengotorisasi apa yang dapat dan tidak dapat dilakukan oleh pengguna atau grup. Dengan izin berikut, Anda dapat menjalankan perintah CREATE EXTERNAL FUNCTION.

```
{
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": "arn:aws:lambda:*:*:function:*redshift*"
}
```

Contoh berikut menunjukkan izin dalam kebijakan AmazonRedshiftAllCommandsFullAccess terkelola yang mengizinkan tindakan tertentu untuk peran IAM yang ditetapkan sebagai default untuk kluster. Peran IAM dengan kebijakan izin yang dilampirkan mengotorisasi apa yang dapat dan tidak dapat dilakukan oleh pengguna atau grup. Dengan izin berikut, Anda dapat menjalankan perintah CREATE EXTERNAL SCHEMA dan CREATE EXTERNAL TABLE yang diperlukan untuk Amazon Redshift Spectrum.

```
{
  "Effect": "Allow",
  "Action": [
    "glue:CreateDatabase",
    "glue>DeleteDatabase",
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:UpdateDatabase",
    "glue:CreateTable",
    "glue>DeleteTable",
    "glue:BatchDeleteTable",
    "glue:UpdateTable",
    "glue:GetTable",
    "glue:GetTables",
    "glue:BatchCreatePartition",
    "glue:CreatePartition",
    "glue>DeletePartition",
    "glue:BatchDeletePartition",
    "glue:UpdatePartition",
    "glue:GetPartition",
    "glue:GetPartitions",
  ]
}
```



```

        "glue:BatchGetPartition"
    ],
    "Resource": [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*redshift*"
    ]
}

```

Contoh berikut menunjukkan izin dalam kebijakan `AmazonRedshiftAllCommandsFullAccess` terkelola yang mengizinkan tindakan tertentu untuk peran IAM ditetapkan sebagai default untuk kluster. Peran IAM dengan kebijakan izin yang dilampirkan mengotorisasi apa yang dapat dan tidak dapat dilakukan oleh pengguna atau grup. Dengan izin berikut, Anda dapat menjalankan perintah `CREATE EXTERNAL SCHEMA` menggunakan kueri federasi.

```

{
    "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"
        }
    }
},

```

Mengelola peran IAM yang dibuat untuk cluster menggunakan konsol

Untuk membuat, memodifikasi, dan menghapus peran IAM yang dibuat dari konsol Amazon Redshift, gunakan bagian Clusters di konsol.

Membuat peran IAM sebagai default

Di konsol, Anda dapat membuat peran IAM untuk klaster yang memiliki `AmazonRedshiftAllCommandsFullAccess` kebijakan yang dilampirkan secara otomatis. Peran IAM baru yang Anda buat memungkinkan Amazon Redshift menyalin, memuat, menanyakan, dan menganalisis data dari sumber daya Amazon di akun IAM Anda.

Hanya ada satu set peran IAM sebagai default untuk cluster. Jika Anda membuat peran IAM lain sebagai default cluster saat peran IAM yang ada saat ini ditetapkan sebagai default, peran IAM baru menggantikan peran IAM lainnya sebagai default.

Untuk membuat klaster baru dan peran IAM ditetapkan sebagai default untuk cluster baru

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster. Cluster untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih Buat cluster untuk membuat cluster.
4. Ikuti petunjuk di halaman konsol untuk memasukkan properti untuk konfigurasi Cluster. Untuk informasi selengkapnya tentang langkah ini, lihat [Membuat klaster](#).
5. (Opsional) Pilih Muat data sampel untuk memuat kumpulan data sampel ke cluster Amazon Redshift Anda untuk mulai menggunakan editor kueri untuk menanyakan data.

Jika Anda berada di belakang firewall, port database harus berupa port terbuka yang menerima koneksi masuk.

6. Ikuti petunjuk di halaman konsol untuk memasukkan properti untuk konfigurasi Database.
7. Di bawah Izin cluster, dari Kelola peran IAM, pilih Buat peran IAM.
8. Tentukan bucket Amazon S3 agar peran IAM dapat diakses dengan memilih salah satu metode berikut:
 - Pilih Tidak ada bucket Amazon S3 tambahan untuk membuat peran IAM tanpa menentukan bucket Amazon S3 tertentu.

- Pilih bucket Amazon S3 apa pun untuk memungkinkan pengguna yang memiliki akses ke kluster Amazon Redshift Anda untuk juga mengakses bucket Amazon S3 apa pun dan isinya di dalam Anda. Akun AWS
 - Pilih bucket Amazon S3 Spesifik untuk menentukan satu atau beberapa bucket Amazon S3 yang memiliki izin untuk diakses oleh peran IAM yang dibuat. Kemudian pilih satu atau lebih ember Amazon S3 dari tabel.
9. Pilih Buat peran IAM sebagai default. Amazon Redshift secara otomatis membuat dan menetapkan peran IAM sebagai default untuk kluster Anda.
 10. Pilih Buat cluster untuk membuat cluster. Cluster mungkin membutuhkan waktu beberapa menit untuk siap digunakan.

Menghapus peran IAM dari kluster Anda

Anda dapat menghapus satu atau beberapa peran IAM dari kluster Anda.

Untuk menghapus peran IAM dari kluster Anda

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster. Cluster untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih kluster tempat Anda ingin menghapus peran IAM.
4. Di bawah Izin cluster, pilih satu atau beberapa peran IAM yang ingin Anda hapus dari cluster.
5. Dari Kelola peran IAM, pilih Hapus peran IAM.

Mengaitkan peran IAM dengan kluster Anda

Anda dapat mengaitkan satu atau beberapa peran IAM dengan kluster Anda.

Untuk mengaitkan peran IAM dengan kluster Anda

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster. Cluster untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih kluster yang ingin Anda kaitkan dengan peran IAM.

4. Di bawah Izin cluster, pilih satu atau beberapa peran IAM yang ingin Anda kaitkan dengan klaster.
5. Dari Kelola peran IAM, pilih peran IAM Associate.
6. Pilih satu biji lagi peran IAM untuk diasosiasikan dengan cluster Anda.
7. Pilih peran IAM Associate.

Menyetel peran IAM sebagai default

Anda dapat mengatur peran IAM sebagai default untuk klaster Anda.

Untuk menjadikan peran IAM sebagai default untuk klaster Anda

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster. Cluster untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih klaster yang ingin Anda tetapkan peran IAM default.
4. Di bawah Izin cluster, dari peran IAM Terkait, pilih peran IAM yang ingin Anda jadikan sebagai default untuk klaster.
5. Di bawah Set default, pilih Make default.
6. Saat diminta, pilih Setel default untuk mengonfirmasi membuat peran IAM yang ditentukan sebagai default.

Membuat peran IAM tidak lagi default untuk klaster Anda

Anda dapat membuat peran IAM tidak lagi menjadi default untuk klaster Anda.

Untuk menghapus peran IAM sebagai default untuk cluster Anda

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster. Cluster untuk akun Anda saat ini Wilayah AWS terdaftar. Subset properti dari setiap cluster ditampilkan dalam kolom dalam daftar.
3. Pilih klaster yang ingin Anda kaitkan dengan peran IAM.
4. Di bawah Izin cluster, dari peran IAM Terkait, pilih peran IAM default.
5. Di bawah Setel default, pilih Hapus default.

6. Saat diminta, pilih Hapus default untuk mengonfirmasi pembersihan peran IAM yang ditentukan sebagai default.

Mengelola peran IAM yang dibuat di cluster menggunakan AWS CLI

Anda dapat mengelola peran IAM yang dibuat di cluster menggunakan. AWS CLI

Untuk membuat klaster Amazon Redshift dengan peran IAM ditetapkan sebagai default

Untuk membuat klaster Amazon Redshift dengan peran IAM, tetapkan sebagai default untuk cluster, gunakan perintah. `aws redshift create-cluster` AWS CLI

AWS CLI Perintah berikut membuat cluster Amazon Redshift dan peran IAM bernama `myrole1`. AWS CLI Perintah ini juga menetapkan `myrole1` sebagai default untuk cluster.

```
aws redshift create-cluster \  
  --node-type dc2.large \  
  --number-of-nodes 2 \  
  --master-username adminuser \  
  --master-user-password TopSecret1 \  
  --cluster-identifier mycluster \  
  --iam-roles 'arn:aws:iam::012345678910:role/myrole1'  
'arn:aws:iam::012345678910:role/myrole2' \  
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

Cuplikan berikut adalah contoh responsnya.

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

```
    ]  
    ...  
  }  
}
```

Untuk menambahkan satu atau beberapa peran IAM ke cluster Amazon Redshift

Untuk menambahkan satu atau beberapa peran IAM yang terkait dengan cluster, gunakan `aws redshift modify-cluster-iam-roles` AWS CLI perintah.

AWS CLI Perintah berikut menambahkan `myrole3` dan `myrole4` ke cluster.

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier mycluster \  
  --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3'  
  'arn:aws:iam::012345678910:role/myrole4'
```

Cuplikan berikut adalah contoh responsnya.

```
{  
  "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"  
      }  
    ],  
  },  
}
```

```
    ...  
  }  
}
```

Untuk menghapus satu atau beberapa peran IAM dari klaster Amazon Redshift

Untuk menghapus satu atau beberapa peran IAM yang terkait dengan cluster, gunakan `aws redshift modify-cluster-iam-roles` AWS CLI perintah.

AWS CLI Perintah berikut menghapus `myrole3` dan `myrole4` dari cluster.

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier mycluster \  
  --remove-iam-roles 'arn:aws:iam::012345678910:role/myrole3'  
'arn:aws:iam::012345678910:role/myrole4'
```

Cuplikan berikut adalah contoh responsnya.

```
{  
  "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"  
      }  
    ],  
    ...  
  },  
  ...  
}
```

```
}
}
```

Untuk menetapkan peran IAM terkait sebagai default untuk cluster

Untuk menetapkan peran IAM terkait sebagai default untuk cluster, gunakan `aws redshift modify-cluster-iam-roles` AWS CLI perintah.

AWS CLI Perintah berikut ditetapkan `myrole2` sebagai default untuk cluster.

```
aws redshift modify-cluster-iam-roles \
  --cluster-identifier mycluster \
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole2'
```

Cuplikan berikut adalah contoh responsnya.

```
{
  "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"
      }
    ],
    ...
  }
}
```

Untuk menetapkan peran IAM yang tidak terkait sebagai default untuk cluster

Untuk menetapkan peran IAM yang tidak terkait sebagai default untuk cluster, gunakan perintah. `aws redshift modify-cluster-iam-roles` AWS CLI

AWS CLI Perintah berikut ditambahkan `myrole2` ke cluster Amazon Redshift dan menetapkannya sebagai default untuk cluster.


```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier mycluster \  
  --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3' \  
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole3'
```

Cuplikan berikut adalah contoh responsnya.

```
{  
  "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"  
      }  
    ],  
    ...  
  }  
}
```

Untuk memulihkan cluster dari snapshot dan menetapkan peran IAM sebagai default untuk itu

Saat memulihkan klaster dari snapshot, Anda dapat mengaitkan peran IAM yang ada atau membuat yang baru dan mengaturnya sebagai default untuk cluster.

Untuk memulihkan klaster Amazon Redshift dari snapshot dan menetapkan peran IAM sebagai default cluster, gunakan perintah. `aws redshift restore-from-cluster-snapshot` AWS CLI

AWS CLI Perintah berikut mengembalikan cluster dari snapshot dan menetapkan `myrole2` sebagai default untuk cluster.

```
aws redshift restore-from-cluster-snapshot \  
  --cluster-identifier mycluster-clone \  
  --snapshot-identifier my-snapshot-id \  
  --iam-roles 'arn:aws:iam::012345678910:role/myrole1'  
'arn:aws:iam::012345678910:role/myrole2' \  
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

Cuplikan berikut adalah contoh responsnya.

```
{  
  "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"  
      }  
    ],  
    ...  
  }  
}
```

Menggunakan identitas federasi untuk mengelola akses Amazon Redshift ke sumber daya lokal dan tabel eksternal Amazon Redshift Spectrum

Menggunakan federasi identitas AWS dengan kredensial yang disediakan dari `GetDatabaseCredentials` dapat menyederhanakan otorisasi dan akses ke data lokal dan ke data eksternal. Saat ini, untuk memberi pengguna akses ke data eksternal yang berada di Amazon S3, Anda membuat peran IAM dengan izin yang ditentukan dalam kebijakan izin. Kemudian, pengguna dengan peran terlampir dapat mengakses data eksternal. Ini berfungsi, tetapi jika Anda ingin memberikan aturan granular, seperti membuat kolom tertentu tidak tersedia untuk pengguna tertentu, Anda mungkin harus melakukan konfigurasi tambahan pada skema eksternal. Dalam topik ini, kami menunjukkan cara menyediakan akses ke sumber daya dengan federasi AWS

identitas, alih-alih menggunakan peran IAM tertentu. Federasi identitas, dengan kredensial yang disediakan dari `GetDatabaseCredentials`, dapat menyediakan akses ke dan sumber daya AWS Glue Redshift Spectrum melalui aturan IAM granular yang lebih mudah ditentukan dan diubah. Ini membuatnya lebih mudah untuk menerapkan akses yang sesuai dengan aturan bisnis Anda.

Manfaat menggunakan kredensial federasi adalah sebagai berikut:

- Anda tidak perlu mengelola peran IAM terlampir cluster untuk Redshift Spectrum.
- Administrator cluster dapat membuat skema eksternal yang dapat diakses oleh konsumen dengan konteks IAM yang berbeda. Ini berguna, misalnya, untuk melakukan pemfilteran kolom pada tabel, di mana konsumen yang berbeda menanyakan skema eksternal yang sama dan mendapatkan berbagai bidang dalam catatan yang dikembalikan.
- Anda dapat menanyakan Amazon Redshift menggunakan pengguna dengan izin IAM, bukan hanya dengan peran.

Mempersiapkan identitas untuk masuk dengan identitas federasi

Sebelum masuk dengan identitas federasi, Anda harus melakukan beberapa langkah awal. Instruksi ini mengasumsikan Anda memiliki skema eksternal Redshift Spectrum yang sudah ada yang mereferensikan file data yang disimpan di bucket Amazon S3, dan bucket berada di akun yang sama dengan cluster Amazon Redshift atau gudang data Amazon Redshift Tanpa Server.

1. Buat identitas IAM. Ini bisa menjadi pengguna atau peran IAM. Gunakan nama apa pun yang didukung oleh IAM.
2. Lampirkan kebijakan izin ke identitas. Tentukan salah satu dari berikut ini:
 - `redshift:GetClusterCredentialsWithIAM` (untuk cluster yang disediakan Amazon Redshift)
 - `redshift-serverless:GetCredentials` (untuk Amazon Redshift Tanpa Server)

Anda dapat menambahkan izin dengan editor kebijakan, menggunakan konsol IAM.

Identitas IAM juga memerlukan izin untuk mengakses data eksternal. Berikan akses ke Amazon S3 dengan menambahkan kebijakan AWS terkelola berikut secara langsung:

- `AmazonS3ReadOnlyAccess`
- `AWSGlueConsoleFullAccess`

Kebijakan terkelola terakhir diperlukan jika Anda menggunakan AWS Glue untuk menyiapkan data eksternal Anda. Untuk informasi selengkapnya tentang langkah-langkah pemberian akses ke Amazon Redshift Spectrum, lihat [Membuat peran IAM untuk Amazon Redshift, yang merupakan bagian dari panduan memulai Amazon Redshift](#) dan Redshift Spectrum. Ini menunjukkan langkah-langkah untuk menambahkan kebijakan IAM untuk mengakses Redshift Spectrum.

3. Siapkan klien SQL Anda untuk terhubung ke Amazon Redshift. Gunakan driver Amazon Redshift JDBC, dan tambahkan kredensial pengguna Anda ke properti kredensi alat. Klien seperti SQL Workbench/J bekerja dengan baik untuk ini. Mengatur properti `extended client-connection` berikut:

- `AccessKeyID` — Pengidentifikasi kunci akses Anda.
- `SecretAccessKunci` — Kunci akses rahasia Anda. (Perhatikan risiko keamanan mentransmisikan kunci rahasia jika Anda tidak menggunakan enkripsi.)
- `SessionToken`— Satu set kredensi sementara untuk peran IAM.
- `GroupFederation` - Setel ke `true` jika Anda mengonfigurasi identitas federasi untuk kluster yang disediakan. Jangan setel parameter ini jika Anda menggunakan Amazon Redshift Serverless.
- `LogLevel`— Nilai tingkat log integer. Ini bersifat opsional.

4. Setel URL ke titik akhir JDBC yang ditemukan di konsol Amazon Redshift atau Amazon Redshift Tanpa Server. Ganti skema URL Anda dengan `jdbc:redshift:iam:` dan gunakan pemformatan ini:

- Format untuk kluster yang disediakan Amazon Redshift: `jdbc:redshift:iam://<cluster_id>.<unique_suffix>.<region>.redshift.amazonaws.com:<port>/<database_name>`

Contoh: `jdbc:redshift:iam://test1.12345abcdefg.us-east-1.redshift.amazonaws.com:5439/dev`

- Format untuk Amazon Redshift Tanpa Server: `jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com:5439:<port>/<database_name>`

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

Setelah Anda terhubung ke database untuk pertama kalinya, menggunakan identitas IAM, Amazon Redshift secara otomatis membuat identitas Amazon Redshift dengan nama yang sama, diawali IAM: dengan untuk pengguna IAMR: atau untuk peran IAM. Langkah-langkah yang tersisa dalam topik ini menunjukkan contoh untuk pengguna.

Jika pengguna Redshift tidak dibuat secara otomatis, Anda dapat membuatnya dengan menjalankan `CREATE USER` pernyataan, menggunakan akun admin, yang menentukan nama pengguna dalam format. `IAM:<user name>`

5. Sebagai administrator kluster Amazon Redshift Anda, berikan pengguna Redshift izin yang diperlukan untuk mengakses skema eksternal.

```
GRANT ALL ON SCHEMA my_schema to "IAM:my_user";
```

Untuk memberikan kemampuan kepada pengguna Redshift Anda untuk membuat tabel dalam skema eksternal, mereka harus menjadi pemilik skema. Sebagai contoh:

```
ALTER SCHEMA my_schema owner to "IAM:my_user";
```

6. Untuk memverifikasi konfigurasi, jalankan kueri sebagai pengguna, menggunakan klien SQL, setelah izin diberikan. Sampel kueri ini mengambil data dari tabel eksternal.

```
SELECT * FROM my_schema.my_table;
```

Memulai dengan propagasi identitas dan otorisasi ke Redshift Spectrum

Untuk meneruskan identitas federasi ke tabel eksternal kueri, Anda menetapkan `SESSION` sebagai nilai untuk parameter `IAM_ROLE` kueri. `CREATE EXTERNAL SCHEMA` Langkah-langkah berikut menunjukkan cara mengatur dan memanfaatkan `SESSION` untuk mengotorisasi kueri pada skema eksternal.

1. Buat tabel lokal dan tabel eksternal. Tabel eksternal dikatalogkan dengan AWS Glue pekerjaan untuk ini.
2. Connect ke Amazon Redshift dengan identitas IAM Anda. Seperti disebutkan di bagian sebelumnya, ketika identitas terhubung ke Amazon Redshift, pengguna database Redshift dibuat. Pengguna dibuat jika sebelumnya tidak ada. Jika pengguna baru, administrator harus

memberi mereka izin untuk melakukan tugas di Amazon Redshift, seperti menanyakan dan membuat tabel.

3. Connect ke Redshift dengan akun admin Anda. Jalankan perintah untuk membuat skema eksternal, menggunakan SESSION nilai.

```
create external schema spectrum_schema from data catalog
database '<my_external_database>'
region '<my_region>'
iam_role 'SESSION'
catalog_id '<my_catalog_id>;'
```

Perhatikan bahwa `catalog_id` diatur dalam kasus ini. Ini adalah pengaturan baru yang ditambahkan dengan fitur, karena SESSION menggantikan peran tertentu.

Dalam contoh ini, nilai dalam kueri meniru bagaimana nilai nyata muncul.

```
create external schema spectrum_schema from data catalog
database 'spectrum_db'
region 'us-east-1'
iam_role 'SESSION'
catalog_id '123456789012'
```

`catalog_id` Nilai dalam hal ini adalah ID AWS akun Anda.

4. Jalankan kueri untuk mengakses data eksternal Anda, menggunakan identitas IAM yang terhubung dengan Anda pada langkah 2. Sebagai contoh:

```
select * from spectrum_schema.table1;
```

Dalam hal ini, `table1` dapat berupa, misalnya, data berformat JSON dalam file, di bucket Amazon S3.

5. Jika Anda sudah memiliki skema eksternal yang menggunakan peran IAM terlampir cluster, menunjuk ke database atau skema eksternal Anda, Anda dapat mengganti skema yang ada dan menggunakan identitas federasi seperti yang dirinci dalam langkah-langkah ini, atau membuat yang baru.

SESSION menunjukkan bahwa kredensial identitas federasi digunakan untuk menanyakan skema eksternal. Saat Anda menggunakan parameter SESSION kueri, pastikan Anda

`mengaturcatalog_id`. Ini diperlukan karena menunjuk ke katalog data yang digunakan untuk skema. Sebelumnya, `catalog_id` diambil dari nilai yang ditetapkan untuk `iam_role`. Saat Anda mengatur propagasi identitas dan otorisasi dengan cara ini, misalnya, ke Redshift Spectrum, dengan menggunakan kredensial federasi untuk menanyakan skema eksternal, otorisasi melalui peran IAM tidak diperlukan.

Catatan penggunaan

Kesalahan koneksi umum adalah sebagai berikut: Kesalahan IAM mengambil kredensial sementara: Tidak dapat membatalkan respons pengecualian dengan `unmarshallers` yang disediakan. Kesalahan ini adalah hasil dari memiliki driver JDBC lama. Versi driver minimum yang diperlukan untuk identitas federasi adalah 2.1.0.9. Anda bisa mendapatkan driver JDBC dari [Unduh driver Amazon Redshift JDBC](#), versi 2.1.

Sumber daya tambahan

Tautan ini memberikan informasi tambahan untuk mengelola akses ke data eksternal.

- Anda masih dapat mengakses data Redshift Spectrum menggunakan peran IAM. Untuk informasi selengkapnya, lihat [Mengotorisasi Amazon Redshift untuk mengakses layanan AWS lain atas nama Anda](#).
- Saat Anda mengelola akses ke tabel eksternal AWS Lake Formation, Anda dapat menanyakannya menggunakan Redshift Spectrum dengan identitas IAM federasi. Anda tidak lagi harus mengelola peran IAM terlampir cluster untuk Redshift Spectrum untuk menanyakan data yang terdaftar. AWS Lake Formation Untuk informasi selengkapnya, lihat [Menggunakan AWS Lake Formation Amazon Redshift Spectrum](#).

Mengelola kata sandi admin Amazon Redshift menggunakan AWS Secrets Manager

Amazon Redshift dapat diintegrasikan dengan AWS Secrets Manager untuk menghasilkan dan mengelola kredensi admin Anda di dalam rahasia terenkripsi. Dengan AWS Secrets Manager, Anda dapat mengganti kata sandi admin Anda dengan panggilan API untuk mengambil rahasia secara terprogram saat diperlukan. Menggunakan rahasia alih-alih kredensial hard-code mengurangi risiko kredensial tersebut terpapar atau dikompromikan. Untuk informasi selengkapnya AWS Secrets Manager, lihat [Panduan AWS Secrets Manager Pengguna](#).

Anda dapat menentukan bahwa Amazon Redshift mengelola kata sandi admin Anda menggunakan AWS Secrets Manager saat Anda melakukan salah satu operasi berikut:

- Membuat klaster yang disediakan atau namespace tanpa server
- Memulihkan namespace cluster atau tanpa server dari snapshot

Saat Anda menentukan bahwa Amazon Redshift mengelola kata sandi admin di AWS Secrets Manager, Amazon Redshift membuat kata sandi dan menyimpannya di Secrets Manager. Anda dapat mengakses rahasia secara langsung AWS Secrets Manager untuk mengambil kredensi untuk pengguna admin. Secara opsional, Anda dapat menentukan kunci yang dikelola pelanggan untuk mengenkripsi rahasia jika Anda perlu mengakses rahasia dari akun lain AWS. Anda juga dapat menggunakan kunci KMS yang AWS Secrets Manager menyediakan.

Amazon Redshift mengelola pengaturan untuk rahasia dan memutar rahasia setiap 30 hari secara default. Anda dapat memutar rahasia secara manual kapan saja. Jika Anda menghapus klaster yang disediakan atau namespace tanpa server yang mengelola rahasia AWS Secrets Manager, rahasia dan metadata terkait juga akan dihapus.

Untuk menyambung ke klaster atau namespace tanpa server dengan kredensial yang dikelola rahasia, Anda dapat mengambil rahasia dari menggunakan AWS Secrets Manager konsol Secrets Manager atau panggilan Secrets Manager API. `GetSecretValue` Untuk informasi selengkapnya, lihat [Mengambil rahasia dari AWS Secrets Manager](#) dan [Connect ke database SQL dengan kredensi dalam AWS Secrets Manager rahasia di Panduan Pengguna](#).AWS Secrets Manager

Izin diperlukan untuk integrasi AWS Secrets Manager

Pengguna harus memiliki izin yang diperlukan untuk melakukan operasi yang terkait dengan AWS Secrets Manager integrasi. Buat kebijakan IAM yang memberikan izin untuk melakukan operasi API tertentu pada sumber daya tertentu yang mereka butuhkan. Kemudian lampirkan kebijakan tersebut ke set izin IAM atau peran yang memerlukan izin tersebut. Untuk informasi selengkapnya, lihat [Manajemen identitas dan akses di Amazon Redshift](#).

Pengguna yang menentukan bahwa Amazon Redshift mengelola kata sandi AWS Secrets Manager admin harus memiliki izin untuk melakukan operasi berikut:

- `secretsmanager:CreateSecret`
- `secretsmanager:RotateSecret`
- `secretsmanager:DescribeSecret`

- `secretsmanager:UpdateSecret`
- `secretsmanager>DeleteSecret`
- `secretsmanager:GetRandomPassword`
- `secretsmanager:TagResource`

Jika pengguna ingin meneruskan kunci KMS dalam `MasterPasswordSecretKmsKeyId` parameter untuk kluster yang disediakan, atau `AdminPasswordSecretKmsKeyId` parameter untuk ruang nama tanpa server, mereka memerlukan izin berikut selain izin yang tercantum di atas.

- `kms:Decrypt`
- `kms:GenerateDataKey`
- `kms:CreateGrant`
- `kms:RetireGrant`

Memutar rahasia kata sandi admin

Secara default, Amazon Redshift secara otomatis memutar rahasia Anda setiap 30 hari untuk memastikan kredensial Anda tidak tetap sama untuk waktu yang lama. Saat Amazon Redshift memutar rahasia kata sandi admin, AWS Secrets Manager memperbarui rahasia yang ada untuk memuat kata sandi admin baru. Amazon Redshift mengubah kata sandi admin untuk cluster agar sesuai dengan kata sandi dalam rahasia yang diperbarui.

Anda dapat memutar rahasia segera alih-alih menunggu rotasi terjadwal dengan menggunakan AWS Secrets Manager. Untuk informasi selengkapnya tentang memutar rahasia, lihat [Memutar AWS Secrets Manager rahasia](#) di Panduan AWS Secrets Manager Pengguna.

Mengambil Nama Sumber Daya Amazon rahasia (ARN) di Amazon Redshift

Anda dapat melihat Nama Sumber Daya Amazon (ARN) untuk mengetahui rahasia apa pun yang dikelola dengan AWS Secrets Manager menggunakan konsol Amazon Redshift. Setelah Anda memiliki ARN rahasia, Anda dapat melihat detail tentang rahasia Anda dan data terenkripsi dalam rahasia Anda menggunakan. AWS Secrets Manager Untuk informasi selengkapnya tentang mengambil rahasia menggunakan ARN, [lihat Mengambil](#) rahasia di AWS Secrets Manager Panduan Pengguna.

Melihat detail tentang rahasia untuk cluster yang disediakan Amazon Redshift

Lihat Nama Sumber Daya Amazon (ARN) untuk rahasia klaster Anda menggunakan konsol Amazon Redshift dengan prosedur berikut:

1. Masuk ke AWS Management Console dan buka konsol Amazon Redshift.
2. Di panel ikhtisar Cluster, pilih cluster yang rahasianya ingin Anda lihat.
3. Pilih tab Properti.
4. Lihat ARN rahasia di bawah kredensi Admin ARN. ARN ini adalah pengidentifikasi rahasia, yang dapat Anda gunakan AWS Secrets Manager untuk melihat detail rahasia.

Melihat detail tentang rahasia untuk namespace Amazon Redshift Tanpa Server

Lihat Nama Sumber Daya Amazon (ARN) untuk rahasia namespace tanpa server Anda menggunakan konsol Amazon Redshift dengan prosedur berikut:

1. Masuk ke AWS Management Console dan buka konsol Amazon Redshift.
2. Dari dasbor klaster yang disediakan, pilih Buka Tanpa Server di kanan atas halaman.
3. Dari dasbor Tanpa Server, gulir ke panel Namespace/ Workgroups dan pilih namespace yang rahasianya ingin Anda lihat.
4. Di panel Informasi umum, lihat ARN rahasia di bawah kredensi Admin ARN. ARN ini adalah pengidentifikasi rahasia, yang dapat Anda gunakan AWS Secrets Manager untuk melihat detail rahasia.

Membuat rahasia untuk kredensi koneksi database

Anda dapat membuat rahasia Secrets Manager untuk menyimpan kredensial yang digunakan untuk menyambung ke klaster yang disediakan Amazon Redshift atau namespace dan workgroup Redshift Tanpa Server. Anda juga dapat menggunakan rahasia ini saat menjadwalkan kueri di editor kueri Amazon Redshift v2.

Untuk membuat rahasia untuk database di klaster yang disediakan Amazon Redshift menggunakan konsol Secrets Manager

1. Buka konsol Secrets Manager (<https://console.aws.amazon.com/secretsmanager/>).
2. Arahkan ke daftar Rahasia dan pilih Simpan rahasia baru.
3. Pilih Kredensial untuk gudang data Amazon Redshift. Masukkan informasi Anda dalam langkah-langkah untuk membuat rahasia sebagai berikut:

- Di Kredensial untuk Nama Pengguna, masukkan nama pengguna administratif gudang data.
 - Di Kredensial untuk Kata Sandi, masukkan kata sandi untuk nama Pengguna.
 - Untuk kunci Enkripsi, pilih kunci enkripsi Anda.
 - Untuk gudang Data, pilih klaster yang disediakan Amazon Redshift yang berisi data Anda.
 - Untuk nama Rahasia, masukkan nama untuk rahasianya.
 - Untuk Deskripsi, masukkan deskripsi rahasia.
 - Untuk Tag, masukkan kunci Tag dengan kata **Redshift**. Kunci tag ini diperlukan untuk mencantumkan rahasia saat Anda mencoba menyambung ke gudang data menggunakan editor kueri Amazon Redshift v2. Rahasia harus memiliki kunci tag yang dimulai dengan string **Redshift** untuk rahasia yang akan terdaftar di bawah AWS Secrets Manager pada konsol manajemen.
4. Lanjutkan memasukkan informasi tentang rahasia Anda melalui beberapa langkah hingga Anda Menyimpan perubahan pada langkah Tinjauan.

Nilai spesifik kredensial, engine, host, port, dan pengidentifikasi cluster Anda disimpan dalam rahasia. Juga, rahasianya ditandai dengan kunci `Redshift` tag.

Untuk membuat rahasia untuk database di namespace Redshift Serverless menggunakan konsol Redshift Serverless

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pilih Redshift tanpa server dan navigasikan ke konfigurasi Namespace.
3. Pilih namespace untuk membuat kredensial rahasia.
4. Buka Tindakan, Edit kredensial admin.
5. Untuk kata sandi Admin, pilih Kelola kredensial admin di AWS Secrets Manager
6. Pilih Simpan perubahan untuk menyimpan perubahan Anda.

Konfirmasikan bahwa muncul pesan bahwa kata sandi berhasil diubah. Anda juga dapat melihat rahasia di konsol Secrets Manager. Anda dapat menggunakan rahasia ini untuk menyambung ke database di workgroup di konsol Redshift Serverless dan editor kueri Amazon Redshift v2, menggunakan metode koneksi. AWS Secrets Manager Rahasianya harus memiliki kunci tag yang dimulai dengan string "Redshift" agar rahasianya terdaftar di aplikasi web editor kueri v2. Rahasia

harus memiliki kunci tag yang dimulai dengan string **Redshift** untuk rahasia yang akan terdaftar di bawah AWS Secrets Manager pada konsol manajemen.

Untuk membuat rahasia untuk database di namespace Redshift Serverless menggunakan konsol Secrets Manager

1. Buka konsol Secrets Manager (<https://console.aws.amazon.com/secretsmanager/>).
2. Arahkan ke daftar Rahasia dan pilih Simpan rahasia baru.
3. Pilih Kredensial untuk gudang data Amazon Redshift. Masukkan informasi Anda dalam langkah-langkah untuk membuat rahasia sebagai berikut:
 - Di Kredensial untuk Nama Pengguna, masukkan nama pengguna administratif gudang data.
 - Di Kredensial untuk Kata Sandi, masukkan kata sandi untuk nama Pengguna.
 - Untuk kunci Enkripsi, pilih kunci enkripsi Anda.
 - Untuk gudang Data, pilih namespace Redshift Tanpa Server yang berisi data Anda.
 - Untuk nama Rahasia, masukkan nama untuk rahasianya.
 - Untuk Deskripsi, masukkan deskripsi rahasia.
 - Untuk Tag, masukkan kunci Tag dengan kata **Redshift**. Kunci tag ini diperlukan untuk mencantumkan rahasia saat Anda mencoba menyambung ke gudang data menggunakan editor kueri Amazon Redshift v2. Rahasia harus memiliki kunci tag yang dimulai dengan string **Redshift** untuk rahasia yang akan terdaftar di bawah AWS Secrets Manager pada konsol manajemen.
4. Lanjutkan memasukkan informasi tentang rahasia Anda melalui beberapa langkah hingga Anda Menyimpan perubahan pada langkah Tinjauan.

Nilai spesifik kredensial, nama database, host, port, namespace, dan mesin Anda disimpan dalam rahasia. Juga, rahasianya ditandai dengan kunci **Redshift** tag.

Untuk membuat rahasia untuk database di namespace Redshift Tanpa Server menggunakan AWS CLI

Anda dapat menggunakan AWS CLI untuk membuat rahasia. Salah satu metode adalah dengan menggunakan AWS CloudShell untuk menjalankan AWS CLI perintah Secrets Manager sebagai berikut. Anda harus memiliki izin yang tepat untuk menjalankan AWS CLI perintah yang ditunjukkan dalam prosedur berikut.

1. Di AWS konsol, buka prompt AWS CloudShell perintah. Untuk informasi selengkapnya AWS CloudShell, lihat [Apa yang ada AWS CloudShell](#) di Panduan AWS CloudShell Pengguna.
2. Misalnya, untuk rahasia MyTestSecret masukkan perintah Secrets Manager untuk menyimpan rahasia yang digunakan untuk menyambung ke database atau menjadwalkan kueri Amazon Redshift query editor v2. Ganti nilai berikut dalam perintah dengan nilai untuk lingkungan Anda:
 - *admin* adalah nama pengguna administrator untuk gudang data.
 - *passwd0rd* adalah kata sandi administrator.
 - *dev* adalah nama database awal di gudang data.
 - *wilayah* adalah Wilayah AWS yang berisi gudang data. Sebagai contoh, us-east-1.
 - *123456789012* adalah. Akun AWS
 - *namespace-id* adalah pengenal namespace yang mirip dengan. c3928f0e-c889-4d2b-97a5-5738324d5d3e Anda dapat menemukan pengenal ini di halaman detail konsol Amazon Redshift untuk namespace tanpa server.

```
aws secretsmanager create-secret \
--name MyTestSecret \
--description "My test secret created with the CLI." \
--secret-string "{\"username\":\"admin\",\"password\":\"passwd0rd\",\"dbname\":\"dev\",\"engine\":\"redshift\"}" \
--tags "[{\"Key\":\"redshift-serverless:namespaceArn\",\"Value\":\"arn:aws:redshift-serverless:region:123456789012:namespace/namespace-id\"}]"
```

Pertimbangan menggunakan Amazon AWS Secrets Manager Redshift

Saat menggunakan AWS Secrets Manager untuk mengelola kredensi admin klaster atau namespace tanpa server yang disediakan, pertimbangkan hal berikut:

- Saat Anda menjeda klaster yang kredensialnya dikelola oleh admin AWS Secrets Manager, rahasia klaster Anda tidak akan dihapus dan Anda akan terus ditagih untuk rahasia tersebut. Rahasia hanya dihapus ketika Anda menghapus cluster.
- Jika klaster Anda dijeda saat Amazon Redshift mencoba memutar rahasia terlampirnya, rotasi akan gagal. Dalam hal ini, Amazon Redshift menghentikan rotasi otomatis dan tidak akan mencoba memutarnya lagi, bahkan setelah Anda melanjutkan cluster. Anda harus memulai ulang jadwal

rotasi otomatis menggunakan panggilan `secretsmanager:RotateSecret` API untuk terus memutar rahasia Anda AWS Secrets Manager secara otomatis.

- Jika namespace tanpa server Anda tidak memiliki grup kerja yang terkait saat Amazon Redshift mencoba memutar rahasia terlampirnya, rotasi akan gagal dan tidak akan mencoba memutarnya lagi, bahkan setelah Anda melampirkan grup kerja. Anda harus memulai ulang jadwal rotasi otomatis menggunakan panggilan `secretsmanager:RotateSecret` API untuk terus memutar rahasia Anda AWS Secrets Manager secara otomatis.

Pencatatan dan pemantauan di Amazon Redshift

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan kinerja Amazon Redshift dan AWS solusi Anda. Anda dapat mengumpulkan data pemantauan dari semua bagian AWS solusi sehingga Anda bisa melakukan debug kegagalan multitiket secara lebih mudah jika kegagalan ini terjadi. AWS menyediakan beberapa alat untuk memantau sumber daya Amazon Redshift Anda dan merespons potensi insiden:

CloudWatch Alarm Amazon

Dengan menggunakan CloudWatch alarm Amazon, Anda melihat satu metrik selama periode waktu yang Anda tentukan. Jika metrik melebihi ambang batas tertentu, pemberitahuan dikirim ke topik Amazon SNS atau kebijakan AWS Auto Scaling. CloudWatch Alarm tidak menimbulkan tindakan karena alarm berada dalam status tertentu. Lebih tepatnya, status harus berubah dan dipertahankan selama periode tertentu. Untuk informasi selengkapnya, lihat [Mengelola alarm-alarm](#). Untuk daftar metrik, lihat [Memantau Amazon Redshift menggunakan metrik CloudWatch](#).

AWS CloudTrail Log

CloudTrail memberikan catatan operasi API yang diambil oleh pengguna, peran IAM, atau AWS layanan di Amazon Redshift. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon Redshift, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail lainnya. Untuk informasi selengkapnya, lihat [Logging dengan CloudTrail](#).

Pencatatan audit basis data

Amazon Redshift mencatat informasi tentang koneksi dan aktivitas pengguna di database Anda. Log ini membantu Anda memantau database untuk tujuan keamanan dan pemecahan masalah, proses yang disebut audit database. Log dapat disimpan di:

- Bucket Amazon S3 - Ini menyediakan akses dengan fitur keamanan data untuk pengguna yang bertanggung jawab untuk memantau aktivitas dalam database.
- Amazon CloudWatch - Anda dapat melihat data pencatatan audit menggunakan fitur bawaan CloudWatch, seperti fitur visualisasi dan tindakan pengaturan.

 Note

[SYS_CONNECTION_LOG](#) mengumpulkan data log koneksi untuk Amazon Redshift Tanpa Server. Perhatikan bahwa saat Anda mengumpulkan data pencatatan audit untuk Amazon Redshift Tanpa Server, data tersebut tidak dapat dikirim ke file log, hanya ke file log CloudWatch

Topik

- [Log Amazon Redshift](#)
- [Mengaktifkan pencatatan log](#)
- [Mengirim log audit ke Amazon CloudWatch](#)
- [Mengelola file log di Amazon S3](#)
- [Memecahkan masalah pencatatan audit Amazon Redshift di Amazon S3](#)
- [Mencatat panggilan Amazon Redshift API dengan AWS CloudTrail](#)
- [Mengkonfigurasi audit menggunakan konsol](#)
- [Mengonfigurasi logging dengan menggunakan API Amazon AWS CLI Redshift dan Amazon](#)

Log Amazon Redshift

Amazon Redshift mencatat informasi dalam file log berikut:

- Log koneksi - Upaya otentikasi log, koneksi, dan pemutusan.
- Log pengguna — Log informasi tentang perubahan definisi pengguna database.
- Log aktivitas pengguna — Log setiap kueri sebelum dijalankan pada database.

Koneksi dan log pengguna berguna terutama untuk tujuan keamanan. Anda dapat menggunakan log koneksi untuk memantau informasi tentang pengguna yang terhubung ke database dan informasi koneksi terkait. Informasi ini mungkin alamat IP mereka, ketika mereka membuat permintaan, jenis

otentikasi apa yang mereka gunakan, dan sebagainya. Anda dapat menggunakan log pengguna untuk memantau perubahan definisi pengguna database.

Log aktivitas pengguna berguna terutama untuk tujuan pemecahan masalah. Ini melacak informasi tentang jenis kueri yang dilakukan pengguna dan sistem dalam database.

Log koneksi dan log pengguna keduanya sesuai dengan informasi yang disimpan dalam tabel sistem di database Anda. Anda dapat menggunakan tabel sistem untuk mendapatkan informasi yang sama, tetapi file log menyediakan mekanisme yang lebih sederhana untuk pengambilan dan peninjauan. File log mengandalkan izin Amazon S3 daripada izin database untuk melakukan kueri terhadap tabel. Selain itu, dengan melihat informasi dalam file log daripada menanyakan tabel sistem, Anda mengurangi dampak berinteraksi dengan database.

Note

File log tidak terkini seperti tabel log sistem yang [STL_USERLOG](#) dan [STL_CONNECTION_LOG](#). Catatan yang lebih tua dari, tetapi tidak termasuk, catatan terbaru disalin ke file log.

Note

Untuk Amazon Redshift Tanpa Server, [SYS_CONNECTION_LOG](#) mengumpulkan data log koneksi. Saat Anda mengumpulkan data pencatatan audit untuk Amazon Redshift Tanpa Server, data tersebut tidak dapat dikirim ke file log, hanya ke file log. CloudWatch

Log koneksi

Log upaya otentikasi, dan koneksi dan pemutusan. Tabel berikut menjelaskan informasi dalam log koneksi. Untuk informasi selengkapnya tentang bidang ini, lihat [STL_CONNECTION_LOG di Panduan Pengembang Database Amazon Redshift](#). [Untuk informasi selengkapnya tentang data log koneksi yang dikumpulkan untuk Amazon Redshift Serverless, lihat SYS_CONNECTION_LOG.](#)

Nama kolom	Deskripsi
kejadian	Koneksi atau acara otentikasi.
rekor waktu	Waktu peristiwa itu terjadi.

Nama kolom	Deskripsi
remotehost	Nama atau alamat IP host jarak jauh.
remote port	Nomor port untuk host jarak jauh.
pid	ID proses yang terkait dengan pernyataan.
dbname	Nama basis data.
nama pengguna	Nama pengguna.
authmethod	Metode otentikasi.
durasi	Durasi koneksi dalam mikrodetik.
sslversion	Versi Secure Sockets Layer (SSL).
sslcipher	Sandi SSL.
mtu	Unit transmisi maksimum (MTU).
sslkompresi	Jenis kompresi SSL.
sslexpansion	Jenis ekspansi SSL.
iamauthguid	ID otentikasi AWS Identity and Access Management (IAM) untuk permintaan tersebut. AWS CloudTrail Ini adalah pengenal untuk panggilan GetClusterCredentials API untuk membuat kredensial yang digunakan untuk koneksi tertentu.
application_name	Nama awal atau yang diperbarui dari aplikasi untuk sesi.
os_versi	Versi sistem operasi yang ada di mesin klien yang terhubung ke cluster Amazon Redshift Anda.
driver_version	Versi driver ODBC atau JDBC yang terhubung ke cluster Amazon Redshift Anda dari alat klien SQL pihak ketiga Anda.

Nama kolom	Deskripsi
plugin_name	Nama plugin yang digunakan untuk terhubung ke cluster Amazon Redshift Anda.
protocol_version	Versi protokol internal yang digunakan driver Amazon Redshift saat membuat koneksi dengan server.
sessionid	Pengidentifikasi unik global untuk sesi saat ini.
Kompresi	Algoritma kompresi yang digunakan untuk koneksi.

Log pengguna

Merekam detail untuk perubahan berikut pada pengguna database:

- Buat pengguna
- Jatuhkan pengguna
- Ubah pengguna (ganti nama)
- Mengubah pengguna (mengubah properti)

Nama kolom	Deskripsi
userid	ID pengguna yang terpengaruh oleh perubahan.
nama pengguna	Nama pengguna pengguna yang terpengaruh oleh perubahan.
nama pengguna lama	Untuk tindakan ganti nama, nama pengguna asli. Untuk tindakan lain, bidang ini kosong.
tindakan	Tindakan yang terjadi. Nilai yang valid: <ul style="list-style-type: none"> • Mengubah • Buat • Jatuhkan • Ubah Nama

Nama kolom	Deskripsi
digunakan createdb	Jika benar (1), menunjukkan bahwa pengguna telah membuat izin database.
menggunakan ansuper	Jika benar (1), menunjukkan bahwa pengguna adalah superuser.
menggunakan ancatupd	Jika benar (1), menunjukkan bahwa pengguna dapat memperbarui katalog sistem.
valuntil	Tanggal kedaluwarsa kata sandi.
pid	ID Proses.
xid	ID Transaksi.
rekor waktu	Waktu di UTC kueri dimulai.

Kueri tampilan sistem [SYS_USERLOG](#) untuk menemukan informasi tambahan tentang perubahan pada pengguna. Tampilan ini mencakup data log dari Amazon Redshift Tanpa Server.

Log aktivitas pengguna

Log setiap query sebelum dijalankan pada database.

Nama kolom	Deskripsi
rekor waktu	Waktu peristiwa itu terjadi.
db	Nama basis data.
pengguna	Nama pengguna.
pid	ID proses yang terkait dengan pernyataan.
userid	ID pengguna.
xid	ID Transaksi.

Nama kolom	Deskripsi
query	Awalan LOG: diikuti oleh teks kueri, termasuk baris baru.

Mengaktifkan pencatatan log

Pencatatan audit tidak diaktifkan secara default di Amazon Redshift. Saat Anda mengaktifkan logging di klaster, Amazon Redshift mengeksport log ke Amazon CloudWatch, atau membuat dan mengunggah log ke Amazon S3, yang menangkap data dari saat pencatatan audit diaktifkan hingga saat ini. Setiap pembaruan logging merupakan kelanjutan dari log sebelumnya.

Audit logging ke CloudWatch atau ke Amazon S3 adalah proses opsional. Logging ke tabel sistem tidak opsional dan terjadi secara otomatis. Untuk informasi selengkapnya tentang pencatatan ke tabel sistem, lihat [Referensi Tabel Sistem](#) di Panduan Pengembang Database Amazon Redshift.

Log koneksi, log pengguna, dan log aktivitas pengguna diaktifkan bersama-sama dengan menggunakan Referensi API Amazon Redshift, atau AWS Command Line Interface (AWS CLI). AWS Management Console Untuk log aktivitas pengguna, Anda juga harus mengaktifkan parameter `enable_user_activity_logging` database. Jika Anda hanya mengaktifkan fitur audit logging, tetapi bukan parameter terkait, audit database mencatat informasi log hanya untuk log koneksi dan log pengguna, tetapi tidak untuk log aktivitas pengguna. `enable_user_activity_logging` Parameter tidak diaktifkan (`false`) secara default. Anda dapat mengaturnya `true` untuk mengaktifkan log aktivitas pengguna. Untuk informasi selengkapnya, lihat [Grup parameter Amazon Redshift](#).

Mengirim log audit ke Amazon CloudWatch

Saat Anda mengaktifkan login ke CloudWatch, Amazon Redshift mengeksport data log koneksi klaster, pengguna, dan aktivitas pengguna ke grup log Amazon Logs. CloudWatch Data log tidak berubah, dalam hal skema. CloudWatch dibangun untuk memantau aplikasi, dan Anda dapat menggunakannya untuk melakukan analisis real-time atau mengaturnya untuk mengambil tindakan. Anda juga dapat menggunakan Amazon CloudWatch Logs untuk menyimpan catatan log Anda dalam penyimpanan yang tahan lama.

Menggunakan CloudWatch untuk melihat log adalah alternatif yang disarankan untuk menyimpan file log di Amazon S3. Ini tidak memerlukan banyak konfigurasi, dan mungkin sesuai dengan persyaratan pemantauan Anda, terutama jika Anda sudah menggunakannya untuk memantau layanan dan aplikasi lain.

Grup log dan peristiwa log di Amazon CloudWatch

Setelah memilih log Amazon Redshift mana yang akan diekspor, Anda dapat memantau peristiwa log di Amazon CloudWatch Logs. Grup log baru secara otomatis dibuat untuk Amazon Redshift Tanpa Server, di bawah awalan berikut, yang `log_type` mewakili jenis log.

```
/aws/redshift/cluster/<cluster_name>/<log_type>
```

Misalnya, jika Anda memilih untuk mengekspor log koneksi, data log disimpan dalam grup log berikut.

```
/aws/redshift/cluster/cluster1/connectionlog
```

Peristiwa log diekspor ke grup log menggunakan aliran log. Untuk mencari informasi dalam peristiwa log untuk titik akhir tanpa server Anda, gunakan konsol Amazon CloudWatch Logs, API, atau Amazon CloudWatch Logs. AWS CLI Untuk informasi tentang mencari dan memfilter data log, lihat [Membuat metrik dari peristiwa log menggunakan filter](#).

Di CloudWatch, Anda dapat mencari data log Anda dengan sintaks kueri yang menyediakan perincian dan fleksibilitas. Untuk informasi selengkapnya, lihat [sintaks kueri Wawasan CloudWatch Log](#).

Migrasi ke pencatatan CloudWatch audit Amazon

Dalam kasus apa pun di mana Anda mengirim log ke Amazon S3 dan Anda mengubah konfigurasi, misalnya untuk mengirim log ke CloudWatch, log yang tetap di Amazon S3 tidak terpengaruh. Anda masih dapat menanyakan data log di ember Amazon S3 di mana ia berada.

Mengelola file log di Amazon S3

Jumlah dan ukuran file log Amazon Redshift di Amazon S3 sangat bergantung pada aktivitas di cluster Anda. Jika Anda memiliki cluster aktif yang menghasilkan sejumlah besar log, Amazon Redshift mungkin menghasilkan file log lebih sering. Anda mungkin memiliki serangkaian file log untuk jenis aktivitas yang sama, seperti memiliki beberapa log koneksi dalam jam yang sama.

Saat Amazon Redshift menggunakan Amazon S3 untuk menyimpan log, Anda dikenakan biaya untuk penyimpanan yang Anda gunakan di Amazon S3. Sebelum Anda mengonfigurasi logging ke Amazon S3, rencanakan berapa lama Anda perlu menyimpan file log. Sebagai bagian dari ini, tentukan kapan file log dapat dihapus atau diarsipkan, berdasarkan kebutuhan audit Anda. Paket yang Anda buat sangat bergantung pada jenis data yang Anda simpan, seperti data yang tunduk pada kepatuhan

atau persyaratan peraturan. Untuk informasi selengkapnya tentang harga Amazon S3, buka [Harga Amazon Simple Storage Service \(S3\)](#).

Batasan saat Anda mengaktifkan logging ke Amazon S3

Audit logging memiliki kendala sebagai berikut:

- Anda hanya dapat menggunakan enkripsi kunci terkelola Amazon S3 (SSE-S3) (AES-256).
- Bucket Amazon S3 harus mematikan fitur Kunci Objek S3.

Izin bucket untuk pencatatan audit Amazon Redshift

Saat Anda mengaktifkan logging ke Amazon S3, Amazon Redshift mengumpulkan informasi pencatatan dan mengunggahnya ke file log yang disimpan di Amazon S3. Anda dapat menggunakan ember yang sudah ada atau ember baru. Amazon Redshift memerlukan izin IAM berikut ke bucket:

- `s3:GetBucketACL` Layanan ini memerlukan izin baca ke bucket Amazon S3 sehingga dapat mengidentifikasi pemilik bucket.
- `s3:PutObject` Layanan ini memerlukan izin objek put untuk mengunggah log. Selain itu, peran pengguna atau IAM yang mengaktifkan logging harus memiliki `s3:PutObject` izin ke bucket Amazon S3. Setiap kali log diunggah, layanan menentukan apakah pemilik bucket saat ini cocok dengan pemilik bucket pada saat logging diaktifkan. Jika pemilik ini tidak cocok, Anda menerima kesalahan.

Jika, saat mengaktifkan pencatatan audit, Anda memilih opsi untuk membuat bucket baru, izin yang benar akan diterapkan padanya. Namun, jika Anda membuat bucket sendiri di Amazon S3, atau menggunakan bucket yang sudah ada, pastikan untuk menambahkan kebijakan bucket yang menyertakan nama bucket. Log dikirimkan menggunakan kredensi prinsipal layanan. *Untuk sebagian besar Wilayah AWS, Anda menambahkan nama utama layanan Redshift, `redshift.amazonaws.com`.*

Kebijakan bucket menggunakan format berikut. `ServiceName` dan `BucketName` merupakan placeholder untuk nilai-nilai Anda sendiri. Tentukan juga tindakan dan sumber daya terkait dalam kebijakan bucket.

```
{
  "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/*"
    ]
  }
]
}

```

Contoh berikut adalah kebijakan ember untuk Wilayah AS Timur (Virginia N.) dan ember bernama `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/*"
      ]
    }
  ]
}

```

Wilayah yang tidak diaktifkan secara default, juga dikenal sebagai Wilayah “keikutsertaan”, memerlukan nama utama layanan khusus Wilayah. Untuk ini, nama prinsipal layanan mencakup

wilayah, dalam format. `redshift.region.amazonaws.com` Misalnya, `redshift.ap-east-1.amazonaws.com` untuk Wilayah Asia Pasifik (Hong Kong). Untuk daftar Wilayah yang tidak diaktifkan secara default, lihat [Mengelola Wilayah AWS](#) di Referensi Umum AWS.

Note

Nama utama layanan khusus Wilayah sesuai dengan Wilayah tempat cluster berada.

Praktik terbaik untuk file log

Saat Redshift mengunggah file log ke Amazon S3, file besar dapat diunggah menjadi beberapa bagian. Jika unggahan multibagian tidak berhasil, sebagian file dapat tetap berada di bucket Amazon S3. Hal ini dapat mengakibatkan biaya penyimpanan tambahan, jadi penting untuk memahami apa yang terjadi ketika unggahan multipart gagal. Untuk penjelasan rinci tentang unggahan multibagian untuk log audit, lihat [Mengunggah dan menyalin objek menggunakan unggahan multibagian dan membatalkan unggahan multibagian](#).

Untuk informasi selengkapnya tentang membuat bucket S3 dan menambahkan kebijakan bucket, lihat [Membuat Bucket](#) dan [Mengedit Izin Bucket di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Struktur bucket untuk pencatatan audit Amazon Redshift

Secara default, Amazon Redshift mengatur file log di bucket Amazon S3 dengan menggunakan bucket dan struktur objek berikut:

```
AWSLogs/AccountID/ServiceName/Region/Year/Month/Day/AccountID_ServiceName_Region
```

```
Contohnya adalah: AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz
```

Jika Anda memberikan awalan kunci Amazon S3, letakkan awalan di awal kunci.

```
Misalnya, jika Anda menentukan awalan myprefix: myprefix/AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz
```


Awalan key Amazon S3 tidak dapat melebihi 512 karakter. Itu tidak dapat berisi spasi (), tanda kutip ganda (“), tanda kutip tunggal (’), garis miring terbalik (\). Ada juga sejumlah karakter khusus dan karakter kontrol yang tidak diizinkan. Kode heksadesimal untuk karakter ini adalah sebagai berikut:

- x00 ke x20
- x22
- x27
- x5c
- x7f atau lebih besar

Memecahkan masalah pencatatan audit Amazon Redshift di Amazon S3

Pencatatan audit Amazon Redshift dapat terganggu karena alasan berikut:

- Amazon Redshift tidak memiliki izin untuk mengunggah log ke bucket Amazon S3. Verifikasi bahwa bucket dikonfigurasi dengan kebijakan IAM yang benar. Untuk informasi selengkapnya, lihat [Izin bucket untuk pencatatan audit Amazon Redshift](#).
- Pemilik ember berubah. Saat Amazon Redshift mengunggah log, Amazon Redshift memverifikasi bahwa pemilik bucket sama seperti saat logging diaktifkan. Jika pemilik bucket telah berubah, Amazon Redshift tidak dapat mengunggah log hingga Anda mengonfigurasi bucket lain yang akan digunakan untuk pencatatan audit.
- Ember tidak dapat ditemukan. Jika bucket dihapus di Amazon S3, Amazon Redshift tidak dapat mengunggah log. Anda harus membuat ulang bucket atau mengonfigurasi Amazon Redshift untuk mengunggah log ke bucket lain.

Mencatat panggilan Amazon Redshift API dengan AWS CloudTrail

Amazon Redshift terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon Redshift. CloudTrail menangkap semua panggilan API untuk Amazon Redshift sebagai peristiwa. Untuk informasi selengkapnya tentang integrasi Amazon Redshift dengan AWS CloudTrail, lihat [Logging with CloudTrail](#).

Anda dapat menggunakan CloudTrail secara independen dari atau selain pencatatan audit database Amazon Redshift.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

Mengkonfigurasi audit menggunakan konsol

Konfigurasi Amazon Redshift untuk mengekspor data log audit. Log dapat diekspor ke CloudWatch, atau sebagai file ke ember Amazon S3.

Mengaktifkan pencatatan audit menggunakan konsol

Langkah-langkah konsol

Untuk mengaktifkan pencatatan audit untuk klaster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, lalu pilih cluster yang ingin Anda perbarui.
3. Pilih tab Properti. Pada panel konfigurasi Database, pilih Edit, lalu Edit pencatatan audit.
4. Pada halaman Edit pencatatan audit, pilih Aktifkan dan pilih bucket S3 atau CloudWatch. Kami merekomendasikan penggunaan CloudWatch karena administrasi mudah dan memiliki fitur yang berguna untuk visualisasi data.
5. Pilih log mana yang akan diekspor.
6. Untuk menyimpan pilihan Anda, pilih Simpan perubahan.

Mengonfigurasi logging dengan menggunakan API Amazon AWS CLI Redshift dan Amazon

Anda dapat menggunakan operasi Amazon Redshift CLI berikut untuk mengonfigurasi pencatatan audit:

- [describe-logging-status](#)
- [nonaktifkan-logging](#)
- [aktifkan-logging](#)

Anda dapat menggunakan operasi Amazon Redshift API berikut untuk mengonfigurasi pencatatan audit:

- [DescribeLoggingStatus](#)
- [DisableLogging](#)
- [EnableLogging](#)

Logging dengan CloudTrail

Pencatatan panggilan dengan AWS CloudTrail

Amazon Redshift, berbagi data, Amazon Redshift Serverless, Amazon Redshift Data API, dan editor kueri v2 semuanya terintegrasi dengannya. AWS CloudTrail CloudTrail adalah layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon Redshift. CloudTrail menangkap semua panggilan API untuk Amazon Redshift sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Redshift dan panggilan kode ke operasi Redshift.

Jika Anda membuat CloudTrail jejak, Anda dapat mengirimkan CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk Redshift. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan hal-hal tertentu. Ini termasuk permintaan yang dibuat untuk Redshift, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Anda dapat menggunakan CloudTrail secara independen dari atau selain pencatatan audit database Amazon Redshift.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

Bekerja dengan informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS. Untuk informasi selengkapnya, lihat [Melihat CloudTrail Acara dengan Riwayat Acara](#) di Panduan AWS CloudTrail Pengguna.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Redshift, buat jejak. CloudTrail menggunakan jejak untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, pelajari topik berikut di Panduan Pengguna AWS CloudTrail:

- [Ikhtisar Pembuatan Jejak](#)
- [CloudTrail Layanan dan Integrasi yang Didukung](#)
- [Mengkonfigurasi Notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima File CloudTrail Log dari Beberapa Wilayah](#) dan [Menerima File CloudTrail Log dari Beberapa Akun](#)

Semua tindakan Amazon Redshift, Amazon Redshift Serverless, Data API, berbagi data, dan editor kueri v2 dicatat oleh CloudTrail. Misalnya, panggilan ke `AuthorizeDataShare`, `CreateNamespaceExecuteStatement`, dan `CreateConnection` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut:

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan.
- Apakah permintaan dibuat oleh layanan AWS lain.

Untuk informasi selengkapnya, lihat [Elemen CloudTrail UserIdentity](#) di AWS CloudTrail Panduan Pengguna.

Memahami entri file log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Sebuah peristiwa mewakili satu permintaan dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh Data Pergeseran Merah Amazon

Contoh berikut menunjukkan entri CloudTrail log yang menggambarkan `AuthorizeDataShare` operasi.

```
{  
  "eventVersion": "1.08",
```

```

"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
  "arn": "arn:aws:sts::111122223333:user/janedoe",
  "accountId": "111122223333",
  "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
      "arn": "arn:aws:sts::111122223333:user/janedoe",
      "accountId": "111122223333",
      "userName": "janedoe"
    },
    "attributes": {
      "creationDate": "2021-08-02T23:40:45Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2021-08-02T23:40:58Z",
"eventSource": "redshift.amazonaws.com",
"eventName": "AuthorizeDataShare",
"awsRegion": "us-east-1",
"sourceIPAddress": "3.227.36.75",
"userAgent": "aws-cli/1.18.118 Python/3.6.10
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 boto3/1.17.41",
"requestParameters": {
  "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
  "consumerIdentifier": "555555555555"
},
"responseElements": {
  "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
  "producerNamespaceArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
  "producerArn": "arn:aws:redshift:us-
east-1:111122223333:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
  "allowPubliclyAccessibleConsumers": true,
  "dataShareAssociations": [
    {
      "consumerIdentifier": "555555555555",
      "status": "AUTHORIZED",

```

```

        "createdDate": "Aug 2, 2021 11:40:56 PM",
        "statusChangeDate": "Aug 2, 2021 11:40:57 PM"
    }
]
},
"requestID": "87ee1c99-9e41-42be-a5c4-00495f928422",
"eventID": "03a3d818-37c8-46a6-aad5-0151803bdb09",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}

```

Contoh Tanpa Server Amazon Redshift

Amazon Redshift Serverless terintegrasi AWS CloudTrail untuk memberikan catatan tindakan yang diambil di Amazon Redshift Tanpa Server. CloudTrail menangkap semua panggilan API untuk Amazon Redshift Serverless sebagai peristiwa. [Untuk informasi selengkapnya tentang fitur Amazon Redshift Tanpa Server, lihat ikhtisar fitur Amazon Redshift Tanpa Server.](#)

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateNamespace tindakan.

```

{
  "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",
}

```

Contoh API Data Amazon Redshift

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan ExecuteStatement tindakan.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
    "arn": "arn:aws:sts::123456789012:user/janedoe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "janedoe"
  },
  "eventTime": "2020-08-19T17:55:59Z",
  "eventSource": "redshift-data.amazonaws.com",
  "eventName": "ExecuteStatement",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.18.118 Python/3.6.10
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 boto3/1.17.41",
  "requestParameters": {
    "clusterIdentifier": "example-cluster-identifier",
    "database": "example-database-name",
    "dbUser": "example_db_user_name",
    "sql": "****OMITTED****"
  },
  "responseElements": {
    "clusterIdentifier": "example-cluster-identifier",
    "createdAt": "Aug 19, 2020 5:55:58 PM",
    "database": "example-database-name",
    "dbUser": "example_db_user_name",
    "id": "5c52b37b-9e07-40c1-98de-12ccd1419be7"
  },
  "requestID": "00c924d3-652e-4939-8a7a-cd0612eeb8ac",
  "eventID": "c1fb7076-102f-43e5-9ec9-40820bcc1175",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan ExecuteStatement tindakan yang menunjukkan clientToken digunakan untuk idempotensi.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
```



```

    "type": "IAMUser",
    "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
    "arn": "arn:aws:sts::123456789012:user/janedoe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "janedoe"
  },
  "eventTime": "2020-08-19T17:55:59Z",
  "eventSource": "redshift-data.amazonaws.com",
  "eventName": "ExecuteStatement",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.18.118 Python/3.6.10
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 boto3/1.17.41",
  "requestParameters": {
    "clusterIdentifier": "example-cluster-identifier",
    "database": "example-database-name",
    "dbUser": "example_db_user_name",
    "sql": "***OMITTED***",
    "clientToken": "32db2e10-69ac-4534-b3fc-a191052616ce"
  },
  "responseElements": {
    "clusterIdentifier": "example-cluster-identifier",
    "createdAt": "Aug 19, 2020 5:55:58 PM",
    "database": "example-database-name",
    "dbUser": "example_db_user_name",
    "id": "5c52b37b-9e07-40c1-98de-12ccd1419be7"
  },
  "requestID": "00c924d3-652e-4939-8a7a-cd0612eeb8ac",
  "eventID": "c1fb7076-102f-43e5-9ec9-40820bcc1175",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}

```

Contoh editor kueri Amazon Redshift v2

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateConnection tindakan.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",

```

```

    "principalId": "AAKEOFPINEXAMPLE:session",
    "arn": "arn:aws:sts::123456789012:assumed-role/MyRole/session",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAKEOFPINEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/MyRole",
        "accountId": "123456789012",
        "userName": "MyRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-09-21T17:19:02Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-09-21T22:22:05Z",
  "eventSource": "sqlworkbench.amazonaws.com",
  "eventName": "CreateConnection",
  "awsRegion": "ca-central-1",
  "sourceIPAddress": "192.2.0.2",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0)
Gecko/20100101 Firefox/102.0",
  "requestParameters": {
    "password": "****",
    "databaseName": "****",
    "isServerless": false,
    "name": "****",
    "host": "redshift-cluster-2.c8robpbxvbf9.ca-central-1.redshift.amazonaws.com",
    "authenticationType": "****",
    "clusterId": "redshift-cluster-2",
    "username": "****",
    "tags": {
      "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
    }
  }
},
"responseElements": {
  "result": true,
  "code": "",
  "data": {

```

```

      "id": "arn:aws:sqlworkbench:ca-central-1:123456789012:connection/ce56b1be-
dd65-4bfb-8b17-12345123456",
      "name": "****",
      "authenticationType": "****",
      "databaseName": "****",
      "secretArn": "arn:aws:secretsmanager:ca-
central-1:123456789012:secret:sqlworkbench!7da333b4-9a07-4917-b1dc-12345123456-qTCoFm",
      "clusterId": "redshift-cluster-2",
      "dbUser": "****",
      "userSettings": "****",
      "recordDate": "2022-09-21 22:22:05",
      "updatedAt": "2022-09-21 22:22:05",
      "accountId": "123456789012",
      "tags": {
        "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
      },
      "isServerless": false
    }
  },
  "requestID": "9b82f483-9c03-4cdd-bb49-a7009e7da714",
  "eventID": "a7cdd442-e92f-46a2-bc82-2325588d41c3",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management"
}

```

ID akun Amazon Redshift di log AWS CloudTrail

Saat Amazon Redshift memanggil AWS layanan lain untuk Anda, panggilan tersebut dicatat dengan ID akun milik Amazon Redshift. Itu tidak login dengan ID akun Anda. Misalnya, Amazon Redshift memanggil AWS Key Management Service (AWS KMS) operasi seperti `CreateGrant`, `DecryptEncrypt`, dan `RetireGrant` mengelola enkripsi di klaster Anda. Dalam hal ini, panggilan dicatat dengan AWS CloudTrail menggunakan ID akun Amazon Redshift.

Amazon Redshift menggunakan ID akun di tabel berikut saat memanggil layanan lain AWS.

Wilayah	Wilayah	account-id
Wilayah US East (N. Virginia)	us-east-1	368064434614

Wilayah	Wilayah	account-id
Wilayah AS Timur (Ohio)	us-east-2	790247189693
Wilayah AS Barat (California Utara)	us-west-1	703715109447
Wilayah AS Barat (Oregon)	us-west-2	473191095985
Wilayah Afrika (Cape Town)	af-south-1	420376844563
Wilayah Asia Pacific (Hong Kong)	ap-east-1	651179539253
Wilayah Asia Pasifik (Hyderabad)	ap-south-2	297058826802
Wilayah Asia Pasifik (Jakarta)	ap-southeast-3	623197973179
Wilayah Asia Pasifik (Melbourne)	ap-southeast-4	945512339897
Wilayah Asia Pasifik (Mumbai)	ap-south-1	408097707231
Wilayah Asia Pasifik (Osaka)	ap-northeast-3	398671365691
Wilayah Asia Pasifik (Seoul)	ap-northeast-2	713597048934
Wilayah Asia Pacific (Singapore)	ap-southeast-1	960118270566
Wilayah Asia Pasifik (Sydney)	ap-southeast-2	485979073181
Wilayah Asia Pasifik (Tokyo)	ap-northeast-1	615915377779
Wilayah Kanada (Pusat)	ca-central-1	764870610256
Wilayah Kanada Barat (Calgary)	ca-west-1	830903446466
Wilayah Eropa (Frankfurt)	eu-central-1	434091160558
Wilayah Eropa (Irlandia)	eu-west-1	246478207311

Wilayah	Wilayah	account-id
Wilayah Eropa (London)	eu-west-2	885798887673
Wilayah Eropa (Milan)	eu-south-1	041313461515
Wilayah Eropa (Paris)	eu-west-3	694668203235
Wilayah Eropa (Spanyol)	eu-south-2	028811157404
Wilayah Eropa (Stockholm)	eu-north-1	553461782468
Wilayah Eropa (Zürich)	eu-central-2	668912161003
Wilayah Israel (Tel Aviv)	il-central-1	901883065212
Wilayah Timur Tengah (Bahrain)	me-south-1	051362938876
Wilayah Timur Tengah (UEA)	me-central-1	595013617770
Wilayah Amerika Selatan (Sao Paulo)	sa-east-1	392442076723

Contoh berikut menunjukkan entri CloudTrail log untuk operasi AWS KMS Dekripsi yang dipanggil oleh Amazon Redshift.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AR0AI5QPCMKLTL4VHFCYY:i-0f53e22dbe5df8a89",
    "arn": "arn:aws:sts::790247189693:assumed-role/prod-23264-role-wp/i-0f53e22dbe5df8a89",
    "accountId": "790247189693",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2017-03-03T16:24:54Z"
      }
    }
  },
```

```

        "sessionIssuer": {
            "type": "Role",
            "principalId": "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"
}

```

Validasi Kepatuhan untuk Amazon Redshift

Auditor pihak ke 3 menilai keamanan dan kepatuhan Amazon Redshift sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk daftar layanan AWS dalam cakupan program kepatuhan tertentu, lihat [Layanan AWS dalam Cakupan berdasarkan Program Kepatuhan](#). Untuk informasi umum, lihat [Program Kepatuhan AWS](#).

Anda bisa mengunduh laporan audit pihak ke tiga menggunakan AWS Artifact. Untuk informasi lebih lanjut, lihat [Mengunduh laporan di AWS Artifact](#).

Tanggung jawab kepatuhan Anda ketika menggunakan Amazon Redshift ditentukan oleh sensitivitas data Anda, tujuan kepatuhan organisasi Anda, serta peraturan perundangan yang berlaku. Jika penggunaan Amazon Redshift Anda tunduk pada kepatuhan standar seperti HIPAA, PCI, atau FedRAMP, AWS menyediakan sumber daya untuk membantu:

- [Panduan Quick Start Keamanan dan Kepatuhan](#) yang membahas pertimbangan arsitektural dan langkah-langkah untuk men-deploy lingkungan dasar yang berfokus pada keamanan dan kepatuhan di AWS.
- [Laporan resmi perancangan untuk keamanan dan kepatuhan HIPAA](#), yang menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang mematuhi HIPAA.
- [AWS Sumber Daya Kepatuhan](#), buku kerja, dan panduan yang mungkin berlaku untuk industri dan lokasi Anda.
- [AWS Config](#), AWS layanan, dapat menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub](#), AWS layanan, menyediakan tampilan komprehensif status keamanan Anda dalam AWS yang membantu Anda memeriksa kepatuhan terhadap standar dan praktik terbaik industri. Security Hub menggunakan kontrol keamanan untuk mengevaluasi konfigurasi sumber daya dan standar keamanan untuk membantu Anda mematuhi berbagai kerangka kerja kepatuhan. Untuk informasi selengkapnya tentang penggunaan Security Hub untuk mengevaluasi sumber daya [Amazon Redshift](#), lihat [kontrol Amazon Redshift](#) di Panduan AWS Security Hub Pengguna.

Dokumen Kepatuhan dan keamanan berikut mencakup Amazon Redshift dan tersedia sesuai permintaan AWS Artifact. Untuk informasi selengkapnya, lihat [AWS Artifact](#).

- Katalog Kontrol Kepatuhan Komputasi Cloud (C5)
- ISO 27001:2013 Pernyataan Penerapan (SoA)

- Sertifikasi ISO 27001:2013
- ISO 27017:2015 Pernyataan Penerapan (SoA)
- Sertifikasi ISO 27017:2015
- ISO 27018:2015 Pernyataan Penerapan (SoA)
- Sertifikasi ISO 27018:2014
- Sertifikasi ISO 9001:2015
- Pengesahan Kepatuhan (AOC) PCI DSS dan Ringkasan Tanggung Jawab
- Laporan Kontrol Organisasi Layanan (SOC) 1
- Laporan Kontrol Organisasi Layanan (SOC) 2
- Laporan Kontrol Organisasi Layanan (SOC) 2 untuk Kerahasiaan

Ketahanan di Amazon Redshift

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Availability Zones (AZ). AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi yang terhubung dengan jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Availability Zone, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara Availability Zone tanpa gangguan. Zona Ketersediaan lebih tersedia, toleran terhadap kegagalan, dan bisa diskalakan jika dibandingkan dengan satu infrastruktur pusat data tradisional atau beberapa infrastruktur pusat data.

Hampir semua AWS Wilayah memiliki beberapa Availability Zone dan pusat data. Anda dapat menerapkan aplikasi Anda di beberapa Zona Ketersediaan di Wilayah yang sama untuk toleransi kesalahan dan latensi rendah.

Untuk memindahkan klaster ke Availability Zone lain tanpa kehilangan data atau perubahan pada aplikasi Anda, Anda dapat mengatur relokasi untuk klaster Anda. Dengan relokasi, Anda dapat melanjutkan operasi ketika ada gangguan layanan pada klaster Anda dengan dampak minimal. Saat relokasi klaster diaktifkan, Amazon Redshift mungkin memilih untuk memindahkan klaster dalam beberapa situasi. Untuk informasi lebih lanjut tentang relokasi di Amazon Redshift, lihat [Merelokasi klaster Anda](#).

Dalam skenario kegagalan di mana peristiwa tak terduga terjadi di Availability Zone, Anda dapat menyiapkan penerapan beberapa Availability Zone (Multi-AZ) untuk memastikan bahwa gudang data Amazon Redshift Anda dapat terus beroperasi. Amazon Redshift menerapkan sumber daya

komputasi yang sama di dua Availability Zone yang dapat diakses melalui satu titik akhir. Jika terjadi kegagalan Availability Zone secara keseluruhan, sumber daya komputasi yang tersisa di Availability Zone kedua akan tersedia untuk melanjutkan pemrosesan beban kerja. Untuk informasi selengkapnya tentang penerapan Multi-AZ, lihat [Mengkonfigurasi penyebaran Multi-AZ](#).

Untuk informasi lebih lanjut tentang AWS Wilayah dan Availability Zones, lihat [Infrastruktur AWS global](#).

Keamanan infrastruktur di Amazon Redshift

Sebagai layanan terkelola, Amazon Redshift dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan](#) Infrastruktur dalam Kerangka Kerja Pilar Keamanan yang AWS Diarsiteksikan dengan Baik.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Amazon Redshift melalui jaringan. Klien harus mendukung hal berikut:

- Transport Layer Security (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau, Anda bisa menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara untuk menandatangani permintaan.

Isolasi jaringan

Cloud pribadi virtual (VPC) berdasarkan layanan Amazon VPC adalah jaringan pribadi Anda yang terisolasi secara logis di AWS Cloud. Anda dapat menerapkan kluster Amazon Redshift dalam VPC dengan mengambil langkah-langkah berikut:

- Buat VPC di AWS Wilayah. Untuk informasi lebih lanjut, lihat [Apa itu Amazon VPC?](#) di Panduan Pengguna Amazon VPC.
- Buat dua atau lebih subnet VPC pribadi. Untuk informasi lebih lanjut, lihat [VPC dan subnet](#) di Panduan Pengguna Amazon VPC.

- Menerapkan klaster Amazon Redshift. Untuk informasi selengkapnya, lihat [Grup subnet klaster Amazon Redshift](#).

Klaster Amazon Redshift dikunci secara default pada saat penyediaan. Untuk mengizinkan lalu lintas jaringan masuk dari klien Amazon Redshift, kaitkan grup keamanan VPC dengan klaster Amazon Redshift. Untuk informasi selengkapnya, lihat [Grup subnet klaster Amazon Redshift](#).

Untuk mengizinkan lalu lintas hanya ke atau dari rentang alamat IP tertentu, perbarui grup keamanan dengan VPC Anda. Contohnya adalah mengizinkan lalu lintas hanya dari atau ke jaringan perusahaan Anda.

Saat mengonfigurasi daftar kontrol akses jaringan yang terkait dengan subnet klaster Amazon Redshift Anda diberi tag, pastikan rentang S3 CIDR AWS Wilayah masing-masing ditambahkan ke daftar yang diizinkan untuk aturan ingress dan egress. Dengan demikian, Anda dapat menjalankan operasi berbasis S3 seperti Redshift Spectrum, COPY, dan UNLOAD tanpa gangguan apa pun.

Perintah contoh berikut mengurai respons JSON untuk semua alamat IPv4 yang digunakan di Amazon S3 di Wilayah us-east-1.

```
curl https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] |
  select(.region=="us-east-1") | select(.service=="S3") | .ip_prefix'

54.231.0.0/17

52.92.16.0/20

52.216.0.0/15
```

Untuk petunjuk tentang cara mendapatkan rentang IP S3 untuk wilayah tertentu, lihat [rentang alamat AWS IP](#).

Amazon Redshift mendukung penerapan klaster ke dalam VPC penyewaan khusus. Untuk informasi selengkapnya, lihat [Instans khusus](#) di Panduan Pengguna Amazon EC2.

Grup keamanan klaster Amazon Redshift

Saat Anda menyediakan klaster Amazon Redshift, klaster tersebut dikunci secara default sehingga tidak ada yang memiliki akses ke sana. Untuk memberi pengguna lain akses masuk ke klaster Amazon Redshift, Anda mengaitkan klaster dengan grup keamanan. Jika Anda menggunakan

platform EC2-VPC, Anda dapat menggunakan grup keamanan Amazon VPC yang ada atau menentukan yang baru dan kemudian mengaitkannya dengan cluster. Untuk informasi lebih lanjut tentang mengelola cluster pada platform EC2-VPC, lihat [Mengelola cluster dalam VPC](#)

Menghubungkan ke Amazon Redshift menggunakan titik akhir VPC antarmuka

Anda dapat terhubung langsung ke layanan Amazon Redshift API menggunakan antarmuka VPC endpoint (AWS PrivateLink) di virtual private cloud (VPC) Anda alih-alih terhubung melalui internet. Untuk informasi tentang tindakan Amazon Redshift API, lihat [Tindakan](#) di Referensi API Amazon Redshift. Untuk informasi selengkapnya AWS PrivateLink, lihat [Titik akhir VPC Antarmuka \(AWS PrivateLink\) di Panduan](#) Pengguna Amazon VPC. Perhatikan bahwa koneksi JDBC/ODBC ke cluster bukan bagian dari layanan Amazon Redshift API.

Saat Anda menggunakan titik akhir VPC antarmuka, komunikasi antara VPC dan Amazon Redshift dilakukan sepenuhnya di dalam jaringan, yang dapat memberikan keamanan AWS yang lebih besar. Setiap titik akhir VPC diwakili oleh satu atau lebih antarmuka jaringan elastis dengan alamat IP pribadi di subnet VPC Anda. Untuk informasi selengkapnya tentang antarmuka jaringan elastis, lihat [Antarmuka jaringan elastis](#) dalam Panduan Pengguna Amazon EC2.

Titik akhir VPC antarmuka menghubungkan VPC Anda langsung ke Amazon Redshift. Itu tidak menggunakan gateway internet, perangkat terjemahan alamat jaringan (NAT), koneksi jaringan pribadi virtual (VPN), atau AWS Direct Connect koneksi. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan Amazon Redshift API.

Untuk menggunakan Amazon Redshift melalui VPC Anda, Anda memiliki dua opsi. Salah satunya adalah terhubung dari instance yang ada di dalam VPC Anda. Yang lainnya adalah menghubungkan jaringan pribadi Anda ke VPC Anda dengan menggunakan AWS VPN opsi atau. AWS Direct Connect Untuk informasi selengkapnya tentang AWS VPN opsi, lihat [Koneksi VPN](#) di Panduan Pengguna Amazon VPC. Untuk informasi tentang AWS Direct Connect, lihat [Membuat hubungan](#) di Panduan Pengguna AWS Direct Connect .

Anda dapat membuat titik akhir VPC antarmuka untuk terhubung ke Amazon Redshift menggunakan perintah `or ()`. AWS Management Console AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat [Membuat Titik Akhir Antarmuka](#).

Setelah Anda membuat antarmuka VPC endpoint, Anda dapat mengaktifkan nama host DNS pribadi untuk titik akhir. Jika Anda melakukannya, titik akhir Amazon Redshift (`https://redshift.Region.amazonaws.com`) default akan diselesaikan ke titik akhir VPC Anda.

Jika Anda tidak mengaktifkan nama host DNS pribadi, Amazon VPC menyediakan nama endpoint DNS yang dapat Anda gunakan dalam format berikut.

```
VPC_endpoint_ID.redshift.Region.vpce.amazonaws.com
```

Untuk informasi selengkapnya, lihat [Antarmuka VPC endpoint \(AWS PrivateLink\)](#) dalam Panduan Pengguna Amazon VPC.

Amazon Redshift mendukung panggilan ke semua [operasi API-nya](#) di dalam VPC Anda.

Anda dapat melampirkan kebijakan titik akhir VPC ke titik akhir VPC untuk mengontrol akses bagi prinsipal (IAM). AWS Identity and Access Management Anda juga dapat mengaitkan grup keamanan dengan titik akhir VPC untuk mengontrol akses masuk dan keluar berdasarkan asal dan tujuan lalu lintas jaringan. Contohnya adalah berbagai alamat IP. Untuk informasi selengkapnya, silakan lihat [Mengendalikan Akses ke Layanan dengan titik akhir VPC](#) dalam Panduan Pengguna Amazon VPC.

Membuat kebijakan titik akhir VPC untuk Amazon Redshift

Anda dapat membuat kebijakan untuk titik akhir VPC untuk Amazon Redshift untuk menentukan hal berikut:

- Kepala sekolah yang bisa atau tidak bisa melakukan tindakan
- Tindakan-tindakan yang dapat dilakukan
- Sumber daya yang dapat digunakan untuk mengambil tindakan

Untuk informasi selengkapnya, lihat [Mengendalikan akses ke layanan dengan VPC endpoint](#) di Panduan Pengguna Amazon VPC.

Berikut ini, Anda dapat menemukan contoh kebijakan titik akhir VPC.

Topik

- [Contoh: Kebijakan titik akhir VPC untuk menolak semua akses dari akun tertentu AWS](#)
- [Contoh: Kebijakan titik akhir VPC untuk mengizinkan akses VPC hanya ke peran IAM tertentu](#)
- [Contoh: Kebijakan titik akhir VPC untuk mengizinkan akses VPC hanya ke prinsipal IAM tertentu \(pengguna\)](#)
- [Contoh: Kebijakan titik akhir VPC untuk mengizinkan operasi Amazon Redshift hanya-baca](#)

- [Contoh: Kebijakan titik akhir VPC yang menolak akses ke cluster tertentu](#)

Contoh: Kebijakan titik akhir VPC untuk menolak semua akses dari akun tertentu AWS

Kebijakan titik akhir VPC berikut menyangkal *123456789012* semua akses AWS akun ke sumber daya menggunakan titik akhir ini.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "123456789012"
        ]
      }
    }
  ]
}
```

Contoh: Kebijakan titik akhir VPC untuk mengizinkan akses VPC hanya ke peran IAM tertentu

Kebijakan titik akhir VPC berikut memungkinkan akses penuh hanya ke peran `redshiftroleIAM` di akun `123456789012`. AWS Semua prinsipal IAM lain ditolak aksesnya menggunakan titik akhir.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
```

```

    "Resource": "*",
    "Principal": {
      "AWS": [
        "arn:aws:iam::123456789012:role/redshiftrrole"
      ]
    }
  ]
}

```

Ini hanya sampel. Dalam sebagian besar kasus penggunaan, kami menyarankan untuk melampirkan izin untuk tindakan tertentu untuk mempersempit ruang lingkup izin.

Contoh: Kebijakan titik akhir VPC untuk mengizinkan akses VPC hanya ke prinsipal IAM tertentu (pengguna)

Kebijakan titik akhir VPC berikut memungkinkan akses penuh hanya ke pengguna redshiftadminIAM di akun 123456789012. AWS Semua prinsipal IAM lain ditolak aksesnya menggunakan titik akhir.

```

{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/redshiftadmin"
        ]
      }
    }
  ]
}

```

Ini hanya sampel. Dalam sebagian besar kasus penggunaan, kami menyarankan untuk melampirkan izin ke peran sebelum menetapkan ke pengguna. Selain itu, sebaiknya gunakan tindakan khusus untuk mempersempit ruang lingkup izin.

Contoh: Kebijakan titik akhir VPC untuk mengizinkan operasi Amazon Redshift hanya-baca

Kebijakan titik akhir VPC berikut hanya mengizinkan AWS akun *123456789012* untuk melakukan tindakan Amazon Redshift yang ditentukan.

Tindakan yang ditentukan menyediakan akses hanya-baca yang setara untuk Amazon Redshift. Semua tindakan lain pada VPC ditolak untuk akun yang ditentukan. Juga, semua akun lain ditolak aksesnya. Untuk daftar tindakan Amazon Redshift, lihat [Tindakan, Sumber Daya, dan Kunci Kondisi untuk Amazon Redshift](#) di Panduan Pengguna IAM.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:DescribeAccountAttributes",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterVersions",
        "redshift:DescribeDefaultClusterParameters",
        "redshift:DescribeEventCategories",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeHsmClientCertificates",
        "redshift:DescribeHsmConfigurations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeQuery",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "redshift:DescribeResize",
        "redshift:DescribeSavedQueries",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeStorage",
        "redshift:DescribeTable",
        "redshift:DescribeTableRestoreStatus",
        "redshift:DescribeTags",
        "redshift:FetchResults",
        "redshift:GetReservedNodeExchangeOfferings"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Principal": {
        "AWS": [
```

```

        "123456789012"
    ]
}

```

Contoh: Kebijakan titik akhir VPC yang menolak akses ke cluster tertentu

Kebijakan titik akhir VPC berikut memungkinkan akses penuh untuk semua akun dan prinsipal. Pada saat yang sama, ia menolak akses apa pun untuk AWS akun *123456789012* ke tindakan yang dilakukan di cluster Amazon Redshift dengan ID cluster. *my-redshift-cluster* Tindakan Amazon Redshift lainnya yang tidak mendukung izin tingkat sumber daya untuk kluster masih diizinkan. Untuk daftar tindakan Amazon Redshift dan jenis sumber daya yang sesuai, lihat [Tindakan, Sumber Daya, dan Kunci Kondisi untuk Amazon Redshift](#) di Panduan Pengguna IAM.

```

{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-
cluster",
      "Principal": {
        "AWS": [
          "123456789012"
        ]
      }
    }
  ]
}

```


Analisis konfigurasi dan kelemahan di Amazon Redshift

AWS menangani tugas-tugas keamanan basic seperti sistem operasi tamu (OS) dan patching basis data, konfigurasi firewall, dan pemulihan bencana (DR). Prosedur ini telah ditinjau oleh pihak ketiga yang disertifikasi. Untuk informasi selengkapnya, lihat [Validasi Kepatuhan untuk Amazon Redshift](#), yang [Model tanggung jawab bersama](#), dan [Praktik Terbaik Keamanan, Identitas, dan Kepatuhan](#).

Amazon Redshift secara otomatis menerapkan upgrade dan menambal gudang data Anda sehingga Anda dapat fokus pada aplikasi Anda dan bukan pada administrasinya. Patch dan upgrade diterapkan selama jendela pemeliharaan dikonfigurasi. Untuk informasi selengkapnya, lihat [Jendela pemeliharaan](#).

Editor kueri Amazon Redshift v2 adalah AWS-dikelola aplikasi. Semua tambalan dan pembaruan diterapkan oleh AWS sesuai kebutuhan.

Tugas jaringan

Anda dapat melakukan tugas-tugas jaringan seperti menyesuaikan koneksi Anda ke database Redshift. Anda juga dapat melakukan tugas terkait DNS, seperti menyiapkan nama domain khusus. Tugas konfigurasi ini tersedia untuk Anda jika Anda memiliki klaster yang disediakan Amazon Redshift atau dengan grup kerja Amazon Redshift Tanpa Server.

Topik

- [Menggunakan nama domain khusus untuk koneksi klien](#)
- [Bekerja dengan titik akhir VPC yang dikelola Redshift](#)
- [Perutean VPC yang disempurnakan di Amazon Redshift](#)

Menggunakan nama domain khusus untuk koneksi klien

Anda dapat membuat nama domain khusus, juga dikenal sebagai URL khusus, untuk klaster Amazon Redshift dan grup kerja Amazon Redshift Tanpa Server. Ini adalah catatan easy-to-read DNS yang merutekan koneksi klien SQL ke titik akhir Anda. Anda dapat mengonfigurasinya untuk cluster atau workgroup yang ada kapan saja. Ini memberikan beberapa manfaat:

- Nama domain kustom adalah string yang lebih sederhana daripada URL default, yang biasanya mencakup nama cluster atau nama workgroup dan wilayah. Lebih mudah untuk mengingat dan menggunakan.
- Anda dapat dengan cepat merutekan lalu lintas ke klaster atau grup kerja baru dalam kasus fail-over, misalnya. Ini membuatnya sehingga klien tidak perlu membuat perubahan konfigurasi ketika mereka terhubung kembali. Koneksi dapat dialihkan kembali secara terpusat, dengan gangguan minimal.
- Anda dapat menghindari berbagi informasi pribadi seperti nama server di URL koneksi. Anda dapat menyembunyikannya di URL khusus.

Saat Anda menyiapkan nama domain khusus, menggunakan CNAME, tidak ada biaya tambahan dari Amazon Redshift. Anda mungkin ditagih dari penyedia DNS Anda untuk nama domain, jika Anda membuat yang baru, tetapi biaya ini biasanya kecil. Untuk informasi selengkapnya, lihat [Menyiapkan nama domain khusus](#).

Keamanan untuk nama domain khusus

Amazon Redshift atau Amazon Redshift Serverless memerlukan sertifikat Secure Sockets Layer (SSL) yang divalidasi untuk titik akhir kustom agar komunikasi tetap aman dan memverifikasi kepemilikan nama domain. Anda dapat menggunakan AWS Certificate Manager akun Anda dengan manajemen sertifikat AWS KMS key untuk aman. Validasi keamanan mencakup verifikasi nama host lengkap (`sslmode=verify-full`).

Memperbarui sertifikat

Perpanjangan sertifikat dikelola oleh Amazon Redshift hanya jika Anda memilih validasi DNS, bukan validasi email. Jika Anda menggunakan validasi email, Anda dapat menggunakan sertifikat, tetapi Anda harus melakukan perpanjangan sendiri, sebelum kedaluwarsa. Kami menyarankan Anda memilih validasi DNS untuk sertifikat Anda. Anda dapat memantau tanggal kedaluwarsa sertifikat yang diimpor di AWS Certificate Manager

Menyiapkan nama domain khusus

Menyiapkan nama domain khusus terdiri dari beberapa tugas: Ini termasuk mendaftarkan nama domain dengan penyedia DNS Anda dan membuat sertifikat. Setelah Anda melakukan pekerjaan ini, Anda mengonfigurasi nama domain khusus di konsol Amazon Redshift, atau di konsol Amazon Redshift Tanpa Server, atau mengonfigurasinya dengan perintah. AWS CLI Bagian berikut merinci langkah-langkahnya.

Daftarkan nama domain dan pilih sertifikat

Anda harus memiliki nama domain internet terdaftar untuk mengonfigurasi nama domain khusus di Amazon Redshift. Anda dapat mendaftarkan domain internet menggunakan Route 53, atau menggunakan penyedia pendaftaran domain pihak ketiga. Anda menyelesaikan tugas-tugas ini di luar konsol Amazon Redshift. Domain terdaftar adalah prasyarat untuk menyelesaikan prosedur yang tersisa untuk membuat domain khusus.

Note

Jika Anda menggunakan klaster yang disediakan, sebelum melakukan langkah-langkah untuk mengonfigurasi nama domain kustom, klaster tersebut harus diaktifkan relokasi. Untuk informasi selengkapnya, lihat [Merelokasi klaster Anda](#). Langkah ini tidak diperlukan untuk Amazon Redshift Serverless.

Nama domain kustom biasanya mencakup domain root dan subdomain, seperti `mycluster.example.com`. Untuk mengkonfigurasinya, lakukan langkah-langkah berikut:

Buat entri DNS CNAME untuk nama domain kustom Anda

1. Daftarkan domain root, misalnya `example.com`. Secara opsional, Anda dapat menggunakan domain yang ada. Nama kustom Anda dapat dibatasi oleh pembatasan karakter tertentu, atau validasi penamaan lainnya. Untuk informasi selengkapnya tentang mendaftarkan domain dengan Route 53, lihat [Mendaftarkan domain baru](#).
2. Tambahkan data CNAME DNS yang mengarahkan nama domain kustom Anda ke titik akhir Redshift untuk kluster atau grup kerja Anda. Anda dapat menemukan titik akhir di properti untuk kluster atau grup kerja, di konsol Redshift atau di konsol Amazon Redshift Tanpa Server. Salin URL JDBC yang tersedia di properti kluster atau grup kerja, di bawah Informasi umum. URL muncul seperti berikut:
 - Untuk cluster Amazon Redshift: `redshift-cluster-sample.abc123456.us-east-1.redshift.amazonaws.com`
 - Untuk grup kerja Amazon Redshift Tanpa Server: `endpoint-name.012345678901.us-east-1-dev.redshift-serverless-dev.amazonaws.com`

Jika URL memiliki awalan JDBC, hapus.

Note

Catatan DNS tergantung pada ketersediaan, karena setiap nama harus unik dan tersedia untuk digunakan dalam organisasi Anda.

Batasan


Ada beberapa batasan terkait pembuatan catatan CNAME untuk domain khusus:

- Membuat beberapa nama domain khusus untuk kluster yang disediakan atau grup kerja Amazon Redshift Tanpa Server yang sama tidak didukung. Anda hanya dapat mengaitkan satu catatan CNAME.
- Mengaitkan catatan CNAME dengan lebih dari satu kluster atau grup kerja tidak didukung. CNAME untuk setiap sumber daya Redshift harus unik.

Setelah mendaftarkan domain dan membuat catatan CNAME, Anda memilih sertifikat baru atau yang sudah ada. Anda melakukan langkah ini menggunakan AWS Certificate Manager:

Meminta sertifikat dari ACM untuk nama domain

1. Masuk ke AWS Management Console dan buka konsol ACM di <https://console.aws.amazon.com/acm/>.
2. Pilih Minta sertifikat.
3. Masukkan nama domain kustom Anda di bidang Nama domain.

 Note

Anda dapat menentukan banyak awalan, selain domain sertifikat, untuk menggunakan satu sertifikat untuk beberapa catatan domain khusus. Untuk mengilustrasikan, Anda dapat menggunakan catatan tambahan seperti `one.example.com`, `two.example.com`, atau catatan DNS wildcard seperti `*.example.com` dengan sertifikat yang sama.

4. Pilih Tinjau dan minta.
5. Pilih Konfirmasi dan minta.
6. Untuk permintaan yang valid, pemilik domain internet yang terdaftar harus menyetujui permintaan tersebut sebelum ACM mengeluarkan sertifikat. Pastikan status muncul sebagai Diterbitkan di konsol ACM, setelah Anda selesai dengan langkah-langkahnya.

Kami menyarankan Anda membuat [sertifikat tervalidasi DNS](#) yang memenuhi kelayakan untuk perpanjangan terkelola, yang tersedia dengan. AWS Certificate Manager Perpanjangan terkelola berarti ACM memperbarui sertifikat Anda secara otomatis atau mengiriminya pemberitahuan email saat kedaluwarsa mendekati. Untuk informasi selengkapnya, lihat [Perpanjangan terkelola untuk sertifikat ACM](#).

Buat domain kustom

Anda dapat menggunakan konsol Amazon Redshift atau Amazon Redshift Tanpa Server untuk membuat URL domain khusus Anda. Jika Anda belum mengonfigurasinya, properti nama domain kustom akan muncul sebagai tanda hubung (-) di bawah Informasi umum. Setelah membuat catatan CNAME dan sertifikat, Anda mengaitkan nama domain khusus untuk klaster atau grup kerja.

Untuk membuat asosiasi domain kustom, izin IAM berikut diperlukan:

- `redshift:CreateCustomDomainAssociation`— Anda dapat membatasi izin ke cluster tertentu dengan menambahkan ARN-nya.
- `redshiftServerless:CreateCustomDomainAssociation`— Anda dapat membatasi izin ke workgroup tertentu dengan menambahkan ARN nya.
- `acm:DescribeCertificate`

Sebagai praktik terbaik, kami menyarankan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).

Anda menetapkan nama domain kustom dengan melakukan langkah-langkah berikut.

1. Pilih klaster di konsol Redshift, atau workgroup di konsol Amazon Redshift Tanpa Server, dan pilih Buat nama domain khusus di bawah menu Tindakan. Dialog muncul.
2. Masukkan nama domain kustom.
3. Pilih ARN dari AWS Certificate Manager untuk Sertifikat ACM. Konfirmasikan perubahan Anda. Sesuai panduan dalam langkah-langkah yang Anda ambil untuk membuat sertifikat, sebaiknya Anda memilih sertifikat yang divalidasi DNS yang memenuhi syarat untuk perpanjangan terkelola. AWS Certificate Manager
4. Verifikasi di properti cluster bahwa nama domain kustom dan sertifikat domain kustom ARN diisi dengan entri Anda. Tanggal kedaluwarsa sertifikat domain kustom juga terdaftar.

Setelah domain kustom dikonfigurasi, menggunakan hanya `sslmode=verify-full` berfungsi untuk domain kustom yang baru. Itu tidak berfungsi untuk titik akhir default. Tetapi Anda masih dapat terhubung ke titik akhir default dengan menggunakan mode ssl lainnya, seperti `sslmode=verify-ca`

Note


Sebagai pengingat, [relokasi cluster](#) bukanlah prasyarat untuk mengonfigurasi fitur jaringan Redshift tambahan. Anda tidak perlu menyalakannya untuk mengaktifkan yang berikut:

- Menghubungkan dari VPC lintas akun atau lintas wilayah ke Redshift — Anda dapat terhubung dari satu AWS virtual private cloud (VPC) ke yang lain yang berisi database Redshift. Ini membuatnya lebih mudah untuk mengelola, misalnya, akses klien dari akun yang berbeda atau VPC, tanpa harus menyediakan akses VPC lokal ke identitas yang

terhubung ke database. Untuk informasi selengkapnya, lihat [Menghubungkan ke Amazon Redshift Tanpa Server dari titik akhir VPC Redshift](#) di akun atau wilayah lain.

- Menyiapkan nama domain khusus — Anda dapat membuat nama domain khusus, seperti yang dijelaskan dalam topik ini, untuk membuat nama titik akhir lebih relevan dan sederhana.

Mengganti nama cluster yang memiliki domain khusus yang ditetapkan, menggunakan konsol

 Note

Rangkaian langkah ini tidak berlaku untuk workgroup Amazon Redshift Serverless. Anda tidak dapat mengubah nama workgroup.

Untuk mengganti nama cluster yang memiliki nama domain khusus, izin `acm:DescribeCertificate` IAM diperlukan.

1. Buka konsol Amazon Redshift dan pilih cluster yang namanya ingin Anda ubah. Pilih Edit untuk mengedit properti cluster.
2. Edit pengenalan Cluster. Anda juga dapat mengubah properti lain untuk cluster. Lalu pilih Simpan Perubahan.
3. Setelah klaster diganti namanya, Anda harus memperbarui catatan DNS untuk mengubah entri CNAME untuk domain kustom untuk menunjuk ke titik akhir Amazon Redshift yang diperbarui.

Jelaskan asosiasi domain khusus, menggunakan perintah CLI

Gunakan perintah di bagian ini untuk mendapatkan daftar nama domain kustom yang terkait dengan klaster tertentu yang disediakan atau dengan workgroup Amazon Redshift Tanpa Server.

Anda memerlukan izin berikut:

- Untuk klaster yang disediakan: `redshift:DescribeCustomDomainAssociations`
- Untuk grup kerja Amazon Redshift Tanpa Server:
`redshiftServerless:ListCnameAssociations`

Sebagai praktik terbaik, kami menyarankan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).

Berikut ini menunjukkan contoh perintah untuk mencantumkan nama domain kustom untuk kluster Amazon Redshift tertentu:

```
aws redshift describe-custom-domain-associations --custom-domain-name customdomainname
```

Anda dapat menjalankan perintah ini ketika Anda memiliki nama domain kustom diaktifkan untuk menentukan nama domain kustom yang terkait dengan cluster. Untuk informasi selengkapnya tentang perintah CLI untuk menjelaskan asosiasi domain kustom, lihat [describe-custom-domain-associations](#)

Demikian pula, berikut ini menunjukkan contoh perintah untuk mencantumkan nama domain kustom untuk workgroup Amazon Redshift Serverless yang diberikan. Ada beberapa cara berbeda untuk ini. Anda hanya dapat memberikan nama domain khusus:

```
aws redshift-serverless list-custom-domain-associations --custom-domain-name customdomainname
```

Anda juga bisa mendapatkan asosiasi dengan hanya memberikan sertifikat ARN:

```
aws redshift-serverless list-custom-domain-associations --custom-domain-certificate-arn certificatearn
```

Anda dapat menjalankan perintah ini ketika Anda memiliki nama domain kustom diaktifkan untuk menentukan nama domain kustom yang terkait dengan workgroup. Anda juga dapat menjalankan perintah untuk mendapatkan properti dari asosiasi domain kustom. Untuk melakukan ini, Anda harus memberikan nama domain kustom dan nama workgroup sebagai parameter. Ini mengembalikan sertifikat ARN, nama workgroup, dan waktu kedaluwarsa sertifikat domain kustom:

```
aws redshift-serverless get-custom-domain-association --workgroup-name workgroupname --custom-domain-name customdomainname
```

[Untuk informasi selengkapnya tentang perintah referensi CLI yang tersedia untuk Amazon Redshift Serverless, lihat redshift-serverless.](#)

Mengaitkan domain kustom dengan sertifikat yang berbeda

Untuk mengubah asosiasi sertifikat untuk nama domain kustom, izin IAM berikut diperlukan:

- `redshift:ModifyCustomDomainAssociation`
- `acm:DescribeCertificate`

Sebagai praktik terbaik, kami menyarankan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).

Gunakan perintah berikut untuk mengaitkan domain kustom dengan sertifikat yang berbeda. `custom-domain-certificate-arn` Argumen `--custom-domain-name` dan adalah wajib. ARN untuk sertifikat baru harus berbeda dari ARN yang ada.

```
aws redshift modify-custom-domain-association --cluster-id redshiftcluster --custom-domain-name customdomainname --custom-domain-certificate-arn certificatearn
```

Contoh berikut menunjukkan cara mengaitkan domain kustom dengan sertifikat yang berbeda untuk workgroup Amazon Redshift Tanpa Server.

```
aws redshift-serverless modify-custom-domain-association --workgroup-name redshiftworkgroup --custom-domain-name customdomainname --custom-domain-certificate-arn certificatearn
```

Ada penundaan maksimum 30 detik sebelum Anda dapat terhubung ke cluster. Bagian dari penundaan terjadi saat kluster Amazon Redshift memperbarui propertinya, dan ada beberapa penundaan tambahan saat DNS diperbarui. Untuk informasi selengkapnya tentang API dan setiap setelan properti, lihat [ModifyCustomDomainAssociation](#).

Menghapus domain kustom

Untuk menghapus nama domain kustom, pengguna harus memiliki izin untuk tindakan berikut:

- Untuk klaster yang disediakan: `redshift>DeleteCustomDomainAssociation`
- Untuk grup kerja Amazon Redshift Tanpa Server:
`redshiftServerless>DeleteCustomDomainAssociation`

Di konsol

Anda dapat menghapus nama domain kustom dengan memilih tombol Tindakan dan memilih Hapus nama domain kustom. Setelah Anda melakukan ini, Anda masih dapat terhubung ke server dengan memperbarui alat Anda untuk menggunakan titik akhir yang tercantum di konsol.

Menggunakan perintah CLI

Contoh berikut menunjukkan cara menghapus nama domain kustom. Operasi hapus mengharuskan Anda memberikan nama domain kustom yang ada untuk klaster.

```
aws redshift delete-custom-domain-association --cluster-id redshiftcluster --custom-domain-name customdomainname
```

Contoh berikut menunjukkan cara menghapus nama domain kustom untuk workgroup Amazon Redshift Tanpa Server. Nama domain kustom adalah parameter yang diperlukan.

```
aws redshift-serverless delete-custom-domain-association --workgroup-name workgroupname --custom-domain-name customdomainname
```

Untuk informasi lebih lanjut, lihat [DeleteCustomDomainAssociation](#).

Connect ke cluster atau workgroup Anda dengan nama domain kustom, menggunakan klien SQL

Untuk terhubung dengan nama domain kustom, izin IAM berikut diperlukan untuk klaster yang disediakan: `redshift:DescribeCustomDomainAssociations` Untuk Amazon Redshift Tanpa Server, Anda tidak perlu menambahkan izin.

Sebagai praktik terbaik, kami menyarankan untuk melampirkan kebijakan izin ke peran IAM dan kemudian menetapkannya ke pengguna dan grup sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon Redshift](#).

Setelah menyelesaikan langkah-langkah untuk membuat CNAME dan menetapkannya ke klaster atau grup kerja di konsol, Anda dapat memberikan URL kustom di properti koneksi klien SQL Anda. Perhatikan bahwa mungkin ada penundaan dari propagasi DNS segera setelah pembuatan catatan CNAME.

1. Buka klien SQL. Misalnya, Anda dapat menggunakan SQL/Workbench J. Buka properti untuk koneksi, dan tambahkan nama domain kustom untuk string koneksi. Misalnya, `jdbc:redshift://mycluster.example.com:5439/dev?sslmode=verify-full`. Dalam contoh ini, `dev` menentukan database default.

2. Tambahkan Username dan Password untuk pengguna database Anda.
3. Uji koneksi. Kemampuan Anda untuk menanyakan sumber daya database seperti tabel tertentu dapat bervariasi, berdasarkan izin yang diberikan kepada pengguna database atau diberikan ke peran database Amazon Redshift yang ditetapkan.

Perhatikan bahwa Anda mungkin harus menyetel klaster atau grup kerja agar dapat diakses publik untuk terhubung dengannya jika ada di VPC. Anda dapat mengubah pengaturan ini di properti jaringan.

Note

Koneksi ke nama domain khusus didukung dengan driver JDBC dan Python. Koneksi ODBC tidak didukung.

Bekerja dengan titik akhir VPC yang dikelola Redshift

Secara default, klaster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server disediakan di cloud pribadi virtual (VPC). VPC dapat diakses dari VPC atau subnet lain ketika Anda mengizinkan akses publik atau mengatur gateway internet, perangkat NAT, atau AWS Direct Connect koneksi untuk mengarahkan lalu lintas ke sana. Anda juga dapat mengakses klaster atau workgroup dengan menyiapkan endpoint VPC yang dikelola RedShift (didukung oleh). AWS PrivateLink

Anda dapat mengatur endpoint VPC yang dikelola RedShift sebagai koneksi pribadi antara VPC yang berisi cluster atau workgroup dan VPC tempat alat klien berjalan. Jika cluster atau workgroup berada di akun lain, pemilik akun (pemberi) harus memberikan akses ke akun penghubung (penerima hibah). Dengan pendekatan ini, Anda dapat mengakses gudang data tanpa menggunakan alamat IP publik atau merutekan lalu lintas melalui internet.

Ini adalah alasan umum untuk mengizinkan akses menggunakan titik akhir VPC yang dikelola RedShift:

- AWS akun A ingin mengizinkan VPC di AWS akun B memiliki akses ke cluster atau workgroup.
- AWS akun A ingin mengizinkan VPC yang juga ada di AWS akun A untuk memiliki akses ke cluster atau workgroup.
- AWS akun A ingin mengizinkan subnet yang berbeda di VPC AWS dalam akun A untuk memiliki akses ke cluster atau workgroup.

Alur kerja untuk menyiapkan titik akhir VPC yang dikelola RedShift untuk mengakses kluster atau grup kerja di akun lain adalah sebagai berikut:

1. Akun pemilik memberikan otorisasi akses ke akun lain dan menentukan ID akun dan AWS pengidentifikasi VPC (atau semua VPC) penerima hibah.
2. Akun penerima hibah diberi tahu bahwa mereka memiliki izin untuk membuat titik akhir VPC yang dikelola RedShift.
3. Akun penerima hibah membuat titik akhir VPC yang dikelola RedShift.
4. Akun penerima hibah mengakses kluster atau grup kerja akun pemilik menggunakan titik akhir VPC yang dikelola RedShift.

Anda dapat melakukan ini menggunakan konsol Amazon Redshift, the AWS CLI, atau Amazon Redshift API.

Pertimbangan saat menggunakan titik akhir VPC yang dikelola RedShift

Note

Untuk membuat atau mengubah titik akhir VPC yang dikelola RedShift, Anda memerlukan `ec2:CreateVpcEndpoint` izin `ec2:ModifyVpcEndpoint` atau kebijakan IAM, selain izin lain yang ditentukan dalam kebijakan terkelola. `AWS AmazonRedshiftFullAccess`

Saat menggunakan titik akhir VPC yang dikelola RedShift, ingatlah hal berikut:

- Pastikan bahwa cluster yang akan diakses adalah tipe node RA3. Workgroup Amazon Redshift Tanpa Server juga berfungsi untuk ini.
- Untuk kluster yang disediakan, pastikan kluster diaktifkan untuk relokasi cluster atau multi-AZ. Untuk informasi tentang persyaratan untuk mengaktifkan relokasi kluster, lihat [Merelokasi kluster Anda](#). Untuk informasi tentang mengaktifkan Multi-AZ, lihat. [Menyiapkan Multi-AZ saat membuat cluster baru](#)
- Pastikan bahwa cluster atau workgroup untuk mengakses melalui grup keamanannya tersedia dalam rentang port yang valid 5431-5455 dan 8191-8215. Defaultnya adalah 5439.
- Anda dapat memodifikasi grup keamanan VPC yang terkait dengan titik akhir VPC yang dikelola RedShift yang ada. Untuk mengubah pengaturan lain, hapus titik akhir VPC yang dikelola RedShift saat ini dan buat yang baru.

- Jumlah endpoint VPC yang dikelola RedShift yang dapat Anda buat terbatas pada kuota endpoint VPC Anda.
- Titik akhir VPC yang dikelola RedShift tidak dapat diakses dari internet. Titik akhir VPC yang dikelola RedShift hanya dapat diakses dalam VPC di mana titik akhir disediakan atau dari VPC mana pun yang diintip dengan VPC di mana titik akhir disediakan sebagaimana diizinkan oleh tabel rute dan grup keamanan.
- Anda tidak dapat menggunakan konsol VPC Amazon untuk mengelola titik akhir VPC yang dikelola RedShift.
- Saat Anda membuat endpoint VPC yang dikelola RedShift untuk kluster yang disediakan, VPC yang Anda pilih harus memiliki grup subnet. Untuk membuat grup subnet, lihat [Mengelola grup subnet cluster menggunakan konsol](#).
- Jika Availability Zone sedang down, Amazon Redshift tidak membuat elastic network interface baru di Availability Zone lainnya. Anda mungkin perlu membuat titik akhir baru dalam kasus ini.

Untuk informasi tentang kuota dan batasan penamaan, lihat. [Kuota dan batas di Amazon Redshift](#)

Untuk informasi lebih lanjut mengenai harga, lihat [harga AWS PrivateLink](#).

Mengelola titik akhir VPC yang dikelola RedShift menggunakan konsol

Anda dapat mengonfigurasi penggunaan titik akhir VPC yang dikelola RedShift dengan menggunakan konsol Amazon Redshift.

Memberi Akses

Jika VPC yang ingin Anda akses ke kluster atau grup kerja Anda ada di AWS akun lain, pastikan untuk mengotorisasinya dari akun pemilik (pemberi).

Untuk mengizinkan VPC di AWS akun lain memiliki akses ke kluster atau grup kerja Anda

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster. Untuk Amazon Redshift Tanpa Server, pilih dasbor Tanpa Server.
3. Untuk kluster yang ingin Anda izinkan aksesnya, lihat detailnya dengan memilih nama cluster. Pilih tab Properties dari cluster.

Bagian Akun yang Diberikan menampilkan akun dan VPC terkait yang memiliki akses ke kluster Anda. Untuk workgroup Amazon Redshift Tanpa Server, pilih workgroup. Akun yang diberikan tersedia di bawah tab Akses data.

4. Pilih Berikan akses untuk menampilkan formulir untuk memasukkan informasi Penerima Hibah untuk menambahkan akun.
5. Untuk ID AWS akun, masukkan ID akun yang Anda berikan akses. Anda dapat memberikan akses ke VPC tertentu atau semua VPC di akun yang ditentukan.
6. Pilih Berikan akses untuk memberikan akses.

Membuat titik akhir VPC yang dikelola Redshift

Jika Anda memiliki kluster atau workgroup, atau Anda telah diberikan akses untuk mengelolanya, Anda dapat membuat endpoint VPC yang dikelola RedShift untuknya.

Untuk membuat titik akhir VPC yang dikelola RedShift

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Konfigurasi.

Halaman Konfigurasi menampilkan titik akhir VPC yang dikelola RedShift yang telah dibuat. Untuk melihat detail titik akhir, pilih namanya. Untuk Amazon Redshift Tanpa Server, titik akhir VPC berada di bawah tab Akses data, saat Anda memilih grup kerja.

3. Pilih Buat titik akhir untuk menampilkan formulir untuk memasukkan informasi tentang titik akhir yang akan ditambahkan.
4. Masukkan nilai untuk nama Endpoint, ID AWS akun 12 digit, Virtual Private Cloud (VPC) tempat titik akhir berada, Subnet dan grup keamanan VPC.

Subnet di Subnet mendefinisikan subnet dan alamat IP tempat Amazon Redshift menyebarkan titik akhir. Amazon Redshift memilih subnet yang memiliki alamat IP yang tersedia untuk antarmuka jaringan yang terkait dengan titik akhir.

Aturan grup keamanan dalam grup keamanan VPC menentukan port, protokol, dan sumber untuk lalu lintas masuk yang Anda otorisasi untuk titik akhir Anda. Anda mengizinkan akses ke port yang dipilih melalui grup keamanan atau rentang CIDR tempat beban kerja Anda berjalan.

5. Pilih Buat titik akhir untuk membuat titik akhir.

Setelah titik akhir dibuat, Anda dapat mengakses kluster atau grup kerja melalui URL yang ditampilkan di URL Endpoint dalam pengaturan konfigurasi untuk titik akhir VPC yang dikelola RedShift.

Mengelola titik akhir VPC yang dikelola RedShift menggunakan AWS CLI

Anda dapat menggunakan operasi Amazon Redshift CLI berikut ini untuk bekerja dengan titik akhir VPC yang dikelola RedShift. Untuk informasi selengkapnya, lihat Referensi Perintah AWS CLI .

- [authorize-endpoint-access](#)
- [revoke-endpoint-access](#)
- [create-endpoint-access](#)
- [modify-endpoint-access](#)
- [delete-endpoint-access](#)
- [describe-endpoint-access](#)
- [describe-endpoint-authorization](#)

Mengelola titik akhir VPC yang dikelola RedShift menggunakan operasi Amazon Redshift API

Anda dapat menggunakan operasi Amazon Redshift API berikut untuk bekerja dengan titik akhir VPC yang dikelola RedShift. Untuk informasi selengkapnya, lihat Referensi API Amazon Redshift.

- [AuthorizeEndpointAccess](#)
- [RevokeEndpointAccess](#)
- [CreateEndpointAccess](#)
- [ModifyEndpointAccess](#)
- [DeleteEndpointAccess](#)
- [DescribeEndpointAccess](#)
- [DescribeEndpointAuthorization](#)

Mengelola titik akhir VPC yang dikelola RedShift menggunakan AWS CloudFormation

Untuk informasi tentang jenis AWS CloudFormation sumber daya untuk membuat titik akhir VPC yang dikelola RedShift AWS CloudFormation menggunakan, [AWS::Redshift::EndpointAccess](#) lihat di Panduan Pengguna.AWS CloudFormation

Perutean VPC yang disempurnakan di Amazon Redshift

Saat Anda menggunakan perutean VPC Amazon Redshift yang disempurnakan, Amazon Redshift memaksa [semua](#) lalu lintas COPY [dan](#) UNLOAD antara cluster dan repositori data Anda melalui virtual private cloud (VPC) berdasarkan layanan Amazon VPC. Dengan menggunakan perutean VPC yang disempurnakan, Anda dapat menggunakan fitur VPC standar, seperti [grup keamanan VPC](#), [daftar kontrol akses jaringan \(ACL\)](#), [titik akhir VPC](#), [kebijakan titik akhir VPC](#), [gateway internet](#), [dan server Sistem Nama Domain \(DNS\)](#), seperti yang dijelaskan dalam [Panduan Pengguna VPC Amazon](#). Anda menggunakan fitur ini untuk mengelola aliran data dengan ketat antara cluster Amazon Redshift dan sumber daya lainnya. Saat Anda menggunakan perutean VPC yang disempurnakan untuk merutekan lalu lintas melalui VPC Anda, Anda juga dapat menggunakan [log aliran VPC](#) untuk memantau lalu lintas COPY dan UNLOAD.

Cluster Amazon Redshift dan grup kerja Amazon Redshift Serverless mendukung peningkatan perutean VPC. Anda tidak dapat menggunakan perutean VPC yang disempurnakan dengan Redshift Spectrum. Untuk informasi selengkapnya, lihat [Redshift Spectrum dan perutean VPC yang disempurnakan](#).

Jika perutean VPC yang disempurnakan tidak diaktifkan, Amazon Redshift merutekan lalu lintas melalui internet, termasuk lalu lintas ke layanan lain di dalam jaringan. AWS

Important

Karena perutean VPC yang disempurnakan memengaruhi cara Amazon Redshift mengakses sumber daya lain, perintah COPY dan UNLOAD mungkin gagal kecuali Anda mengonfigurasi VPC dengan benar. Anda harus secara khusus membuat jalur jaringan antara VPC klaster Anda dan sumber daya data Anda, seperti yang dijelaskan berikut.

Saat Anda menjalankan perintah COPY atau UNLOAD di kluster dengan perutean VPC yang ditingkatkan diaktifkan, VPC Anda merutekan lalu lintas ke sumber daya yang ditentukan menggunakan jalur jaringan paling ketat, atau paling spesifik, yang tersedia.

Misalnya, Anda dapat mengonfigurasi jalur berikut di VPC Anda:

- Titik akhir VPC — Untuk lalu lintas ke bucket Amazon S3 di AWS Wilayah yang sama dengan cluster Anda, Anda dapat membuat titik akhir VPC untuk mengarahkan lalu lintas langsung ke bucket. Saat menggunakan titik akhir VPC, Anda dapat melampirkan kebijakan titik akhir untuk mengelola akses ke Amazon S3. Untuk informasi selengkapnya tentang penggunaan titik akhir dengan Amazon Redshift, lihat [Bekerja dengan VPC endpoint](#). Jika Anda menggunakan Lake Formation, Anda dapat menemukan informasi lebih lanjut tentang membuat koneksi pribadi antara VPC dan AWS Lake Formation di [AWS Lake Formation dan antarmuka VPC endpoint](#) ().AWS PrivateLink

Note

Saat Anda menggunakan titik akhir VPC Redshift dengan titik akhir Amazon S3 VPC Gateway, Anda harus mengaktifkan perutean VPC yang disempurnakan di Redshift. Untuk informasi selengkapnya, lihat [Titik akhir gateway untuk Amazon S3](#).

- Gateway NAT - Anda dapat terhubung ke bucket Amazon S3 di Wilayah AWS lain, dan Anda dapat terhubung ke layanan lain dalam AWS jaringan. Anda juga dapat mengakses instance host di luar AWS jaringan. Untuk melakukannya, konfigurasi [gateway terjemahan alamat jaringan \(NAT\)](#), seperti yang dijelaskan dalam Panduan Pengguna Amazon VPC.
- Internet gateway — Untuk terhubung ke AWS layanan di luar VPC Anda, Anda dapat melampirkan [gateway internet](#) ke subnet VPC Anda, seperti yang dijelaskan dalam Panduan Pengguna Amazon VPC. Untuk menggunakan gateway internet, cluster Anda harus memiliki IP publik untuk memungkinkan layanan lain berkomunikasi dengan cluster Anda.

Untuk informasi selengkapnya, lihat [Titik Akhir VPC di Panduan](#) Pengguna Amazon VPC.

Tidak ada biaya tambahan untuk menggunakan perutean VPC yang disempurnakan. Anda mungkin dikenakan biaya transfer data tambahan untuk operasi tertentu. Ini termasuk operasi seperti UNLOAD ke Amazon S3 di Wilayah yang AWS berbeda. SALIN dari Amazon EMR, atau Secure Shell (SSH) dengan alamat IP publik. Untuk informasi selengkapnya tentang harga, lihat [Harga Amazon EC2](#).

Topik

- [Bekerja dengan VPC endpoint](#)
- [Perutean VPC yang disempurnakan](#)
- [Redshift Spectrum dan perutean VPC yang disempurnakan](#)

Bekerja dengan VPC endpoint

Anda dapat menggunakan titik akhir VPC untuk membuat koneksi terkelola antara cluster Amazon Redshift di VPC dan Amazon Simple Storage Service (Amazon S3). Ketika Anda melakukannya, COPY dan BONGKAR lalu lintas antara database Anda dan data Anda di Amazon S3 tetap berada di Amazon VPC Anda. Anda dapat melampirkan kebijakan titik akhir ke titik akhir Anda untuk mengelola akses ke data Anda dengan lebih dekat. Misalnya, Anda dapat menambahkan kebijakan ke titik akhir VPC yang mengizinkan pembongkaran data hanya ke bucket Amazon S3 tertentu di akun Anda.

Untuk menggunakan titik akhir VPC, buat titik akhir VPC untuk VPC tempat gudang data Anda berada, lalu aktifkan perutean VPC yang disempurnakan. Anda dapat mengaktifkan perutean VPC yang disempurnakan saat membuat klaster atau grup kerja, atau Anda dapat memodifikasi klaster atau grup kerja di VPC untuk menggunakan perutean VPC yang disempurnakan.

Titik akhir VPC menggunakan tabel rute untuk mengontrol perutean lalu lintas antara cluster atau workgroup di VPC dan Amazon S3. Semua cluster dan workgroup dalam subnet yang terkait dengan tabel rute yang ditentukan secara otomatis menggunakan endpoint tersebut untuk mengakses layanan.

VPC Anda menggunakan rute paling spesifik, atau paling ketat, yang cocok dengan lalu lintas Anda untuk menentukan cara merutekan lalu lintas. Misalnya, Anda memiliki rute di tabel rute Anda untuk semua lalu lintas internet (0.0.0.0/0) yang menunjuk ke gateway internet dan titik akhir Amazon S3. Dalam hal ini, rute titik akhir diutamakan untuk semua lalu lintas yang ditujukan untuk Amazon S3. Ini karena rentang alamat IP untuk layanan Amazon S3 lebih spesifik daripada 0.0.0.0/0. Dalam contoh ini, semua lalu lintas internet lainnya masuk ke gateway internet Anda, termasuk lalu lintas yang ditujukan untuk ember Amazon S3 di tempat lain. Wilayah AWS

Untuk informasi selengkapnya tentang membuat titik akhir, lihat [Membuat titik akhir VPC](#) di Panduan Pengguna Amazon VPC.

Anda menggunakan kebijakan titik akhir untuk mengontrol akses dari klaster atau grup kerja ke bucket Amazon S3 yang menyimpan file data Anda. Untuk kontrol yang lebih spesifik, Anda dapat

melampirkan kebijakan endpoint kustom secara opsional. Untuk informasi selengkapnya, lihat [Mengontrol akses ke layanan menggunakan kebijakan titik akhir](#) di Panduan AWS PrivateLink .

Note

AWS Database Migration Service (AWS DMS) adalah layanan cloud yang memungkinkan untuk memigrasikan database relasional, gudang data, dan jenis penyimpanan data lainnya. Ini dapat terhubung ke AWS sumber atau basis data target apa pun, termasuk database Amazon Redshift yang diaktifkan VPC, dengan beberapa batasan konfigurasi. Mendukung titik akhir Amazon VPC memudahkan untuk menjaga keamanan end-to-end jaringan AWS DMS untuk tugas replikasi. Untuk informasi selengkapnya tentang penggunaan Redshift with AWS DMS, lihat [Mengonfigurasi titik akhir VPC AWS DMS sebagai sumber dan titik akhir target](#) di Panduan Pengguna AWS Database Migration Service

Tidak ada biaya tambahan untuk menggunakan titik akhir. Biaya standar untuk transfer data dan penggunaan sumber daya berlaku. Untuk informasi selengkapnya tentang harga, lihat Harga [Amazon EC2](#).

Perutean VPC yang disempurnakan

Anda dapat mengaktifkan perutean VPC yang disempurnakan saat membuat atau memodifikasi kluster, dan saat Anda membuat atau memodifikasi grup kerja Amazon Redshift Tanpa Server.

Untuk bekerja dengan perutean VPC yang disempurnakan untuk sebuah kluster, kluster Anda harus memenuhi persyaratan dan batasan berikut:

- Cluster Anda harus dalam VPC.

Jika Anda melampirkan endpoint Amazon S3 VPC, cluster Anda menggunakan titik akhir VPC hanya untuk akses ke bucket Amazon S3 di Wilayah yang sama. AWS Untuk mengakses bucket di AWS Wilayah lain (tidak menggunakan titik akhir VPC) atau untuk mengakses layanan AWS lain, buat kluster Anda dapat diakses publik atau gunakan gateway [terjemahan alamat jaringan](#) (NAT). Untuk informasi selengkapnya, lihat [Membuat cluster di VPC](#).

- Anda harus mengaktifkan resolusi Domain Name Service (DNS) di VPC Anda. Atau, jika Anda menggunakan server DNS Anda sendiri, pastikan bahwa permintaan DNS ke Amazon S3 diselesaikan dengan benar ke alamat IP yang dikelola oleh AWS Untuk informasi lebih lanjut, lihat [Menggunakan DNS dengan VPC](#) di Panduan Pengguna Amazon VPC.

- Nama host DNS harus diaktifkan di VPC Anda. Nama host DNS diaktifkan secara default.
- Kebijakan titik akhir VPC Anda harus mengizinkan akses ke bucket Amazon S3 apa pun yang digunakan dengan panggilan COPY, UNLOAD, atau CREATE LIBRARY di Amazon Redshift, termasuk akses ke file manifes apa pun yang terlibat. Untuk COPY dari host jarak jauh, kebijakan endpoint Anda harus mengizinkan akses ke setiap mesin host. Untuk informasi selengkapnya, lihat [Izin IAM untuk COPY, UNLOAD, dan CREATE LIBRARY di Panduan Pengembang Database Amazon Redshift](#).

Untuk membuat cluster dengan perutean VPC yang disempurnakan

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Dasbor cluster yang disediakan, lalu pilih Buat klaster dan masukkan properti detail Cluster.
3. Untuk menampilkan bagian Konfigurasi tambahan, pilih untuk menonaktifkan Gunakan default.
4. Arahkan ke bagian Jaringan dan keamanan.
5. Untuk mengaktifkan perutean VPC yang Ditingkatkan, pilih Aktifkan untuk memaksa lalu lintas cluster melalui VPC.
6. Pilih Buat cluster untuk membuat cluster. Cluster mungkin membutuhkan waktu beberapa menit untuk siap digunakan.

Untuk membuat workgroup Amazon Redshift Tanpa Server dengan perutean VPC yang disempurnakan

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Dasbor tanpa server, lalu pilih Buat grup kerja dan masukkan properti untuk grup kerja Anda.
3. Arahkan ke bagian Jaringan dan keamanan.
4. Pilih Aktifkan perutean VPC yang disempurnakan untuk merutekan lalu lintas jaringan melalui VPC.
5. Pilih Berikutnya dan selesai memasukkan properti workgroup Anda sampai Anda membuat workgroup.

Redshift Spectrum dan perutean VPC yang disempurnakan

Amazon Redshift Spectrum tidak mendukung perutean VPC yang disempurnakan dengan cluster yang disediakan. Perutean VPC yang disempurnakan Amazon Redshift merutekan lalu lintas tertentu melalui VPC Anda. Semua lalu lintas antara cluster Anda dan bucket Amazon S3 Anda dipaksa untuk melewati VPC Amazon Anda. Redshift Spectrum berjalan pada sumber daya AWS terkelola yang dimiliki oleh Amazon Redshift. Karena sumber daya ini berada di luar VPC Anda, Redshift Spectrum tidak menggunakan perutean VPC yang disempurnakan.

Lalu lintas antara Redshift Spectrum dan Amazon S3 dirutekan dengan aman melalui jaringan pribadi, AWS di luar VPC Anda. Lalu lintas dalam penerbangan ditandatangani menggunakan protokol Amazon Signature Version 4 (SigV4) dan dienkripsi menggunakan HTTPS. Lalu lintas ini diotorisasi berdasarkan peran IAM yang dilampirkan ke cluster Amazon Redshift Anda. Untuk mengelola lalu lintas Redshift Spectrum lebih lanjut, Anda dapat memodifikasi peran IAM klaster dan kebijakan yang dilampirkan ke bucket Amazon S3. Anda mungkin juga perlu mengonfigurasi VPC Anda untuk memungkinkan klaster Anda mengakses atau AWS Glue Athena, seperti yang dijelaskan berikut ini.

Perhatikan bahwa karena perutean VPC yang disempurnakan memengaruhi cara Amazon Redshift mengakses sumber daya lain, kueri mungkin gagal kecuali Anda mengonfigurasi VPC dengan benar. Untuk informasi selengkapnya, lihat [Perutean VPC yang disempurnakan di Amazon Redshift](#), yang membahas secara lebih rinci membuat titik akhir VPC, gateway NAT, dan sumber daya jaringan lainnya untuk mengarahkan lalu lintas ke bucket Amazon S3 Anda.

Note

Amazon Redshift Serverless mendukung perutean VPC yang disempurnakan untuk kueri ke tabel eksternal di Amazon S3.

Pertimbangan saat menggunakan Amazon Redshift Spectrum

Berikut ini adalah pertimbangan saat menggunakan Redshift Spectrum:

- [Kebijakan akses bucket](#)
- [IAM role klaster](#)
- [Pencatatan dan audit akses Amazon S3](#)
- [Akses ke AWS Glue atau Amazon Athena](#)

Kebijakan akses bucket

Anda dapat mengontrol akses ke data di bucket Amazon S3 dengan menggunakan kebijakan bucket yang dilampirkan ke bucket dan dengan menggunakan peran IAM yang dilampirkan ke cluster.

Redshift Spectrum pada kluster yang disediakan tidak dapat mengakses data yang disimpan di bucket Amazon S3 yang menggunakan kebijakan bucket yang membatasi akses hanya ke titik akhir VPC yang ditentukan. Sebagai gantinya, gunakan kebijakan bucket yang membatasi akses hanya ke prinsipal tertentu, seperti AWS akun tertentu atau pengguna tertentu.

Untuk peran IAM yang diberikan akses ke bucket, gunakan hubungan kepercayaan yang memungkinkan peran hanya diasumsikan oleh prinsipal layanan Amazon Redshift. Saat dilampirkan ke cluster Anda, peran hanya dapat digunakan dalam konteks Amazon Redshift dan tidak dapat dibagikan di luar cluster. Untuk informasi selengkapnya, lihat [Membatasi akses ke peran IAM](#). Kebijakan kontrol layanan (SCP) juga dapat digunakan untuk membatasi peran lebih lanjut, lihat [Mencegah pengguna IAM dan peran membuat perubahan tertentu, dengan pengecualian untuk peran admin tertentu dalam Panduan Pengguna AWS Organizations](#)

Note

Untuk menggunakan Redshift Spectrum, tidak ada kebijakan IAM yang memblokir penggunaan URL presigned Amazon S3 yang dapat diterapkan. URL presigned yang dihasilkan oleh Amazon Redshift Spectrum berlaku selama 1 jam sehingga Amazon Redshift memiliki cukup waktu untuk memuat semua file dari bucket Amazon S3. URL presigned unik dibuat untuk setiap file yang dipindai oleh Redshift Spectrum. Untuk kebijakan bucket yang menyertakan `s3:signatureAge` tindakan, pastikan untuk menetapkan nilainya setidaknya 3.600.000 milidetik.

Contoh kebijakan bucket berikut mengizinkan akses ke bucket yang ditentukan hanya dari lalu lintas yang berasal dari Redshift Spectrum yang dimiliki oleh akun. AWS 123456789012

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "BucketPolicyForSpectrum",
    "Effect": "Allow",
    "Principal": {
      "AWS": ["arn:aws:iam::123456789012:role/redshift"]
    }
  }]
}
```

```

    },
    "Action": ["s3:GetObject", "s3:List*"],
    "Resource": ["arn:aws:s3:::examplebucket/*"],
    "Condition": {
      "StringEquals": {
        "aws:UserAgent": "AWS Redshift/Spectrum"
      }
    }
  }
}

```

IAM role klaster

Peran yang melekat pada klaster Anda harus memiliki hubungan kepercayaan yang memungkinkannya diasumsikan hanya oleh layanan Amazon Redshift, seperti yang ditunjukkan berikut.

```

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

```

Anda dapat menambahkan kebijakan ke peran klaster yang mencegah akses COPY dan UNLOAD ke bucket tertentu. Kebijakan berikut mengizinkan lalu lintas ke bucket yang ditentukan hanya dari 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"}}
  }]
}

```

```
}]
}
```

Untuk informasi selengkapnya, lihat [Kebijakan IAM untuk Spektrum Pergeseran Merah](#) di Panduan Pengembang Database Amazon Redshift.

Pencatatan dan audit akses Amazon S3

Salah satu manfaat menggunakan perutean VPC Amazon Redshift yang disempurnakan adalah bahwa semua lalu lintas COPY dan UNLOAD dicatat di log aliran VPC. Lalu lintas yang berasal dari Redshift Spectrum ke Amazon S3 tidak melewati VPC Anda, jadi tidak masuk ke log aliran VPC. Saat Redshift Spectrum mengakses data di Amazon S3, ia melakukan operasi ini dalam konteks AWS akun dan hak istimewa peran masing-masing. Anda dapat mencatat dan mengaudit akses Amazon S3 menggunakan akses server masuk AWS CloudTrail dan Amazon S3.

Pastikan rentang IP S3 ditambahkan ke daftar izin Anda. Untuk mempelajari lebih lanjut tentang rentang IP S3 yang diperlukan, lihat [Isolasi jaringan](#).

AWS CloudTrail Log

Untuk melacak semua akses ke objek di Amazon S3, termasuk akses Redshift Spectrum, aktifkan pencatatan untuk objek CloudTrail Amazon S3.

Anda dapat menggunakan CloudTrail untuk melihat, mencari, mengunduh, mengarsipkan, menganalisis, dan menanggapi aktivitas akun di seluruh AWS infrastruktur Anda. Untuk informasi selengkapnya, lihat [Memulai dengan CloudTrail](#).

Secara default, hanya CloudTrail melacak tindakan tingkat ember. Untuk melacak tindakan tingkat objek (seperti `GetObject`), aktifkan data dan peristiwa manajemen untuk setiap bucket yang dicatat.

Pencatatan Akses Server Amazon S3

Pencatatan akses server menyediakan catatan terperinci untuk permintaan yang dilakukan ke bucket. Informasi log akses dapat berguna dalam audit keamanan dan akses. Untuk informasi selengkapnya, lihat [Cara Mengaktifkan Pencatatan Akses Server](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk informasi selengkapnya, lihat posting blog AWS Keamanan [Cara Menggunakan Kebijakan Bucket dan Menerapkan Pertahanan Secara Mendalam untuk Membantu Mengamankan Data Amazon S3](#) Anda.

Akses ke AWS Glue atau Amazon Athena

Redshift Spectrum mengakses katalog data Anda di atau AWS Glue Athena. Pilihan lain adalah menggunakan metastore Hive khusus untuk katalog data Anda.

Untuk mengaktifkan akses ke AWS Glue atau Athena, konfigurasi VPC Anda dengan gateway internet atau gateway NAT. Konfigurasi grup keamanan VPC Anda untuk mengizinkan lalu lintas keluar ke titik akhir publik untuk dan Athena. AWS Glue Atau, Anda dapat mengonfigurasi titik akhir VPC antarmuka AWS Glue untuk mengakses. AWS Glue Data Catalog Saat Anda menggunakan titik akhir antarmuka VPC, komunikasi antara VPC Anda dan AWS Glue dilakukan di dalam jaringan. AWS Untuk informasi selengkapnya, lihat [Membuat Titik Akhir Antarmuka](#).

Anda dapat mengonfigurasi jalur berikut di VPC Anda:

- **Internet gateway** —Untuk terhubung ke AWS layanan di luar VPC Anda, Anda dapat melampirkan gateway [internet](#) ke subnet VPC Anda, seperti yang dijelaskan dalam Panduan Pengguna Amazon VPC. Untuk menggunakan gateway internet, cluster Anda harus memiliki alamat IP publik untuk memungkinkan layanan lain berkomunikasi dengan cluster Anda.
- **Gateway NAT** —Untuk menyambung ke bucket Amazon S3 di Wilayah AWS lain atau ke layanan lain dalam AWS jaringan, konfigurasi gateway [terjemahan alamat jaringan \(NAT\)](#), seperti yang dijelaskan dalam Panduan Pengguna Amazon VPC. Gunakan konfigurasi ini juga untuk mengakses instance host di luar AWS jaringan.

Untuk informasi selengkapnya, lihat [Perutean VPC yang disempurnakan di Amazon Redshift](#).

Memantau kinerja klaster Amazon Redshift

Amazon Redshift menyediakan metrik kinerja dan data sehingga Anda dapat melacak kesehatan dan kinerja cluster dan database Anda. Di bagian ini, kami membahas jenis data yang dapat Anda gunakan di Amazon Redshift, khususnya di konsol Amazon Redshift.

Topik

- [Gambaran Umum](#)
- [Memantau Amazon Redshift menggunakan metrik CloudWatch](#)
- [Bekerja dengan data kinerja di konsol Amazon Redshift](#)

Gambaran Umum

Data kinerja yang dapat Anda gunakan di konsol Amazon Redshift terbagi dalam dua kategori:

- **CloudWatch Metrik Amazon** — CloudWatch Metrik Amazon membantu Anda memantau aspek fisik klaster Anda, seperti pemanfaatan CPU, latensi, dan throughput. Data metrik ditampilkan langsung di konsol Amazon Redshift. Anda juga dapat melihatnya di CloudWatch konsol. Atau, Anda dapat menggunakannya dengan cara lain Anda bekerja dengan metrik, seperti dengan AWS CLI atau salah satu AWS SDK.
- **Kueri/Muat data kinerja** - Data kinerja membantu Anda memantau aktivitas dan kinerja database. Data ini digabungkan di konsol Amazon Redshift untuk membantu Anda dengan mudah mengkorelasikan apa yang Anda lihat CloudWatch dalam metrik dengan kueri database tertentu dan peristiwa pemuatan. Anda juga dapat membuat kueri kinerja kustom Anda sendiri dan menjalankannya langsung di database. Data kinerja kueri dan pemuatan hanya ditampilkan di konsol Amazon Redshift. Itu tidak dipublikasikan sebagai CloudWatch metrik.

Data kinerja diintegrasikan ke dalam konsol Amazon Redshift, menghasilkan pengalaman yang lebih kaya dengan cara-cara berikut:

- Data kinerja yang terkait dengan klaster ditampilkan secara kontekstual saat Anda melihat klaster, di mana Anda mungkin memerlukannya untuk membuat keputusan tentang klaster seperti mengubah ukuran.
- Beberapa metrik kinerja ditampilkan dalam unit yang diskalakan lebih tepat di konsol Amazon Redshift dibandingkan dengan. CloudWatch Misalnya `WriteThroughput`, ditampilkan dalam GB/

s (dibandingkan dengan bytes/s in CloudWatch), yang merupakan unit yang lebih relevan untuk ruang penyimpanan tipikal node.

- Anda dapat dengan mudah menampilkan data kinerja untuk node cluster bersama-sama pada grafik yang sama. Dengan cara ini, Anda dapat dengan mudah memantau kinerja semua node dari sebuah cluster. Anda juga dapat melihat data kinerja untuk setiap node.

Amazon Redshift menyediakan data kinerja (baik CloudWatch metrik maupun kueri dan data muat) tanpa biaya tambahan. Data kinerja dicatat setiap menit. Anda dapat mengakses nilai historis data kinerja di konsol Amazon Redshift. [Untuk informasi mendetail tentang penggunaan CloudWatch untuk mengakses data kinerja Amazon Redshift yang diekspos sebagai CloudWatch metrik, lihat Apa itu? CloudWatch](#) di Panduan CloudWatch Pengguna Amazon.

Memantau Amazon Redshift menggunakan metrik CloudWatch

Menggunakan CloudWatch metrik untuk Amazon Redshift, Anda bisa mendapatkan informasi tentang kesehatan dan kinerja klaster Anda dan melihat informasi di tingkat node. Saat bekerja dengan metrik ini, perlu diingat bahwa setiap metrik memiliki satu atau lebih dimensi yang terkait dengannya. Dimensi ini memberi tahu Anda metrik apa yang berlaku, yaitu ruang lingkup metrik. Amazon Redshift memiliki dua dimensi berikut:

- Metrik yang memiliki `NodeID` dimensi adalah metrik yang menyediakan data kinerja untuk node cluster. Kumpulan metrik ini mencakup node pemimpin dan komputasi. Contoh metrik ini meliputi `CPUUtilization`, `ReadIOPS`, `WriteIOPS`.
- Metrik yang hanya memiliki `ClusterIdentifier` dimensi adalah metrik yang menyediakan data kinerja untuk cluster. Contoh metrik ini termasuk `HealthStatus` dan `MaintenanceMode`.

Note

Dalam beberapa kasus metrik, metrik khusus cluster mewakili agregasi perilaku simpul. Dalam kasus ini, berhati-hatilah dalam interpretasi nilai metrik karena perilaku node pemimpin digabungkan dengan node komputasi.

Untuk informasi umum tentang CloudWatch metrik dan dimensi, lihat [CloudWatch konsep](#) di Panduan CloudWatch Pengguna Amazon.

Untuk deskripsi lebih lanjut tentang CloudWatch metrik untuk Amazon Redshift, lihat bagian berikut.

Topik


- [Metrik Pergeseran Merah Amazon](#)
- [Dimensi untuk metrik Amazon Redshift](#)
- [Kueri Amazon Redshift dan memuat data kinerja](#)

Metrik Pergeseran Merah Amazon

Namespace `AWS/Redshift` mencakup metrik berikut. Kecuali dinyatakan lain, metrik dikumpulkan pada interval 1 menit.

Judul

Metrik	Deskripsi
<code>CommitQueueLength</code>	Jumlah transaksi yang menunggu untuk dilakukan pada titik waktu tertentu. Unit: Hitungan Dimensi: <code>ClusterIdentifier</code>
<code>ConcurrencyScalingActiveClusters</code>	Jumlah cluster penskalaan konkurensi yang secara aktif memproses kueri pada waktu tertentu. Unit: Hitungan Dimensi: <code>ClusterIdentifier</code>
<code>ConcurrencyScalingSeconds</code>	Jumlah detik yang digunakan oleh cluster penskalaan konkurensi yang memiliki aktivitas pemrosesan kueri aktif. Unit: Hitungan Dimensi: <code>ClusterIdentifier</code>
<code>CPUUtilization</code>	Persentase penggunaan CPU. Untuk cluster, metrik ini mewakili agregasi dari semua node (pemimpin dan komputasi) nilai pemanfaatan CPU. Unit: Persen

Metrik	Deskripsi
DatabaseConnections	<p>Dimensions: ClusterIdentifier , NodeID</p> <p>Dimensi: ClusterIdentifier</p> <p>Jumlah koneksi database ke cluster.</p> <p>Unit: Hitungan</p> <p>Dimensi: ClusterIdentifier</p>
HealthStatus	<p>Menunjukkan kesehatan cluster. Setiap menit cluster terhubung ke database dan melakukan query sederhana. Jika mampu melakukan operasi ini dengan sukses, cluster dianggap sehat. Kalau tidak, cluster tidak sehat. Status yang tidak sehat dapat terjadi ketika database cluster berada di bawah beban yang sangat berat atau jika ada masalah konfigurasi dengan database di cluster.</p> <div data-bbox="594 974 1507 1625" style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>Di Amazon CloudWatch, metrik ini dilaporkan sebagai 1 atau 0 sedangkan di konsol Amazon Redshift, metrik ini ditampilkan dengan kata-kata HEALTHY atau UNHEALTHY untuk kenyamanan. Saat metrik ini ditampilkan di konsol Amazon Redshift, rata-rata pengambilan sampel diabaikan dan hanya HEALTHY atau ditampilkan. UNHEALTHY Di Amazon CloudWatch, nilai yang berbeda dari 1 dan 0 mungkin terjadi karena masalah pengambilan sampel. Nilai apa pun di bawah 1 HealthStatus untuk dilaporkan sebagai 0 (UNHEALTHY).</p> </div> <p>Unit: Hitung (1/0) (HEALTHY/UNHEALTHY di konsol Amazon Redshift)</p> <p>Dimensi: ClusterIdentifier</p>

Metrik	Deskripsi
MaintenanceMode	<p>Menunjukkan apakah cluster dalam mode pemeliharaan.</p> <div data-bbox="592 304 1507 905" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p>Note</p> <p>Di Amazon CloudWatch, metrik ini dilaporkan sebagai 1 atau 0 sedangkan di konsol Amazon Redshift, metrik ini ditampilkan dengan kata-kata ON atau OFF untuk kenyamanan. Saat metrik ini ditampilkan di konsol Amazon Redshift, rata-rata pengambilan sampel diabaikan dan hanya ON atau ditampilkan. OFF Di Amazon CloudWatch, nilai yang berbeda dari 1 dan 0 mungkin terjadi karena masalah pengambilan sampel. Setiap nilai yang lebih besar dari 0 MaintenanceMode untuk dilaporkan sebagai 1 (ON).</p> </div> <p>Unit: Hitung (1/0) (ON/OFF di konsol Amazon Redshift).</p> <p>Dimensi: ClusterIdentifier</p>
MaxConfiguredConcurrencyScalingClusters	<p>Jumlah maksimum cluster penskalaan konkurensi yang dikonfigurasi dari grup parameter. Untuk informasi selengkapnya, lihat Grup parameter Amazon Redshift.</p> <p>Unit: Count (Jumlah)</p> <p>Dimensi: ClusterIdentifier</p>
NetworkReceiveThroughput	<p>Tingkat di mana node atau cluster menerima data.</p> <p>Unit: Bytes/Detik (MB/s di konsol Amazon Redshift)</p> <p>Dimensions: ClusterIdentifier , NodeID</p> <p>Dimensi: ClusterIdentifier</p>

Metrik	Deskripsi
NetworkTransmitThroughput	<p>Tingkat di mana node atau cluster menulis data.</p> <p>Unit: Bytes/Detik (MB/s di konsol Amazon Redshift)</p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>NodeID</code></p> <p>Dimensi: <code>ClusterIdentifier</code></p>
PercentageDiskSpaceUsed	<p>Persentase ruang disk yang digunakan.</p> <p>Unit: Persen</p> <p>Dimensi: <code>ClusterIdentifier</code></p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>NodeID</code></p>
QueriesCompletedPerSecond	<p>Jumlah rata-rata kueri yang diselesaikan per detik. Dilaporkan dalam interval 5 menit. Metrik ini tidak didukung pada kluster simpul tunggal.</p> <p>Unit: Jumlah/Detik</p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>latency</code></p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>wlmid</code></p>
QueryDuration	<p>Jumlah rata-rata waktu untuk menyelesaikan kueri. Dilaporkan dalam interval 5 menit. Metrik ini tidak didukung pada kluster simpul tunggal.</p> <p>Unit: Mikrodetik</p> <p>Dimensi: <code>ClusterIdentifier</code> , <code>NodeID</code>, <code>latency</code></p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>latency</code></p> <p>Dimensi: <code>ClusterIdentifier</code> , <code>NodeID</code>, <code>wlmid</code></p>

Metrik	Deskripsi
QueryRuntimeBreakdown	<p>Total waktu kueri yang dihabiskan untuk dijalankan berdasarkan tahap kueri. Dilaporkan dalam interval 5 menit.</p> <p>Unit: Milidetik</p> <p>Dimensi: ClusterIdentifier, NodeId, panggung</p> <p>Dimensi: ClusterIdentifier, panggung</p>
ReadIOPS	<p>Jumlah rata-rata operasi pembacaan disk per detik.</p> <p>Unit: Jumlah/Detik</p> <p>Dimensions: ClusterIdentifier , NodeID</p> <p>Dimensi: ClusterIdentifier</p>
ReadLatency	<p>Jumlah rata-rata waktu yang dibutuhkan untuk operasi I/O membaca disk.</p> <p>Unit: detik</p> <p>Dimensions: ClusterIdentifier , NodeID</p> <p>Dimensi: ClusterIdentifier</p>
ReadThroughput	<p>Jumlah byte rata-rata yang dibaca dari disk per detik.</p> <p>Unit: Byte (Gb/s di konsol Amazon Redshift)</p> <p>Dimensions: ClusterIdentifier , NodeID</p> <p>Dimensi: ClusterIdentifier</p>
RedshiftManagedStorageTotalCapacity	<p>Total kapasitas penyimpanan terkelola.</p> <p>Unit: Megabyte</p> <p>Dimensi: ClusterIdentifier</p>

Metrik	Deskripsi
TotalTableCount	<p>Jumlah tabel pengguna terbuka pada titik waktu tertentu. Total ini tidak termasuk tabel Amazon Redshift Spectrum.</p> <p>Unit: Hitungan</p> <p>Dimensi: ClusterIdentifier</p>
WLMQueueLength	<p>Jumlah kueri yang menunggu untuk memasuki antrian manajemen beban kerja (WLM).</p> <p>Unit: Hitungan</p> <p>Dimensions: ClusterIdentifier , service class</p> <p>Dimensions: ClusterIdentifier , QueueName</p>
WLMQueueWaitTime	<p>Total waktu kueri yang dihabiskan menunggu dalam antrian manajemen beban kerja (WLM). Dilaporkan dalam interval 5 menit.</p> <p>Satuan: Milidetik.</p> <p>Dimensions: ClusterIdentifier , QueryPriority</p> <p>Dimensions: ClusterIdentifier , wlmid</p> <p>Dimensions: ClusterIdentifier , QueueName</p>
WLMQueriesCompletedPerSecond	<p>Jumlah rata-rata kueri yang diselesaikan per detik untuk antrian manajemen beban kerja (WLM). Dilaporkan dalam interval 5 menit. Metrik ini tidak didukung pada kluster simpul tunggal.</p> <p>Unit: Jumlah/Detik</p> <p>Dimensions: ClusterIdentifier , wlmid</p> <p>Dimensions: ClusterIdentifier , QueueName</p>

Metrik	Deskripsi
<code>WLMQueryDuration</code>	<p>Rata-rata lamanya waktu untuk menyelesaikan kueri untuk antrian manajemen beban kerja (WLM). Dilaporkan dalam interval 5 menit. Metrik ini tidak didukung pada kluster simpul tunggal.</p> <p>Unit: Mikrodetik</p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>wlmid</code></p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>QueueName</code></p>
<code>WLMRunningQueries</code>	<p>Jumlah kueri yang berjalan dari cluster utama dan cluster penskalaan konkurensi per antrian WLM.</p> <p>Unit: Hitungan</p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>wlmid</code></p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>QueueName</code></p>
<code>WriteIOPS</code>	<p>Jumlah rata-rata operasi tulis per detik.</p> <p>Unit: Jumlah/Detik</p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>NodeID</code></p> <p>Dimensi: <code>ClusterIdentifier</code></p>
<code>WriteLatency</code>	<p>Jumlah rata-rata waktu yang dibutuhkan untuk operasi I/O tulis disk.</p> <p>Unit: detik</p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>NodeID</code></p> <p>Dimensi: <code>ClusterIdentifier</code></p>

Metrik	Deskripsi
WriteThroughput	<p>Jumlah byte rata-rata yang ditulis dari disk per detik.</p> <p>Unit: Byte (Gb/s di konsol Amazon Redshift)</p> <p>Dimensions: <code>ClusterIdentifier</code> , <code>NodeID</code></p> <p>Dimensi: <code>ClusterIdentifier</code></p>
SchemaQuota	<p>Kuota yang dikonfigurasi untuk skema.</p> <p>Unit: Megabyte</p> <p>Dimensi: <code>ClusterIdentifier</code> , <code>Database</code>, <code>Schema</code></p> <p>Berkala/Dorong: <code>Periodic</code></p> <p>Frekuensi: <code>5 minutes</code></p> <p>Kriteria berhenti: Skema turun atau kuota dihapus</p>
NumExceededSchemaQuotas	<p>Jumlah skema dengan kuota terlampaui.</p> <p>Unit: Hitungan</p> <p>Dimensi: <code>ClusterIdentifier</code></p> <p>Berkala/Dorong: <code>Periodic</code></p> <p>Frekuensi: <code>5 minutes</code></p> <p>Kriteria berhenti: <code>N/A</code></p>

Metrik	Deskripsi
StorageUsed	<p>Disk atau ruang penyimpanan yang digunakan oleh skema.</p> <p>Unit: Megabyte</p> <p>Dimensi:ClusterIdentifier ,Database, Schema</p> <p>Berkala/Dorong: Periodic</p> <p>Frekuensi: 5 minutes</p> <p>Kriteria berhenti: Skema turun atau kuota dihapus</p>
PercentageQuotaUsed	<p>Persentase disk atau ruang penyimpanan yang digunakan relatif terhadap kuota skema yang dikonfigurasi.</p> <p>Unit: Persen</p> <p>Dimensi:ClusterIdentifier ,Database, Schema</p> <p>Berkala/Dorong: Periodic</p> <p>Frekuensi: 5 minutes</p> <p>Kriteria berhenti: Skema turun atau kuota dihapus</p>

Metrik	Deskripsi
UsageLimitAvailable	<p>Tergantung pada FeatureType, UsageLimitAvailable mengembalikan yang berikut:</p> <ul style="list-style-type: none">• Jika yaCONCURRENCY_SCALING , UsageLimitAvailable mengembalikan jumlah total waktu yang dapat digunakan dengan penskalaan konkurensi dalam kenaikan 1 menit.• Jika FeatureType yaCROSS_REGION_DATASHARING , UsageLimitAvailable mengembalikan jumlah total data yang dapat dipindai dalam peningkatan 1-TB.• Jika FeatureType yaSPECTRUM, UsageLimitAvailable mengembalikan jumlah total data yang dapat dipindai dalam peningkatan 1-TB. <p>Unit: Menit atau TB</p> <p>Dimensi:ClusterIdentifier ,FeatureType ,UsageLimitId</p>

Metrik	Deskripsi
UsageLimitConsumed	<p>Tergantung pada FeatureType, UsageLimitConsumed mengembalikan yang berikut:</p> <ul style="list-style-type: none"> • Jika yaCONCURRENCY_SCALING , UsageLimitAvailable mengembalikan jumlah total waktu yang digunakan oleh penskalaan konkurensi dalam kenaikan 1 menit. FeatureType • Jika yaCROSS_REGION_DATASHARING , UsageLimitAvailable mengembalikan jumlah total data yang dipindai dalam peningkatan 1-TB. FeatureType • Jika yaSPECTRUM, UsageLimitAvailable mengembalikan jumlah total data yang dipindai dalam peningkatan 1-TB. FeatureType <p>Unit: Menit atau TB</p> <p>Dimensi:ClusterIdentifier ,FeatureType , UsageLimitId</p>

Dimensi untuk metrik Amazon Redshift

Data Amazon Redshift dapat disaring di sepanjang salah satu dimensi dalam tabel berikut.

Dimensi	Deskripsi
latency	<p>Kemungkinan nilainya adalah sebagai berikut:</p> <ul style="list-style-type: none"> • pendek - di bawah 10 detik • sedang — antara 10 detik dan 10 menit • lama — lebih dari 10 menit
NodeID	<p>Filter meminta data yang spesifik untuk node cluster. NodeIDadalah “Leader”, “Shared”, atau “Compute-N” di mana N adalah 0, 1,... untuk jumlah node dalam cluster. “Shared” berarti</p>

Dimensi	Deskripsi
	<p>bahwa cluster hanya memiliki satu node, yaitu node pemimpin dan node komputasi digabungkan.</p> <p>Metrik dilaporkan untuk node pemimpin dan node komputasi hanya untuk <code>CPUUtilization</code>, <code>NetworkTransmitThroughput</code>, dan <code>ReadIOPS</code>. Metrik lain yang menggunakan <code>NodeId</code> dimensi dilaporkan hanya untuk node komputasi.</p>
<code>ClusterIdentifier</code>	<p>Filter meminta data yang khusus untuk cluster. Metrik yang khusus untuk cluster meliputi <code>HealthStatus</code>, <code>MaintenanceMode</code>, dan <code>DatabaseConnections</code>. Metrik umum untuk dimensi ini (misalnya, <code>ReadIOPS</code>) yang juga merupakan metrik node mewakili agregat data metrik node. Berhati-hatilah dalam menafsirkan metrik ini karena mereka menggabungkan perilaku pemimpin dan node komputasi.</p>
<code>service class</code>	<p>Pengidentifikasi untuk kelas WLM layanan.</p>

Dimensi	Deskripsi
stage	<p>Tahapan eksekusi untuk query. Kemungkinan nilainya adalah sebagai berikut:</p> <ul style="list-style-type: none"> • QueryPlanning: Waktu yang dihabiskan mengurai dan mengoptimalkan pernyataan SQL. • QueryWaiting: Waktu yang dihabiskan menunggu di antrian WLM. • QueryExecutingRead: Waktu yang dihabiskan untuk mengeksekusi kueri baca. • QueryExecutingInsert: Waktu yang dihabiskan untuk mengeksekusi kueri sisipan. • QueryExecutingDelete: Waktu yang dihabiskan untuk mengeksekusi kueri hapus. • QueryExecutingUpdate: Waktu yang dihabiskan untuk mengeksekusi kueri pembaruan. • QueryExecutingCtas: Waktu yang dihabiskan untuk mengeksekusi membuat tabel sebagai kueri. • QueryExecutingUnload: Waktu yang dihabiskan untuk mengeksekusi kueri bongkar muat. • QueryExecutingCopy: Waktu yang dihabiskan untuk mengeksekusi kueri salinan. • QueryCommit: Waktu yang dihabiskan untuk berkomitmen.
wlmid	Pengidentifikasi untuk antrian manajemen beban kerja.
QueryPriority	Prioritas kueri. Peluang nilai adalah CRITICAL, HIGHEST, HIGH, NORMAL, LOW, dan LOWEST.
QueueName	Nama antrian manajemen beban kerja.
FeatureType	Fitur yang dibatasi oleh batas penggunaan. Nilai yang mungkin adalah CONCURRENTLY_SCALING , CROSS_REGION_DATAS HARING , dan SPECTRUM.

Dimensi	Deskripsi
UsageLimitId	Pengidentifikasi untuk batas penggunaan.

Kueri Amazon Redshift dan memuat data kinerja

Selain CloudWatch metrik, Amazon Redshift menyediakan kueri dan memuat data kinerja. Data kinerja kueri dan beban dapat digunakan untuk membantu Anda memahami hubungan antara kinerja database dan metrik klaster. Misalnya, jika Anda melihat bahwa CPU cluster melonjak, Anda dapat menemukan lonjakan pada grafik CPU cluster dan melihat kueri yang sedang berjalan pada saat itu. Sebaliknya, jika Anda meninjau kueri tertentu, data metrik (seperti CPU) ditampilkan dalam konteks sehingga Anda dapat memahami dampak kueri pada metrik klaster.

Data kinerja kueri dan pemuatan tidak dipublikasikan sebagai CloudWatch metrik dan hanya dapat dilihat di konsol Amazon Redshift. Data kinerja kueri dan pemuatan dihasilkan dari kueri dengan tabel sistem database Anda (untuk informasi selengkapnya, lihat [Referensi tabel sistem](#) di Panduan Pengembang Amazon Redshift). Anda juga dapat membuat kueri kinerja basis data kustom Anda sendiri, tetapi kami sarankan memulai dengan kueri dan memuat data kinerja yang disajikan di konsol. Untuk informasi selengkapnya tentang mengukur dan memantau performa database Anda sendiri, lihat [Mengelola performa](#) di Panduan Pengembang Amazon Redshift.

Tabel berikut menjelaskan berbagai aspek kueri dan memuat data yang dapat Anda akses di konsol Amazon Redshift.

Kueri/Muat data	Deskripsi
Ringkasan kueri	Daftar kueri dalam periode waktu tertentu. Daftar dapat diurutkan berdasarkan nilai seperti ID kueri, runtime kueri, dan status. Lihat data ini di tab Pemantauan kueri pada halaman detail klaster.
Detail kueri	Memberikan detail tentang kueri tertentu termasuk: <ul style="list-style-type: none"> • Properti kueri seperti ID kueri, tipe, klaster tempat kueri dijalankan, dan runtime. • Detail seperti status kueri dan jumlah kesalahan. • Pernyataan SQL yang dijalankan. • Rencana penjelasan jika tersedia.

Kueri/Muat data	Deskripsi
	<ul style="list-style-type: none"> Data kinerja cluster selama eksekusi kueri (untuk informasi selengkapnya, lihat Melihat data riwayat kueri).
Muat ringkasan	Daftar semua beban dalam periode waktu tertentu. Daftar dapat diurutkan berdasarkan nilai seperti ID kueri, runtime kueri, dan status. Lihat data ini di tab Pemantauan kueri pada halaman detail klaster.
Memuat detail	<p>Memberikan rincian tentang operasi beban tertentu termasuk:</p> <ul style="list-style-type: none"> Memuat properti seperti ID kueri, tipe, klaster tempat kueri dijalankan, dan runtime. Detail seperti status beban dan jumlah kesalahan. Pernyataan SQL yang dijalankan. Daftar file yang dimuat. Data kinerja cluster selama operasi beban (untuk informasi lebih lanjut, lihat Melihat data riwayat kueri).

Bekerja dengan data kinerja di konsol Amazon Redshift

Di bagian ini, Anda dapat menemukan cara melihat data kinerja di konsol Amazon Redshift, yang mencakup informasi tentang kinerja klaster dan kueri. Selain itu, Anda dapat membuat alarm pada metrik cluster langsung dari konsol Amazon Redshift.

Saat melihat data performa di konsol Amazon Redshift, Anda melihatnya berdasarkan klaster. Grafik data kinerja untuk klaster dirancang untuk memberi Anda akses ke data untuk menjawab pertanyaan kinerja Anda yang paling umum. Untuk beberapa data kinerja (lihat [Memantau Amazon Redshift menggunakan metrik CloudWatch](#)), Anda juga dapat menggunakan CloudWatch untuk menyesuaikan grafik metrik lebih lanjut. Misalnya, Anda dapat memilih waktu yang lebih lama atau menggabungkan metrik di seluruh cluster. Untuk informasi selengkapnya tentang bekerja dengan CloudWatch konsol, lihat [Bekerja dengan metrik kinerja di konsol CloudWatch](#).

Tonton video berikut untuk mempelajari cara memantau, mengisolasi, dan mengoptimalkan kueri menggunakan fitur pemantauan kueri di konsol Amazon Redshift: [Pemantauan Kueri dengan Amazon Redshift](#).

Topik

- [Melihat data kinerja cluster](#)
- [Melihat data riwayat kueri](#)
- [Melihat data kinerja database](#)
- [Melihat data konkurensi beban kerja dan penskalaan konkurensi](#)
- [Melihat kueri dan beban](#)
- [Melihat metrik cluster selama operasi pemuatan](#)
- [Menganalisis kinerja beban kerja](#)
- [Mengelola alarm-alarm](#)
- [Bekerja dengan metrik kinerja di konsol CloudWatch](#)

Melihat data kinerja cluster

Dengan menggunakan metrik klaster di Amazon Redshift, Anda dapat melakukan tugas kinerja umum berikut:

- Tentukan apakah metrik klaster tidak normal pada rentang waktu tertentu dan, jika demikian, identifikasi kueri yang bertanggung jawab atas hit kinerja.
- Periksa apakah kueri historis atau saat ini memengaruhi kinerja klaster. Jika Anda mengidentifikasi kueri bermasalah, Anda dapat melihat detailnya termasuk kinerja klaster selama eksekusi kueri. Anda dapat menggunakan informasi ini dalam mendiagnosis mengapa kueri lambat dan apa yang dapat dilakukan untuk meningkatkannya.

Untuk melihat data kinerja

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, lalu pilih nama cluster dari daftar untuk membuka detailnya. Rincian cluster ditampilkan, yang dapat mencakup kinerja Cluster, pemantauan Kueri, Database, Datashares, Jadwal, Pemeliharaan, dan tab Properti.
3. Pilih tab Kinerja klaster untuk informasi kinerja termasuk yang berikut ini:
 - Pemanfaatan CPU
 - Persentase ruang disk yang digunakan

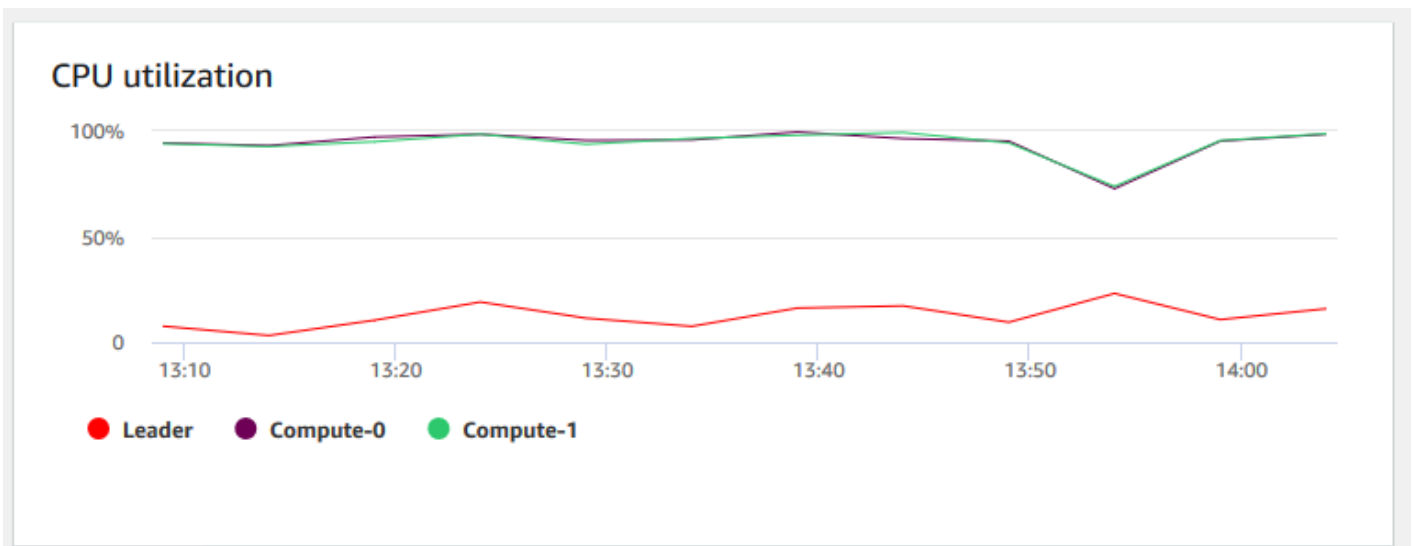
- Koneksi database
- Status kondisi
- Durasi kueri
- Hasil kueri
- Aktivitas penskalaan konkurensi

Banyak lagi metrik yang tersedia. Untuk melihat metrik yang tersedia dan memilih yang ditampilkan, pilih ikon Preferensi.

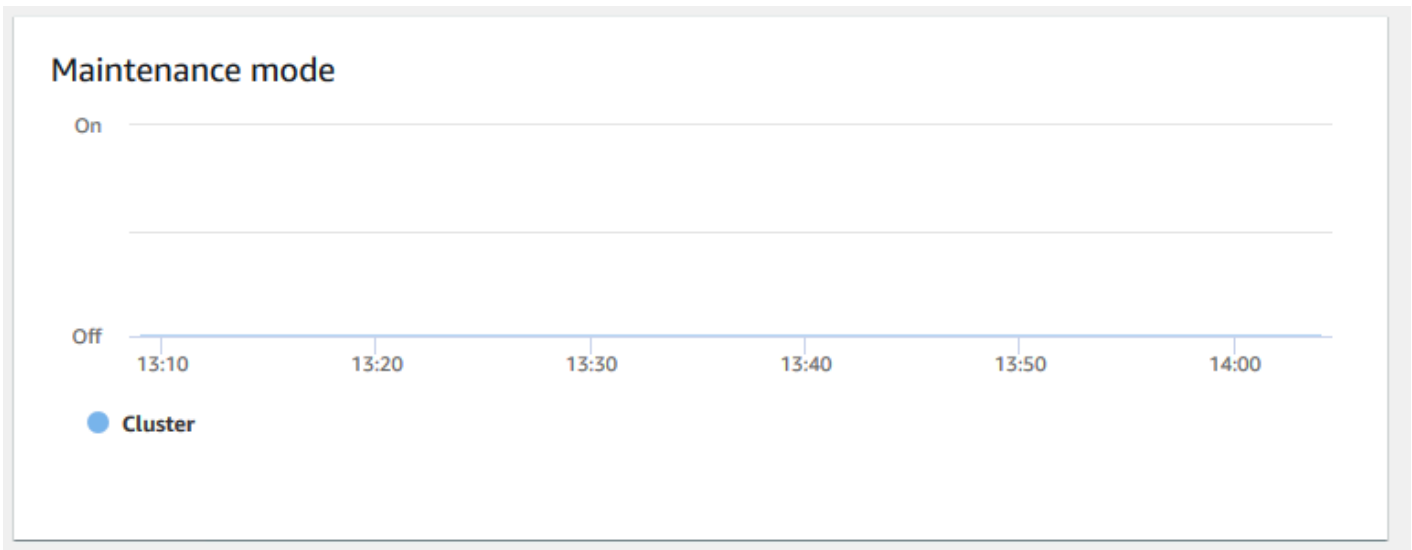
Grafik kinerja cluster

Contoh berikut menunjukkan beberapa grafik yang ditampilkan di konsol Amazon Redshift baru.

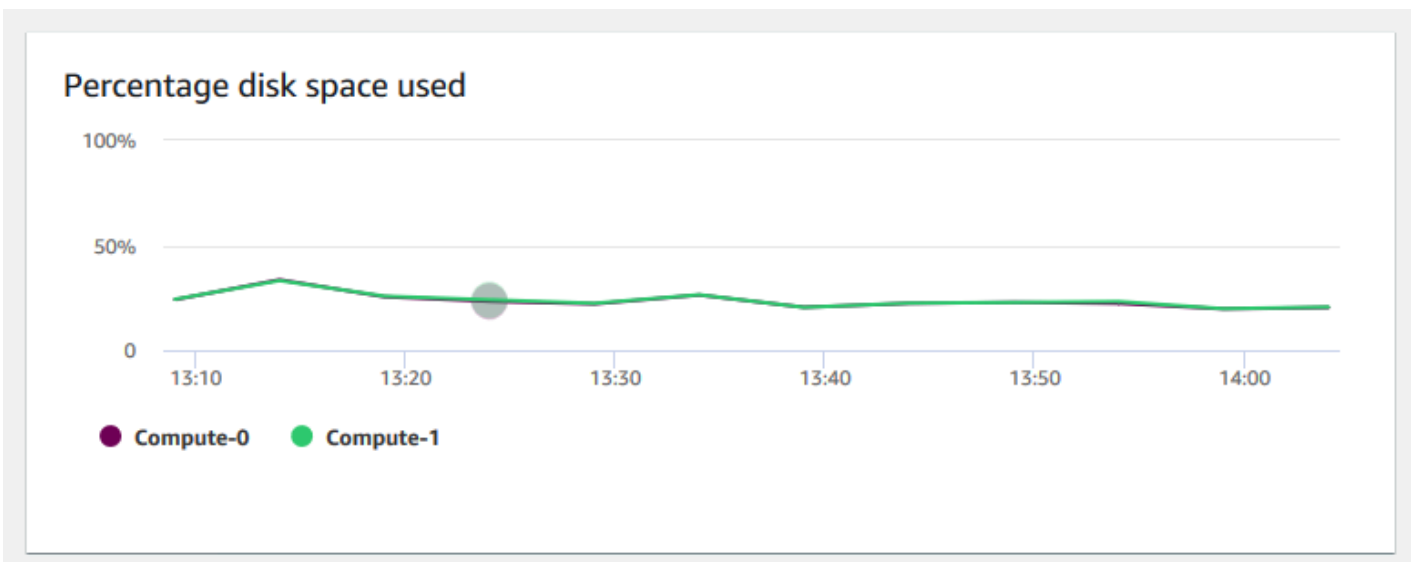
- Pemanfaatan CPU — Menunjukkan persentase pemanfaatan CPU untuk semua node (pemimpin dan komputasi). Untuk menemukan waktu ketika penggunaan klaster terendah sebelum menjadwalkan migrasi cluster atau operasi yang memakan sumber daya lainnya, pantau bagan ini untuk melihat pemanfaatan CPU per individu atau semua node.



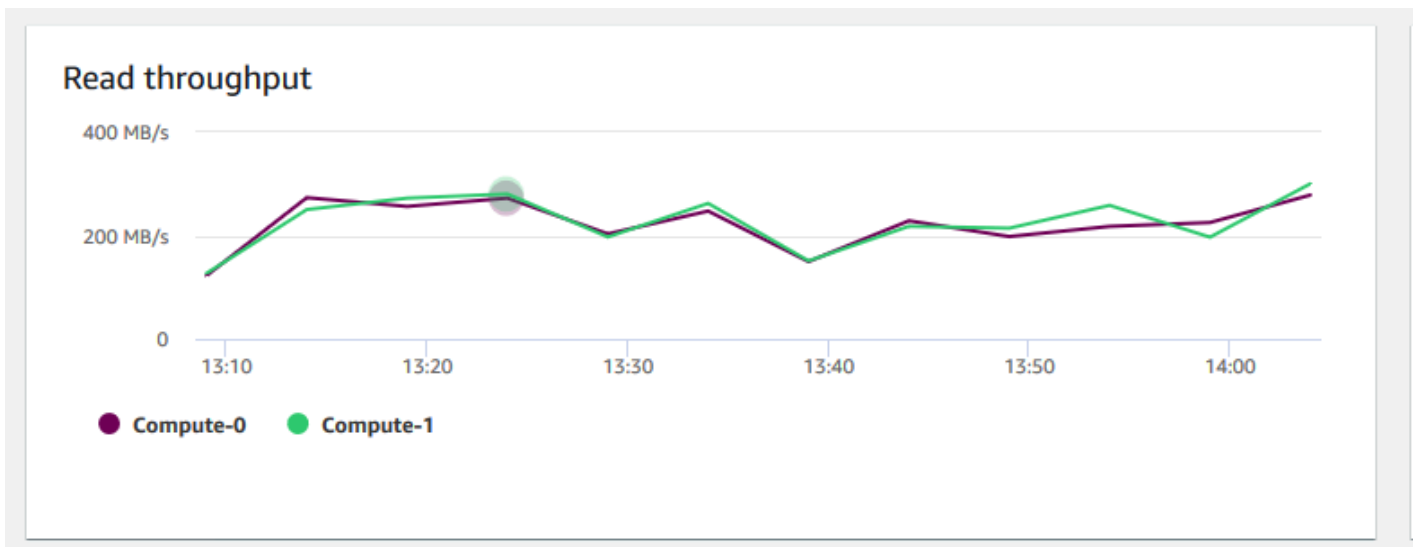
- Mode pemeliharaan - Menunjukkan apakah cluster berada dalam mode pemeliharaan pada waktu yang dipilih dengan menggunakan On dan Off indikator. Anda dapat melihat waktu ketika cluster sedang menjalani pemeliharaan. Anda kemudian dapat mengkorelasikan waktu ini dengan operasi yang dilakukan ke cluster untuk memperkirakan waktu henti di masa depan untuk peristiwa berulang.



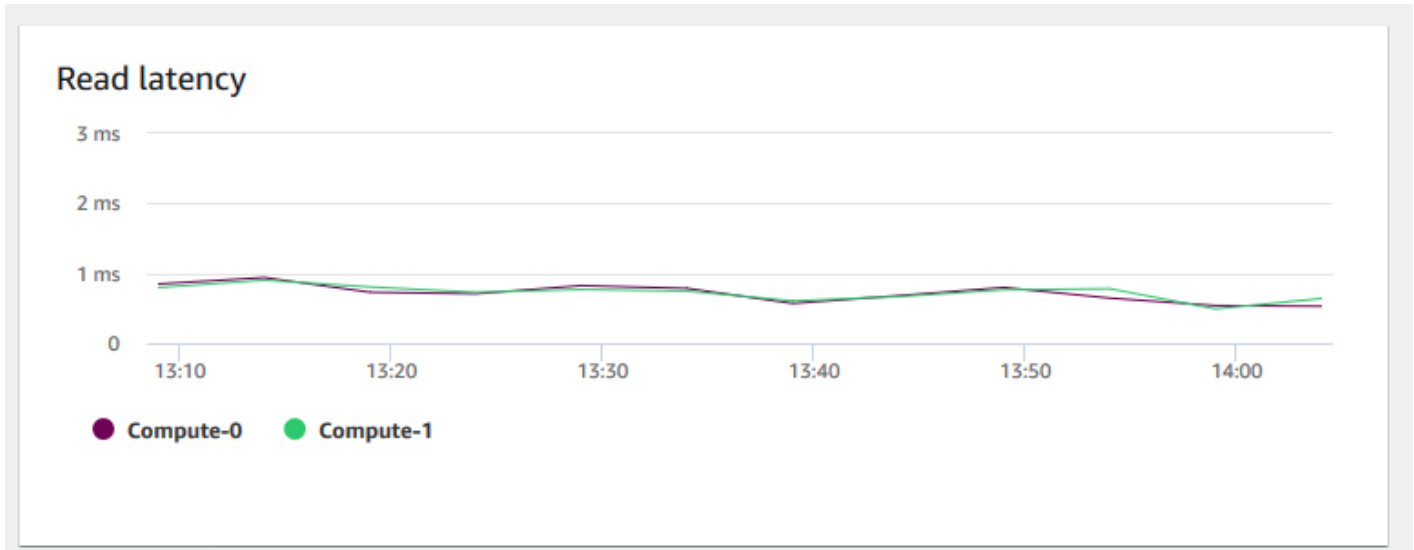
- **Persentase ruang disk yang digunakan** - Menunjukkan persentase penggunaan ruang disk per setiap node komputasi, dan bukan untuk cluster secara keseluruhan. Anda dapat menjelajahi bagan ini untuk memantau pemanfaatan disk. Operasi pemeliharaan seperti VACUUM dan COPY menggunakan ruang penyimpanan sementara menengah untuk operasi penyortiran mereka, sehingga lonjakan penggunaan disk diharapkan.



- **Baca throughput** — Menunjukkan jumlah rata-rata megabyte yang dibaca dari disk per detik. Anda dapat mengevaluasi bagan ini untuk memantau aspek fisik cluster yang sesuai. Throughput ini tidak termasuk lalu lintas jaringan antara instance di cluster dan volumenya.



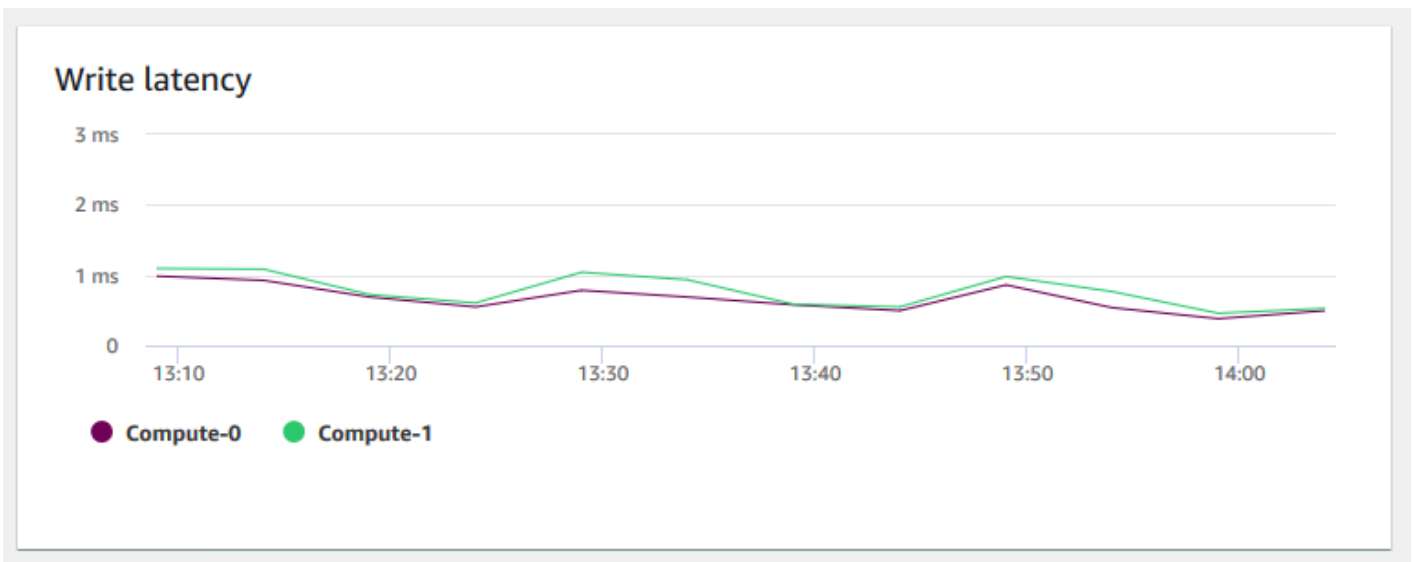
- **Baca latensi** - Menunjukkan jumlah rata-rata waktu yang dibutuhkan untuk operasi I/O baca disk per milidetik. Anda dapat melihat waktu respons untuk mengembalikan data. Ketika latensi tinggi, itu berarti bahwa pengirim menghabiskan lebih banyak waktu idle (tidak mengirim paket baru), yang mengurangi seberapa cepat throughput tumbuh.



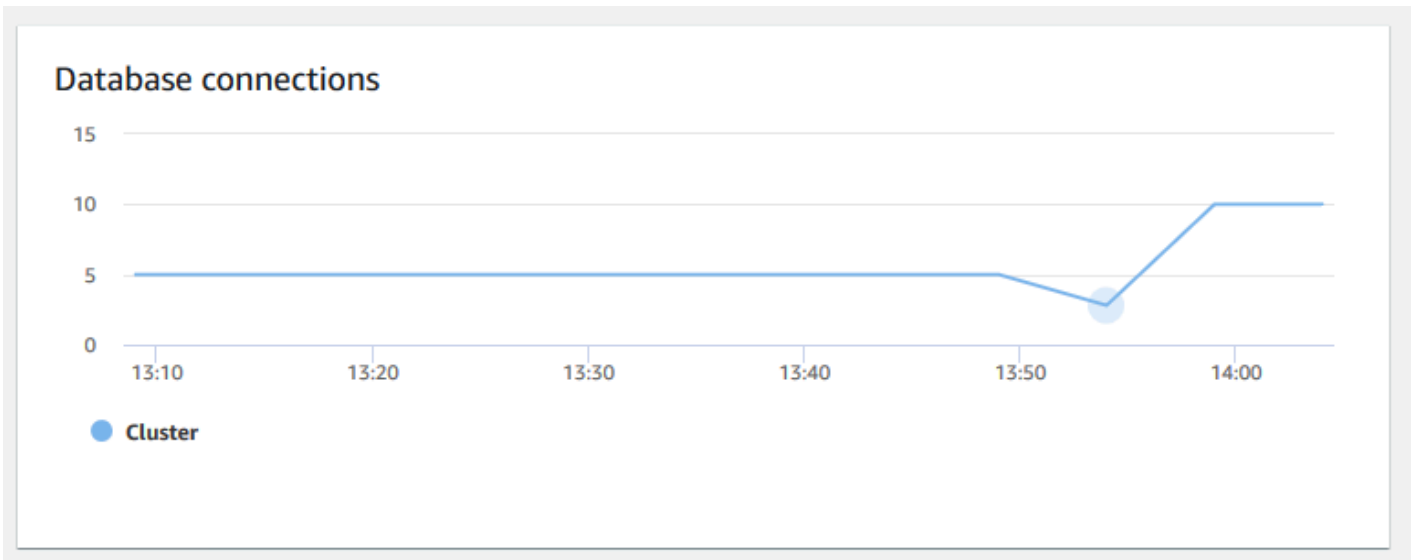
- **Tulis throughput** — Menunjukkan jumlah rata-rata megabyte yang ditulis ke disk per detik. Anda dapat mengevaluasi metrik ini untuk memantau aspek fisik cluster yang sesuai. Throughput ini tidak termasuk lalu lintas jaringan antara instance di cluster dan volumenya.



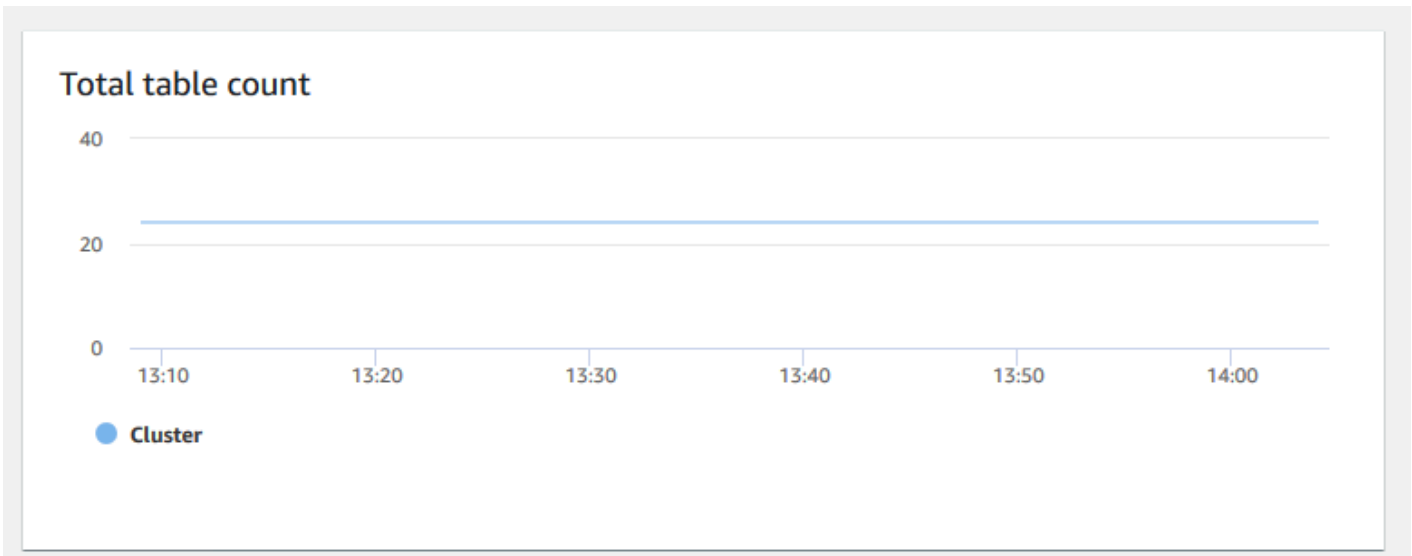
- Latensi tulis - Menunjukkan jumlah rata-rata waktu dalam milidetik yang diambil untuk operasi I/O tulis disk. Anda dapat mengevaluasi waktu untuk pengakuan tulis untuk kembali. Ketika latensi tinggi, itu berarti bahwa pengirim menghabiskan lebih banyak waktu idle (tidak mengirim paket baru), yang mengurangi seberapa cepat throughput tumbuh.



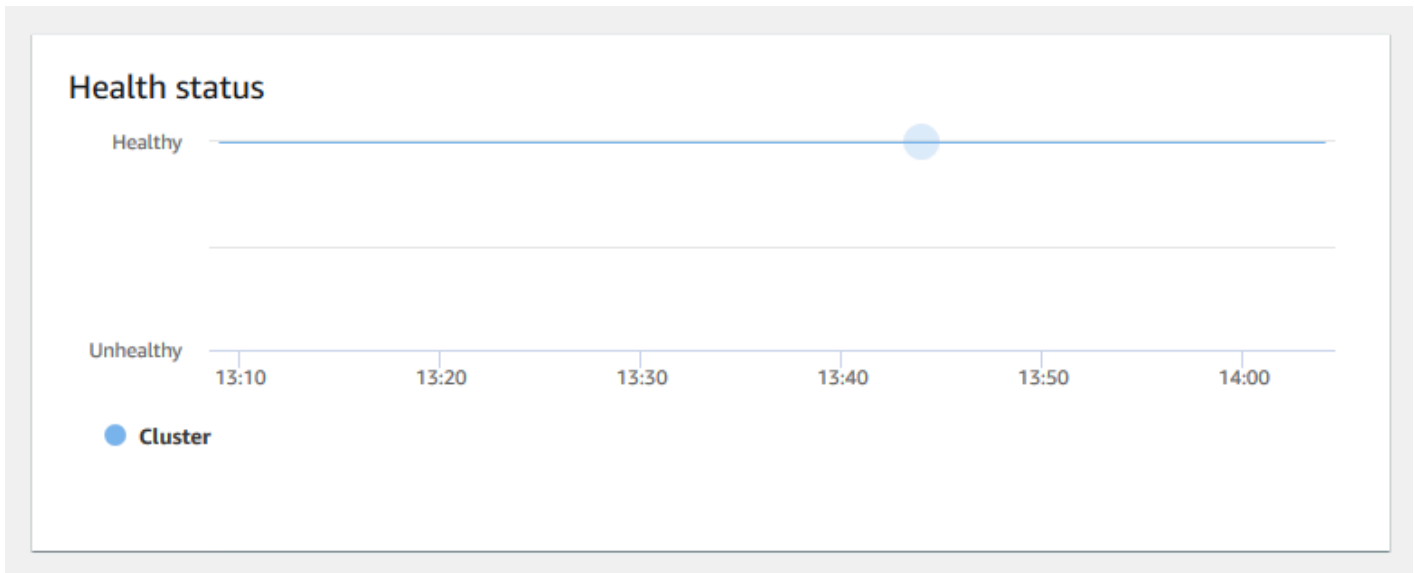
- Koneksi database - Menunjukkan jumlah koneksi database ke sebuah cluster. Anda dapat menggunakan bagan ini untuk melihat berapa banyak koneksi yang dibuat ke database dan menemukan waktu ketika penggunaan cluster terendah.



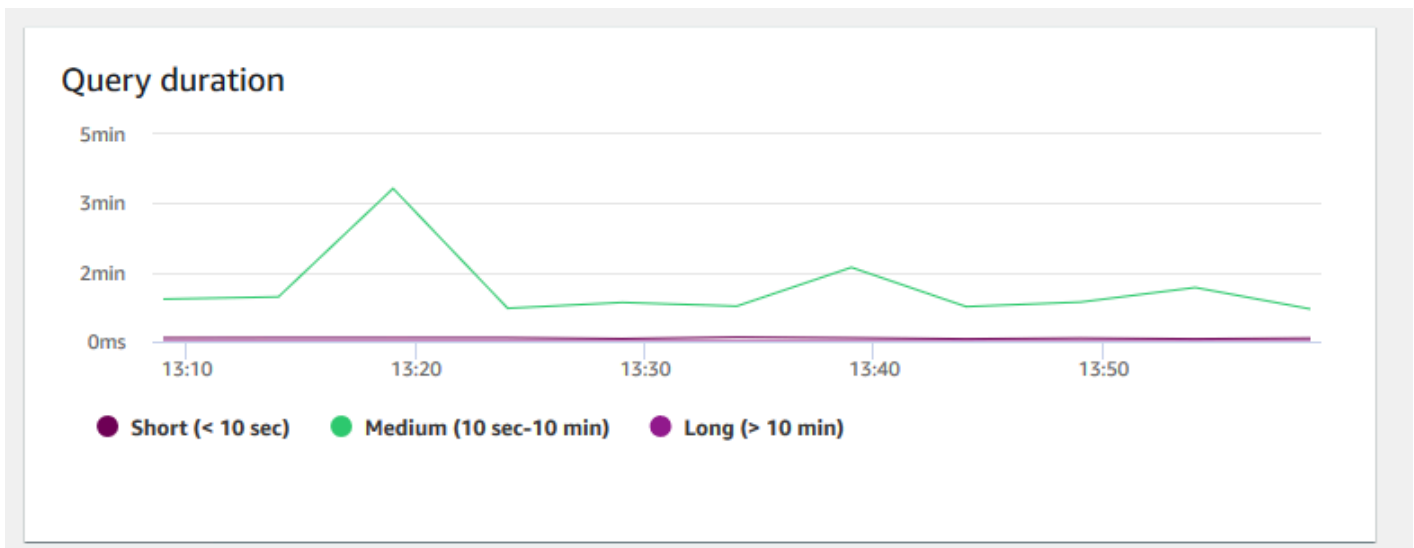
- Jumlah tabel total - Menunjukkan jumlah tabel pengguna yang terbuka pada titik waktu tertentu dalam sebuah cluster. Anda dapat memantau kinerja cluster saat jumlah tabel terbuka tinggi.



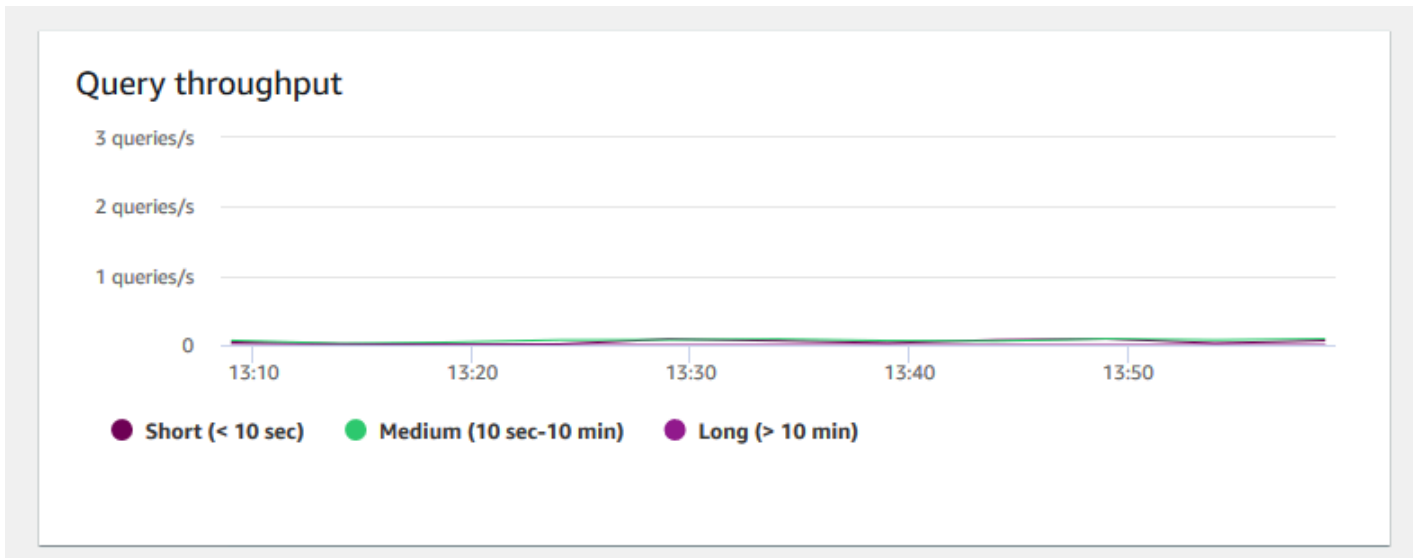
- Status Kesehatan — Menunjukkan kesehatan cluster sebagai Healthy atau Unhealthy. Jika cluster dapat terhubung ke database dan melakukan query sederhana berhasil, cluster dianggap sehat. Kalau tidak, cluster tidak sehat. Status yang tidak sehat dapat terjadi ketika database cluster berada di bawah beban yang sangat berat atau jika ada masalah konfigurasi dengan database di cluster.



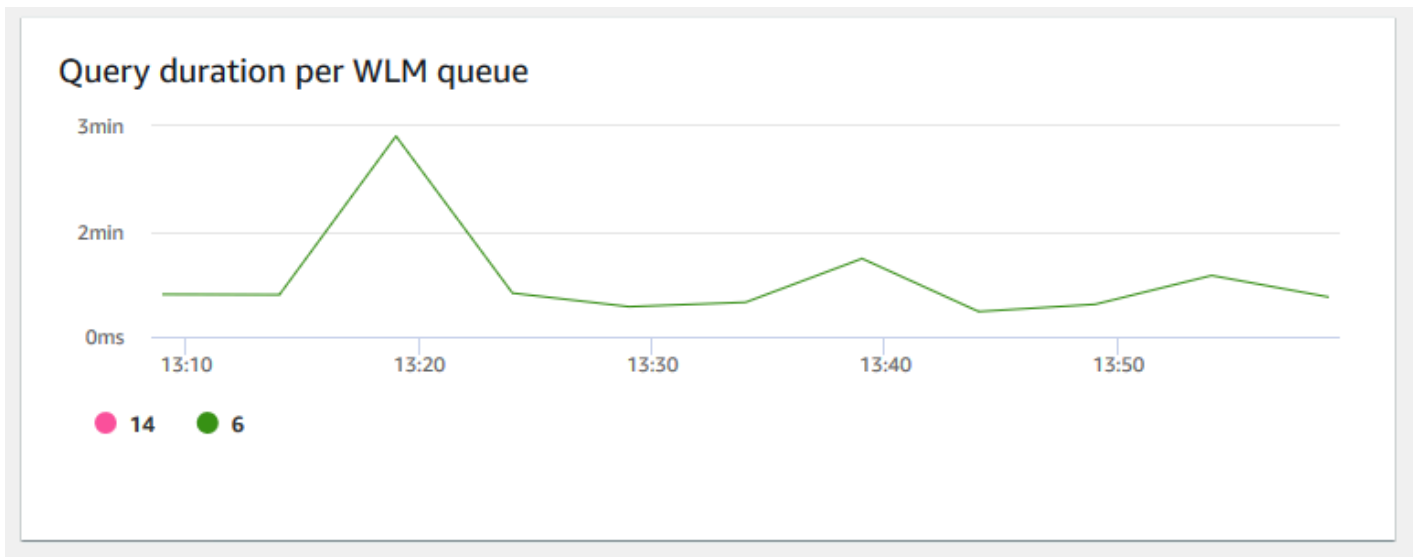
- Durasi kueri - Menunjukkan jumlah waktu rata-rata untuk menyelesaikan kueri dalam mikrodetik. Anda dapat membandingkan data pada bagan ini untuk mengukur kinerja I/O dalam cluster dan menyetel kueri yang paling memakan waktu jika perlu.



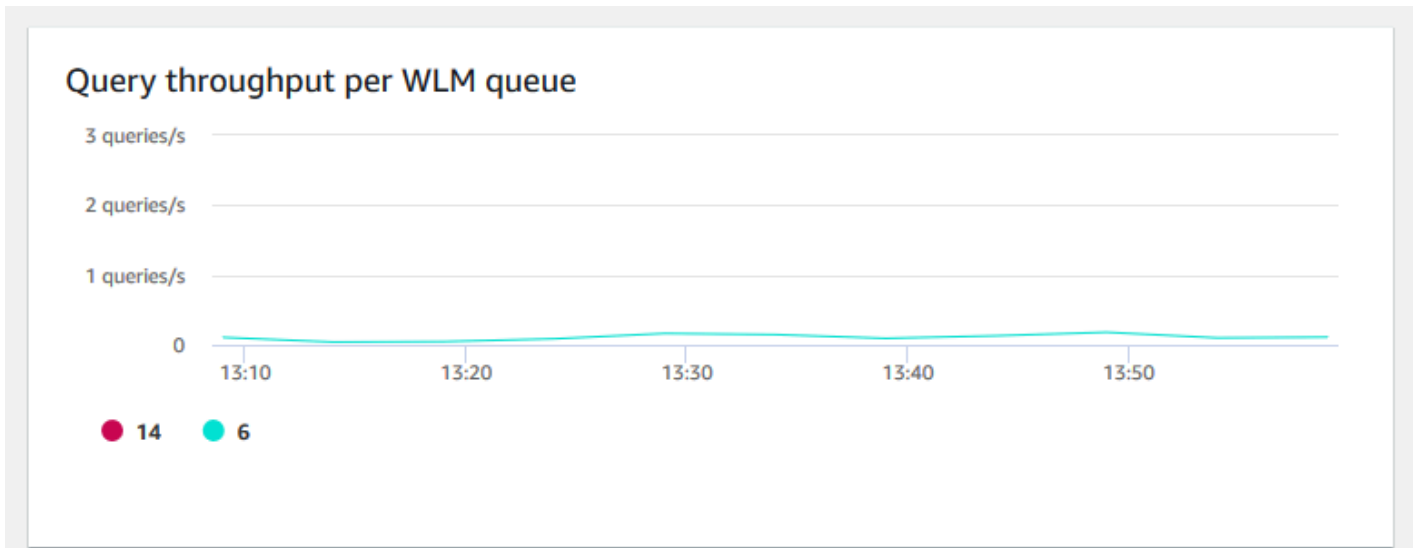
- Throughput kueri - Menunjukkan jumlah rata-rata kueri yang diselesaikan per detik. Anda dapat menganalisis data pada bagan ini untuk mengukur kinerja database dan mengkarakterisasi kemampuan sistem untuk mendukung beban kerja multipengguna secara seimbang.



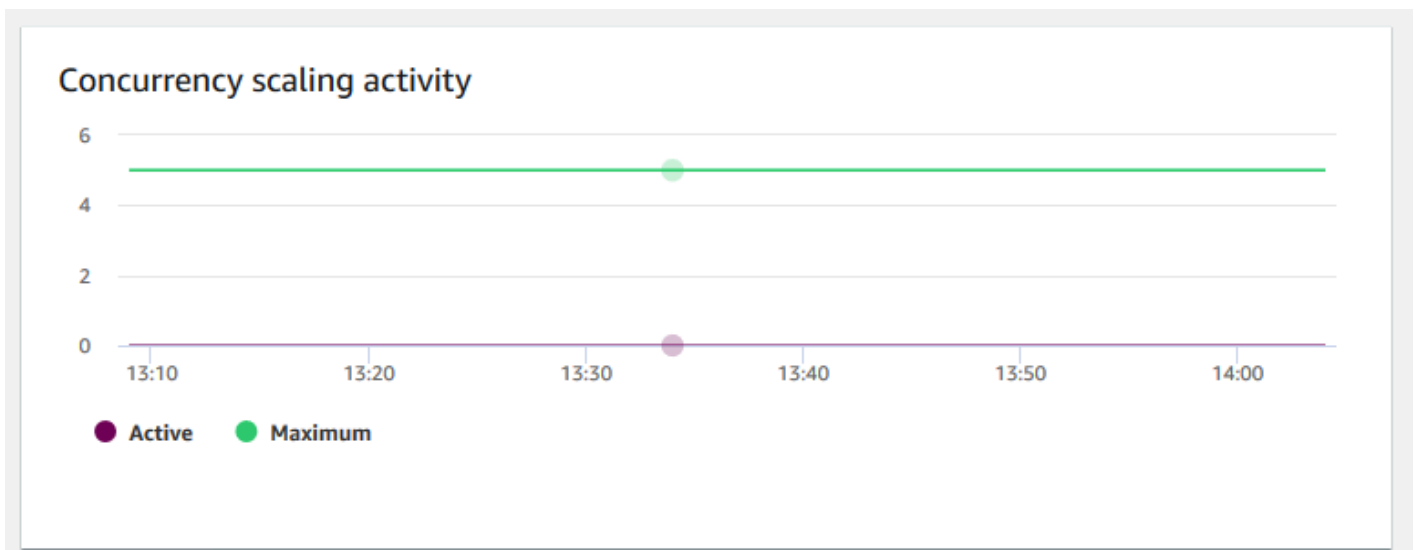
- Durasi kueri per antrian WLM - Menunjukkan jumlah waktu rata-rata untuk menyelesaikan kueri dalam mikrodetik. Anda dapat membandingkan data pada bagan ini untuk mengukur kinerja I/O per antrian WLM dan menyetel kueri yang paling memakan waktu jika perlu.



- Throughput kueri per antrian WLM - Menunjukkan jumlah rata-rata kueri yang diselesaikan per detik. Anda dapat menganalisis data pada bagan ini untuk mengukur kinerja database per antrian WLM.



- **Aktivitas penskalaan konkurensi** — Menunjukkan jumlah cluster penskalaan konkurensi aktif. Saat penskalaan konkurensi diaktifkan, Amazon Redshift secara otomatis menambahkan kapasitas kluster tambahan saat Anda membutuhkannya untuk memproses peningkatan kueri baca bersamaan.



Melihat data riwayat kueri

Anda dapat menggunakan metrik riwayat kueri di Amazon Redshift untuk melakukan hal berikut:

- Mengisolasi dan mendiagnosis masalah kinerja kueri.
- Bandingkan metrik runtime kueri dan metrik kinerja cluster pada timeline yang sama untuk melihat bagaimana keduanya mungkin terkait. Melakukannya membantu mengidentifikasi kueri yang

berkinerja buruk, mencari kueri bottleneck, dan menentukan apakah Anda perlu mengubah ukuran klaster untuk beban kerja Anda.

- Telusuri detail kueri tertentu dengan memilihnya di timeline. Ketika Query ID dan properti lainnya ditampilkan berturut-turut di bawah grafik, maka Anda dapat memilih kueri untuk melihat detail kueri. Detail termasuk, misalnya, pernyataan SQL query, rincian eksekusi, dan rencana kueri. Untuk informasi selengkapnya, lihat [Melihat detail kueri](#).
- Tentukan apakah pekerjaan pemuatan Anda berhasil diselesaikan dan penuhi perjanjian tingkat layanan (SLA) Anda.

Untuk menampilkan data riwayat kueri

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Pada menu navigasi, pilih Cluster, lalu pilih nama cluster dari daftar untuk membuka detailnya. Rincian cluster ditampilkan, yang dapat mencakup kinerja Cluster, pemantauan Kueri, Database, Datashares, Jadwal, Pemeliharaan, dan tab Properti.
3. Pilih tab Pemantauan kueri untuk metrik tentang kueri Anda.
4. Di bagian Pemantauan kueri, pilih tab Riwayat kueri.

Menggunakan kontrol pada jendela, Anda dapat beralih antara daftar Query dan metrik Cluster.

Saat Anda memilih daftar Kueri, tab menyertakan grafik berikut:

- Query runtime — Aktivitas query pada timeline. Gunakan grafik ini untuk melihat kueri mana yang berjalan dalam jangka waktu yang sama. Pilih kueri untuk melihat detail eksekusi kueri lainnya. Sumbu x menunjukkan periode yang dipilih. Anda dapat memfilter kueri grafik dengan menjalankan, menyelesaikan, memuat, dan sebagainya. Setiap bar mewakili kueri, dan panjang bar mewakili runtime dari awal bar sampai akhir. Kueri dapat mencakup pernyataan manipulasi data SQL (seperti SELECT, INSERT, DELETE) dan load (seperti COPY). Secara default, 100 kueri berjalan terpanjang teratas ditampilkan untuk periode waktu yang dipilih.
- Kueri dan beban — Daftar kueri dan beban yang berjalan di cluster. Jendela menyertakan opsi untuk Menghentikan kueri jika kueri sedang berjalan.

Saat Anda memilih metrik Cluster, tab menyertakan grafik berikut:

- Query runtime — Aktivitas query pada timeline. Gunakan grafik ini untuk melihat kueri mana yang berjalan dalam jangka waktu yang sama. Pilih kueri untuk melihat detail eksekusi kueri lainnya.
- Pemanfaatan CPU — Pemanfaatan CPU cluster oleh node pemimpin dan rata-rata node komputasi.
- Kapasitas penyimpanan yang digunakan — Persentase kapasitas penyimpanan yang digunakan.
- Koneksi database aktif — Jumlah koneksi database aktif ke cluster.

Pertimbangkan hal berikut saat bekerja dengan grafik riwayat kueri:

- Pilih bilah yang mewakili kueri tertentu pada bagan runtime Kueri untuk melihat detail tentang kueri tersebut. Anda juga dapat, memilih ID kueri pada Kueri dan memuat daftar untuk melihat detailnya.
- Anda dapat menggesek untuk memilih bagian dari bagan runtime Query untuk memperbesar untuk menampilkan periode waktu tertentu.
- Pada bagan runtime Query, agar semua data dipertimbangkan oleh filter yang Anda pilih, teruskan halaman melalui semua halaman yang tercantum pada daftar Kueri dan muat.
- Anda dapat mengubah kolom mana dan jumlah baris yang ditampilkan pada daftar Kueri dan beban menggunakan jendela preferensi yang ditampilkan oleh ikon roda gigi pengaturan.
- Daftar Kueri dan beban juga dapat ditampilkan dengan menavigasi dari ikon Kueri navigator kiri, Kueri, dan beban. Untuk informasi selengkapnya, lihat [Melihat kueri dan beban](#).

Grafik riwayat kueri

Contoh berikut menunjukkan grafik yang ditampilkan di konsol Amazon Redshift baru.

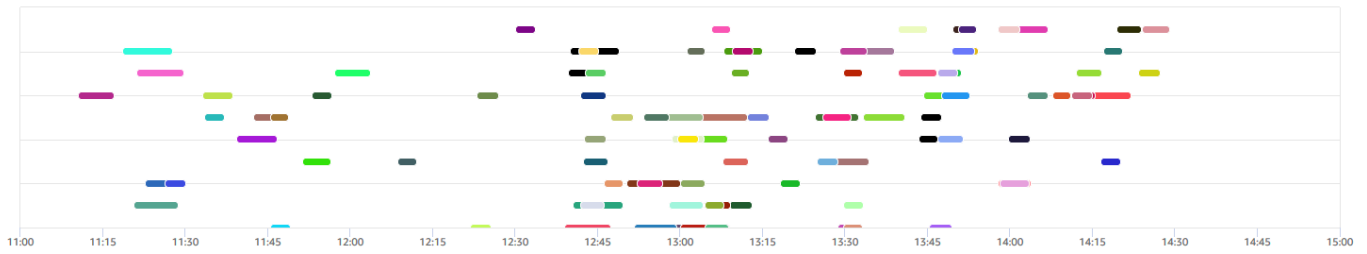
Note

Grafik konsol Amazon Redshift hanya berisi data untuk 100.000 kueri terbaru.

- Waktu proses kueri

Query runtime

The query activity on a timeline. Use this graph to see which queries are running in the same timeframe. Choose a query to view more query execution details.



- Kueri dan beban

Queries and loads(100)

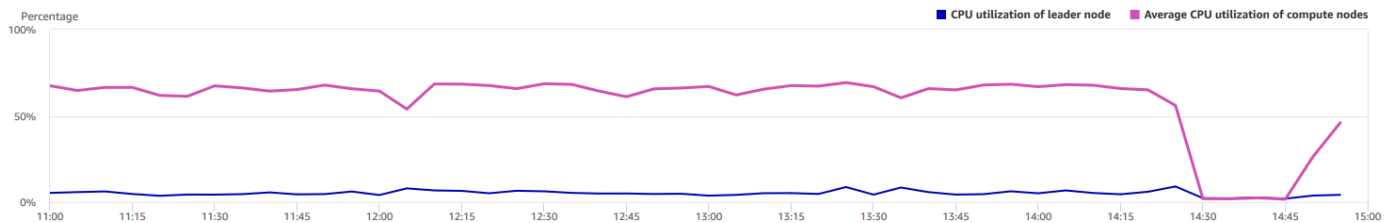
Filter queries

<input type="checkbox"/>	Start time	Query	Status	Duration	SQL	Copy SQL	User	Transaction ID
<input type="checkbox"/>	Apr 13th, 2020 01:00:55 PM 8 days ago	69248	Completed	11 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105501
<input type="checkbox"/>	Apr 13th, 2020 12:58:07 PM 8 days ago	69199	Completed	11 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105414
<input type="checkbox"/>	Apr 13th, 2020 12:54:15 PM 8 days ago	69111,69265,69253	Completed	10 min	with /* query_templates/query22.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105283
<input type="checkbox"/>	Apr 13th, 2020 12:50:17 PM 8 days ago	68976	Completed	10 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105128
<input type="checkbox"/>	Apr 13th, 2020 01:29:23 PM 8 days ago	70089	Completed	10 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	106659
<input type="checkbox"/>	Apr 13th, 2020 11:18:35 AM 8 days ago	65543	Completed	9 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_05cu_run01_nocache.stream-quer ...	Copy	rsperf	101092
<input type="checkbox"/>	Apr 13th, 2020 12:40:30 PM 8 days ago	68729	Completed	9 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	104789

- Pemanfaatan CPU

CPU utilization

The CPU utilization of the cluster by leader node and average of compute nodes.



- Kapasitas penyimpanan yang digunakan

Storage capacity used

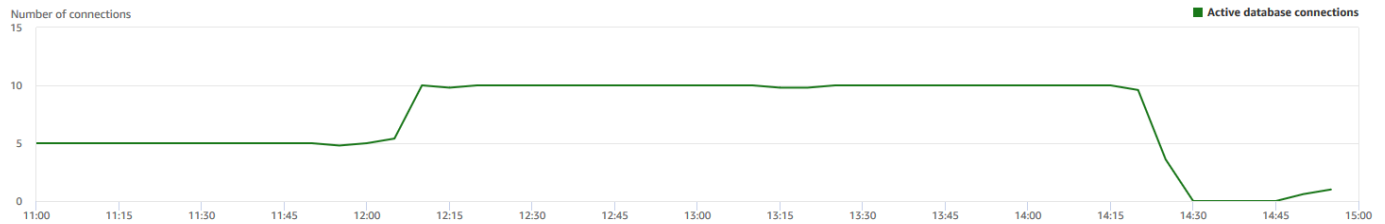
The percent of the storage capacity used.



- Koneksi database aktif

Active database connections

The number of active database connections to the cluster.



Melihat data kinerja database

Anda dapat menggunakan metrik kinerja database di Amazon Redshift untuk melakukan hal berikut:

- Analisis waktu yang dihabiskan oleh kueri dengan memproses tahapan. Anda dapat mencari tren yang tidak biasa dalam jumlah waktu yang dihabiskan dalam satu panggung.
- Analisis jumlah kueri, durasi, dan throughput kueri berdasarkan rentang durasi (pendek, sedang, panjang).
- Cari tren tentang waktu tunggu kueri berdasarkan prioritas kueri (Terendah, Rendah, Normal, Tinggi, Tertinggi, Kritis).
- Cari tren dalam durasi kueri, throughput, atau waktu tunggu berdasarkan antrian WLM.

Untuk menampilkan data kinerja database

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, lalu pilih nama cluster dari daftar untuk membuka detailnya. Detail cluster ditampilkan, termasuk kinerja Cluster, pemantauan Query, Database, Datashares, Jadwal, Pemeliharaan, dan tab Properti.
3. Pilih tab Pemantauan kueri untuk metrik tentang kueri Anda.
4. Di bagian Pemantauan kueri, pilih tab Kinerja basis data.

Menggunakan kontrol di jendela, Anda dapat beralih antara metrik Cluster dan metrik antrian WLM.

Saat Anda memilih metrik Cluster, tab menyertakan grafik berikut:

- Kerusakan eksekusi beban kerja - Waktu yang digunakan dalam tahap pemrosesan kueri.
- Kueri berdasarkan rentang durasi — Jumlah kueri pendek, menengah, dan panjang.
- Throughput kueri — Jumlah rata-rata kueri yang diselesaikan per detik.
- Durasi kueri — Jumlah rata-rata waktu untuk menyelesaikan kueri.
- Waktu tunggu antrian rata-rata berdasarkan prioritas — Total waktu kueri yang dihabiskan menunggu di antrian WLM berdasarkan prioritas kueri.

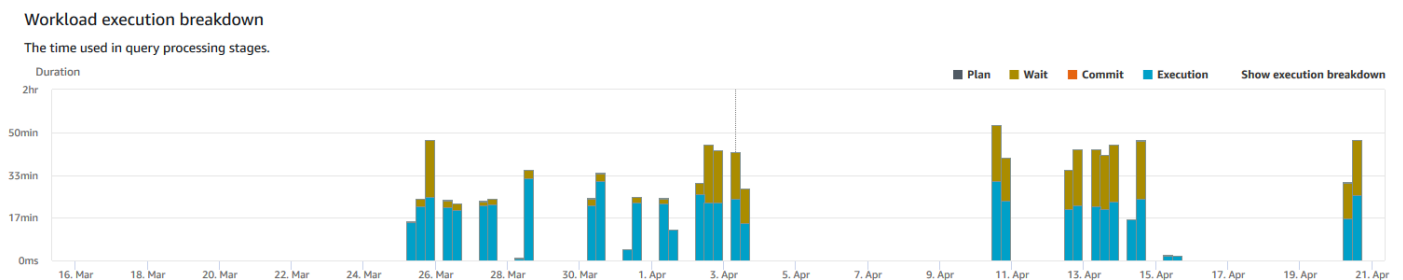
Saat Anda memilih metrik antrian WLM, tab menyertakan grafik berikut:

- Durasi kueri berdasarkan antrian — Durasi kueri rata-rata menurut antrian WLM.
- Hasil kueri berdasarkan antrian — Jumlah rata-rata kueri yang diselesaikan per detik oleh antrian WLM.
- Waktu tunggu kueri berdasarkan antrian — Durasi rata-rata kueri yang dihabiskan menunggu dengan antrian WLM.

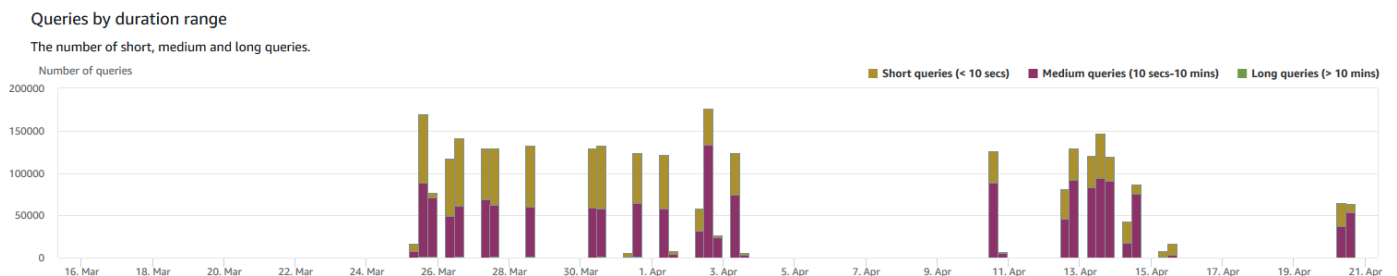
Grafik kinerja database

Contoh berikut menunjukkan grafik yang ditampilkan di konsol Amazon Redshift baru.

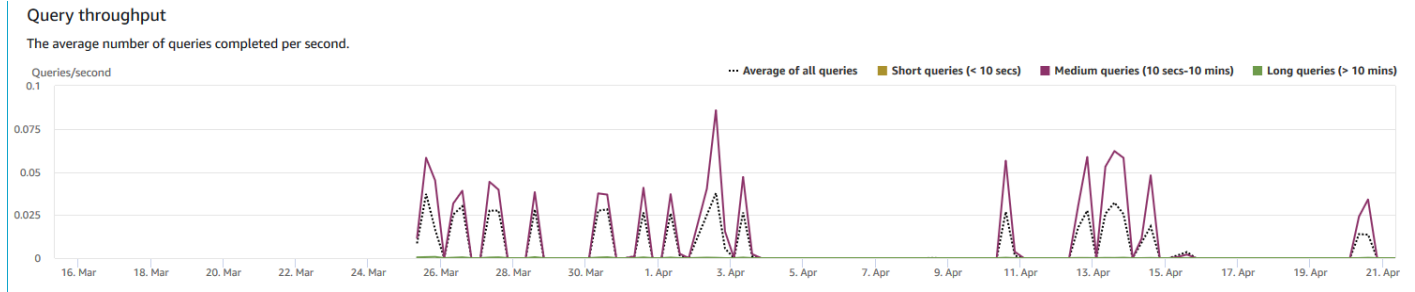
- Rincian eksekusi beban kerja



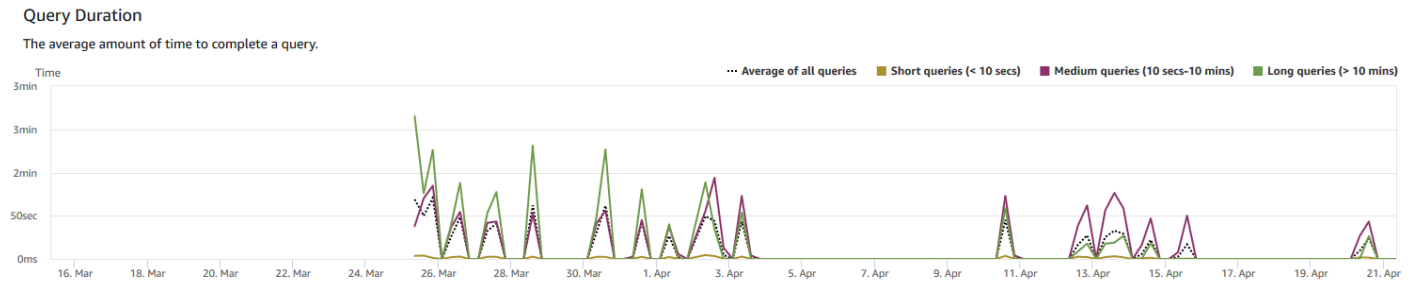
- Kueri berdasarkan rentang durasi



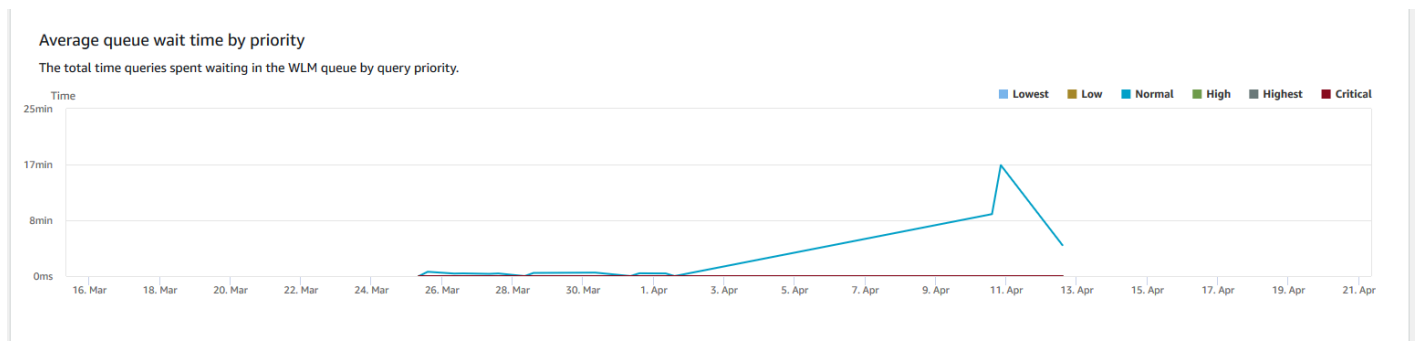
- Hasil kueri



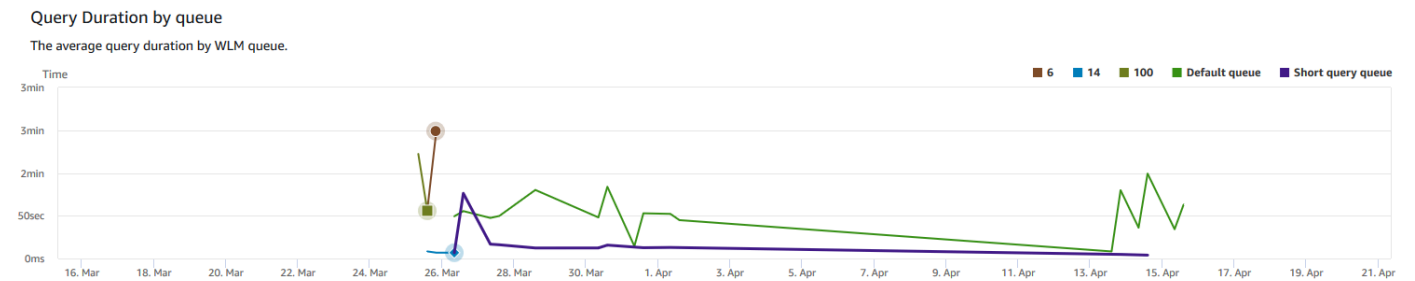
- Durasi kueri



- Waktu tunggu antrian rata-rata berdasarkan prioritas



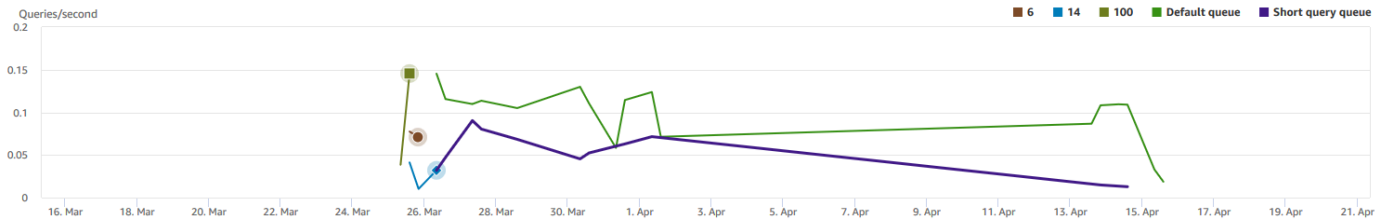
- Durasi kueri berdasarkan antrian



- Hasil kueri berdasarkan antrian

Query throughput by queue

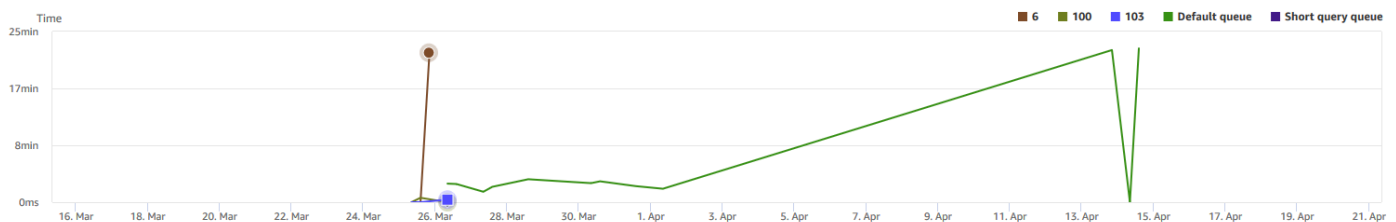
The average number of queries completed per second by WLM queue.



- Kueri waktu tunggu dengan antrian

Query wait time by queue

The average duration of queries spent waiting by WLM queue.



Melihat data konkurensi beban kerja dan penskalaan konkurensi

Dengan menggunakan metrik penskalaan konkurensi di Amazon Redshift, Anda dapat melakukan hal berikut:

- Analisis apakah Anda dapat mengurangi jumlah kueri antrian dengan mengaktifkan penskalaan konkurensi. Anda dapat membandingkan dengan antrian WLM atau untuk semua antrian WLM.
- Lihat aktivitas penskalaan konkurensi dalam kluster penskalaan konkurensi. Ini dapat memberi tahu Anda jika penskalaan konkurensi dibatasi oleh `max_concurrency_scaling_clusters`. Jika demikian, Anda dapat memilih untuk meningkatkan `max_concurrency_scaling_clusters` parameter DB.
- Lihat total penggunaan penskalaan konkurensi yang dijumlahkan di semua cluster penskalaan konkurensi.

Untuk menampilkan data penskalaan konkurensi

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Pada menu navigasi, pilih Cluster, lalu pilih nama cluster dari daftar untuk membuka detailnya. Rincian cluster ditampilkan, yang dapat mencakup kinerja Cluster, pemantauan Kueri, Database, Datashares, Jadwal, Pemeliharaan, dan tab Properti.
3. Pilih tab Pemantauan kueri untuk metrik tentang kueri Anda.
4. Di bagian Pemantauan kueri, pilih tab Konkurensi beban kerja.

Tab ini mencakup grafik berikut:

- Query antrian vs Menjalankan di cluster — Jumlah kueri yang berjalan (dari cluster utama dan cluster penskalaan konkurensi) dibandingkan dengan jumlah kueri yang menunggu di semua antrian WLM di cluster.
- Query antrian vs Menjalankan per antrian — Jumlah kueri yang berjalan (dari cluster utama dan cluster penskalaan konkurensi) dibandingkan dengan jumlah atau kueri yang menunggu di setiap antrian WLM.
- Aktivitas penskalaan konkurensi — Jumlah cluster penskalaan konkurensi yang secara aktif memproses kueri.
- Penggunaan penskalaan konkurensi — Penggunaan cluster penskalaan konkurensi yang memiliki aktivitas pemrosesan kueri aktif.

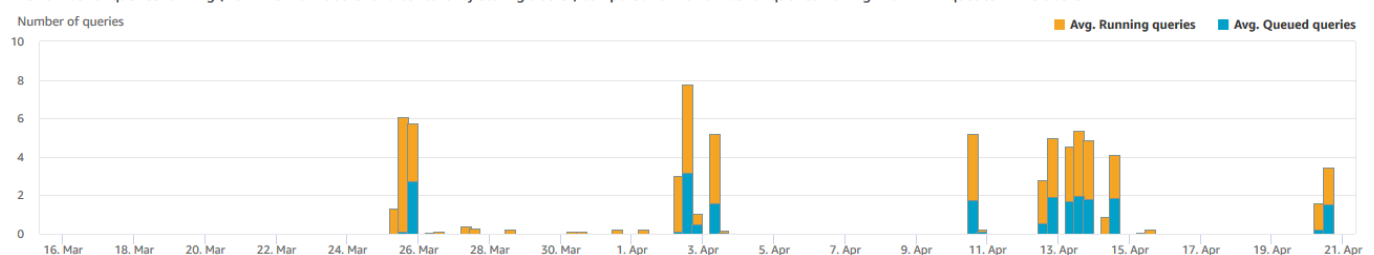
Grafik konkurensi beban kerja

Contoh berikut menunjukkan grafik yang ditampilkan di konsol Amazon Redshift baru. Untuk membuat grafik serupa di Amazon CloudWatch, Anda dapat menggunakan penskalaan konkurensi dan metrik WLM. CloudWatch Untuk informasi selengkapnya tentang CloudWatch metrik untuk Amazon Redshift, lihat. [Memantau Amazon Redshift menggunakan metrik CloudWatch](#)

- Antrian vs Menjalankan kueri di cluster

Queued vs. Running queries on the cluster

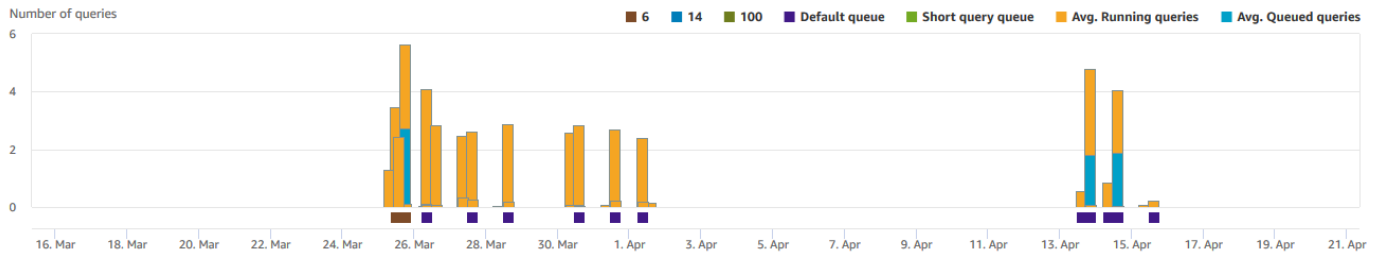
The number of queries running (from the main cluster and concurrency scaling cluster) compared to the number of queries waiting in all WLM queues in the cluster.



- Antrian vs Menjalankan kueri per antrian

Queued vs. Running queries per queue

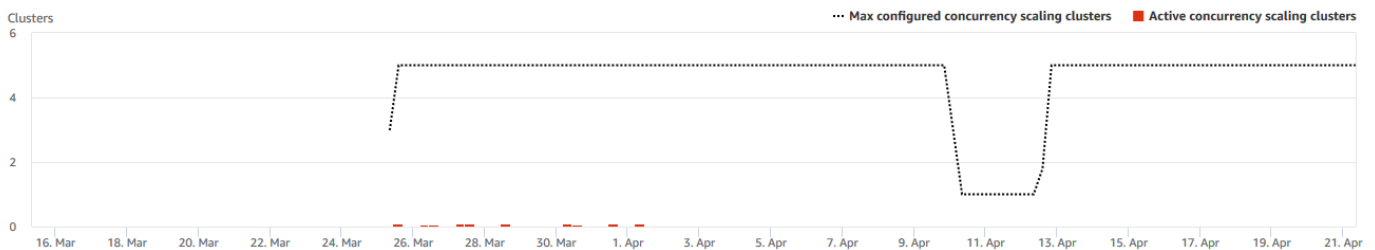
The number of queries running (from the main cluster and concurrency scaling cluster) compared to the number of queries waiting in each WLM queue.



- **Aktivitas penskalaan konkurensi**

Concurrency scaling activity

The number of concurrency scaling clusters that are actively processing queries.



- **Penggunaan penskalaan konkurensi**

Concurrency scaling usage

The usage of concurrency scaling clusters that have active query processing activity.



Melihat kueri dan beban

Konsol Amazon Redshift menyediakan informasi tentang kueri dan beban yang berjalan di database. Anda dapat menggunakan informasi ini untuk mengidentifikasi dan memecahkan masalah kueri yang membutuhkan waktu lama untuk diproses dan yang membuat hambatan mencegah kueri lain diproses secara efisien. Anda dapat menggunakan informasi kueri di konsol Amazon Redshift untuk memantau pemrosesan kueri.

Untuk menampilkan data kinerja kueri

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Kueri dan beban untuk menampilkan daftar kueri untuk akun Anda.

Secara default, daftar menampilkan kueri untuk semua cluster Anda selama 24 jam terakhir. Anda dapat mengubah cakupan tanggal yang ditampilkan di konsol.

Important

Daftar Kueri dan beban menampilkan kueri yang berjalan paling lama di sistem, hingga 100 kueri.

Mengakhiri kueri yang sedang berjalan

Anda juga dapat menggunakan halaman Kueri untuk mengakhiri kueri yang sedang berlangsung.

Note

Kemampuan untuk menghentikan kueri dan pemuatan di konsol Amazon Redshift memerlukan izin khusus. Jika Anda ingin pengguna dapat menghentikan kueri dan pemuatan, pastikan untuk menambahkan `redshift:CancelQuerySession` tindakan ke kebijakan AWS Identity and Access Management (IAM) Anda. Persyaratan ini berlaku baik Anda memilih kebijakan AWS terkelola Amazon Redshift Read Only atau membuat kebijakan kustom di IAM. Pengguna yang memiliki kebijakan Akses Penuh Amazon Redshift sudah memiliki izin yang diperlukan untuk menghentikan kueri dan pemuatan. Untuk informasi selengkapnya tentang tindakan dalam kebijakan IAM untuk Amazon Redshift, lihat [Mengelola akses ke sumber daya](#)

Untuk mengakhiri kueri yang sedang berjalan

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Kueri dan beban untuk menampilkan daftar kueri untuk akun Anda.
3. Pilih kueri berjalan yang ingin Anda akhiri dalam daftar, lalu pilih Hentikan kueri.

Melihat detail kueri

Anda dapat menganalisis detail kueri di konsol Amazon Redshift. Dengan pengenalan kueri, Anda dapat melihat detail kueri. Detail dapat mencakup, misalnya, status penyelesaian kueri, durasi, pernyataan SQL, dan apakah itu kueri pengguna atau yang ditulis ulang oleh Amazon Redshift. Kueri pengguna adalah kueri yang dikirimkan ke Amazon Redshift, baik dari klien SQL atau dihasilkan oleh alat intelijen bisnis. Amazon Redshift mungkin menulis ulang kueri untuk mengoptimalkannya, dan ini dapat menghasilkan beberapa kueri yang ditulis ulang. Meskipun prosesnya dilakukan oleh Amazon Redshift, Anda melihat kueri yang ditulis ulang pada halaman detail kueri bersama dengan kueri pengguna.

Untuk melihat kueri

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Kueri dan beban untuk menampilkan daftar kueri untuk akun Anda. Anda mungkin perlu mengubah pengaturan di halaman ini untuk menemukan kueri Anda.
3. Pilih pengenalan Kueri dalam daftar untuk menampilkan Detail kueri.

Halaman Detail kueri mencakup detail Kueri dan tab paket Kueri dengan metrik tentang kueri.

Metrik mencakup detail tentang kueri seperti waktu mulai, ID kueri, status, dan durasi. Detail lainnya termasuk apakah kueri dijalankan pada cluster utama atau klaster penskalaan konkurensi, dan apakah itu kueri induk atau ditulis ulang.

Menganalisis eksekusi kueri

Untuk menganalisis kueri

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Kueri dan beban untuk menampilkan daftar kueri untuk akun Anda. Anda mungkin perlu mengubah pengaturan di halaman ini untuk menemukan kueri Anda.
3. Pilih pengenalan Kueri dalam daftar untuk menampilkan Detail kueri.

Halaman Detail kueri mencakup detail Kueri dan tab paket Kueri dengan metrik tentang kueri.

Note

Anda juga dapat menavigasi ke halaman Detail kueri dari halaman detail Cluster, tab Riwayat kueri saat Anda menelusuri kueri dalam grafik runtime Kueri.

Halaman detail Query berisi bagian-bagian berikut:

- Daftar kueri yang ditulis ulang, seperti yang ditunjukkan pada gambar berikut.

	Start time	Query	Status	Duration	Executed on	Query type
<input type="radio"/>	Apr 15th, 2020 01:44:44 PM 6 days ago	122927,122928,122929...	Completed	5 min		Parent query
<input checked="" type="radio"/>	Apr 15th, 2020 01:44:44 PM 6 days ago	122927	Completed	4 sec	Main	Rewritten query
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122928	Completed	22 ms	Main	Rewritten query
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122929	Completed	19 ms	Main	Rewritten query
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122931	Completed	5 min	Main	Rewritten query

- Sebuah bagian rincian Query, seperti yang ditunjukkan pada gambar berikut.

Query ID	Cluster	User	Type	Status
122927	✔ dnd-sudhare-qa		Rewritten query	Completed
From April 15, 2020 at 01:44:44 PM To April 15, 2020 at 01:44:48 PM				Total runtime 4sec

- Tab Query details yang berisi SQL yang dijalankan dan detail Eksekusi tentang proses.
- Tab Query plan yang berisi langkah-langkah Query plan dan informasi lain tentang rencana kueri. Tabel ini juga berisi grafik tentang cluster saat kueri dijalankan.
- Status kesehatan cluster

Cluster health status

Cluster health during the workload.

■ Healthy ■ Unhealthy



- Pemanfaatan CPU

CPU utilization

The CPU utilization of the cluster by leader node and average of compute nodes.



- Kapasitas penyimpanan yang digunakan

Storage capacity used

The percent of the storage capacity used.



- Koneksi database aktif

Active database connections

The number of active database connections to the cluster.



Melihat kinerja cluster saat kueri berjalan

Untuk menampilkan kinerja klaster saat kueri dijalankan

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, lalu pilih nama cluster dari daftar untuk membuka detailnya. Rincian cluster ditampilkan, yang dapat mencakup kinerja Cluster, pemantauan Kueri, Database, Datashares, Jadwal, Pemeliharaan, dan tab Properti.
3. Pilih tab Pemantauan kueri untuk detail selengkapnya.

Untuk informasi selengkapnya, lihat [Melihat data riwayat kueri.](#)

Melihat metrik cluster selama operasi pemuatan

Saat Anda melihat kinerja klaster selama operasi pemuatan, Anda dapat mengidentifikasi kueri yang menghabiskan sumber daya dan bertindak untuk mengurangi efeknya. Anda dapat menghentikan beban jika Anda tidak ingin itu berjalan hingga selesai.

Note

Kemampuan untuk menghentikan kueri dan pemuatan di konsol Amazon Redshift memerlukan izin khusus. Jika Anda ingin pengguna dapat menghentikan kueri dan pemuatan, pastikan untuk menambahkan `redshift:CancelQuerySession` tindakan ke kebijakan AWS Identity and Access Management (IAM) Anda. Persyaratan ini berlaku baik Anda memilih kebijakan AWS terkelola Amazon Redshift Read Only atau membuat kebijakan kustom di IAM. Pengguna yang memiliki kebijakan Akses Penuh Amazon Redshift sudah memiliki izin yang diperlukan untuk menghentikan kueri dan pemuatan. Untuk informasi selengkapnya tentang tindakan dalam kebijakan IAM untuk Amazon Redshift, lihat [Mengelola akses ke sumber daya](#)

Untuk menampilkan kinerja cluster selama operasi beban

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, lalu pilih nama cluster dari daftar untuk membuka detailnya. Rincian cluster ditampilkan, yang dapat mencakup kinerja Cluster, pemantauan Kueri, Database, Datashares, Jadwal, Pemeliharaan, dan tab Properti.
3. Pilih tab Pemantauan kueri untuk detail selengkapnya.
4. Di bagian Kueri dan beban, pilih Memuat untuk melihat operasi pemuatan klaster. Jika beban sedang berjalan, Anda dapat mengakhirinya dengan memilih Terminate query.

Menganalisis kinerja beban kerja

Anda bisa mendapatkan tampilan mendetail performa beban kerja Anda dengan melihat bagan rincian eksekusi Workload di konsol. Kami membangun bagan dengan data yang disediakan oleh QueryRuntimeBreakdown metrik. Dengan bagan ini, Anda dapat melihat berapa banyak waktu yang dihabiskan kueri Anda dalam berbagai tahap pemrosesan, seperti menunggu dan merencanakan.

Note

Bagan rincian eksekusi Workload tidak ditampilkan untuk kluster simpul tunggal.

Daftar metrik berikut menjelaskan berbagai tahapan pemrosesan:

- **QueryPlanning:** Waktu yang dihabiskan mengurai dan mengoptimalkan pernyataan SQL.
- **QueryWaiting:** Waktu yang dihabiskan menunggu dalam antrian manajemen beban kerja (WLM).
- **QueryExecutingRead:** Waktu yang dihabiskan untuk menjalankan kueri baca.
- **QueryExecutingInsert:** Waktu yang dihabiskan untuk menjalankan kueri sisipan.
- **QueryExecutingDelete:** Waktu yang dihabiskan untuk menjalankan kueri hapus.
- **QueryExecutingUpdate:** Waktu yang dihabiskan untuk menjalankan kueri pembaruan.
- **QueryExecutingCtas:** Waktu yang dihabiskan untuk menjalankan CREATE TABLE AS query.
- **QueryExecutingUnload:** Waktu yang dihabiskan untuk menjalankan kueri bongkar muat.
- **QueryExecutingCopy:** Waktu yang dihabiskan untuk menjalankan kueri salinan.

Misalnya, grafik berikut di konsol Amazon Redshift menunjukkan jumlah waktu yang dihabiskan kueri dalam tahapan paket, tunggu, baca, dan tulis. Anda dapat menggabungkan temuan dari grafik ini dengan metrik lain untuk analisis lebih lanjut. Dalam beberapa kasus, grafik Anda mungkin menunjukkan bahwa kueri dengan durasi pendek (yang diukur dengan `QueryDuration` metrik) menghabiskan waktu lama dalam tahap menunggu. Dalam kasus ini, Anda dapat meningkatkan tingkat konkurensi WLM untuk antrian tertentu untuk meningkatkan throughput.

Berikut ini, adalah contoh bagan pemecahan eksekusi beban kerja. Dalam bagan, nilai sumbu y adalah durasi rata-rata setiap tahap pada waktu yang ditentukan yang ditampilkan sebagai grafik batang bertumpuk.

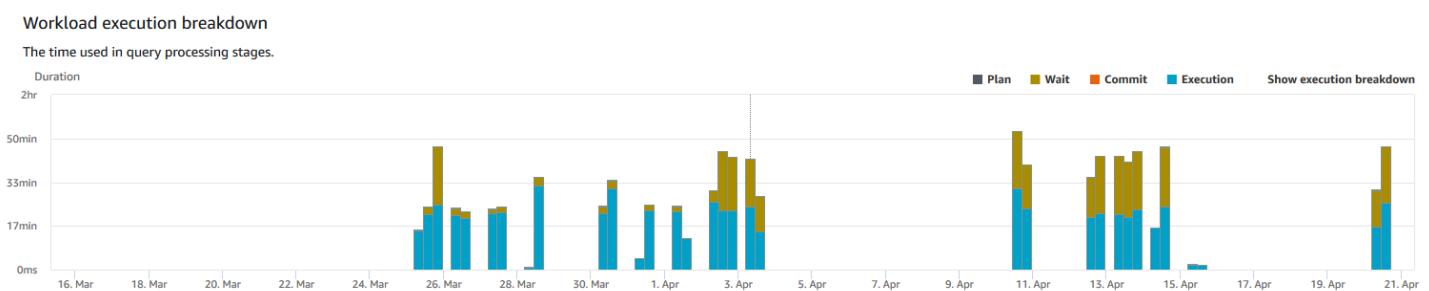
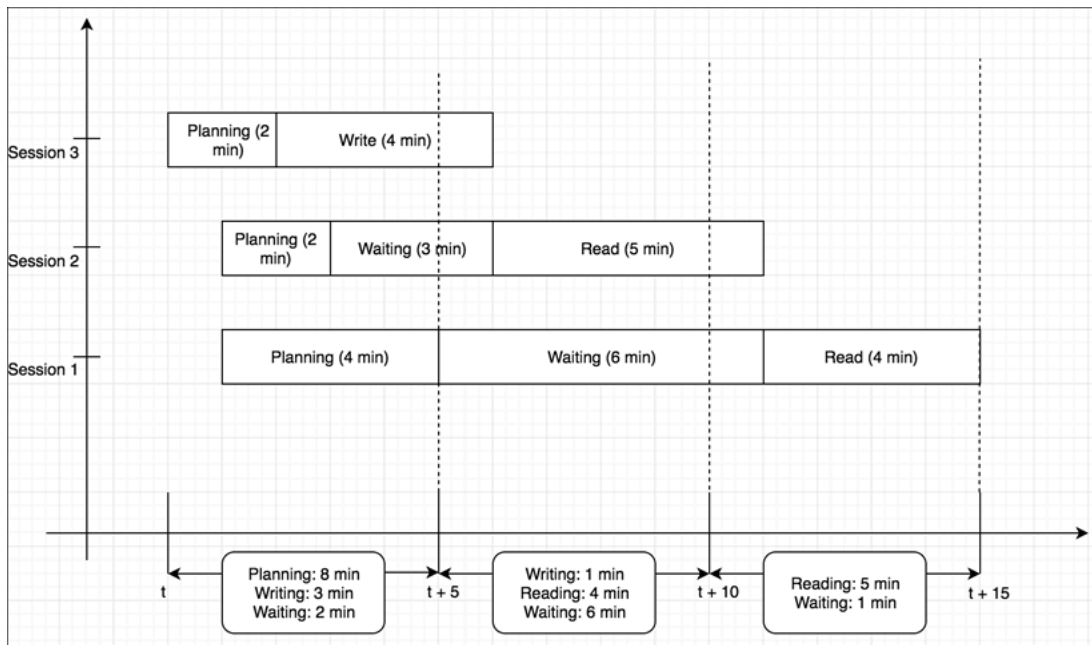


Diagram berikut mengilustrasikan bagaimana Amazon Redshift menggabungkan pemrosesan kueri untuk sesi bersamaan.



Untuk menampilkan bagan rincian beban kerja cluster

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Cluster, lalu pilih nama cluster dari daftar untuk membuka detailnya. Rincian cluster ditampilkan, yang dapat mencakup kinerja Cluster, pemantauan Kueri, Database, Datashares, Jadwal, Pemeliharaan, dan tab Properti.
3. Pilih tab Pemantauan kueri untuk metrik tentang kueri Anda.
4. Di bagian Pemantauan kueri, pilih Kinerja database, dan pilih Metrik klaster.

Metrik berikut dibuat grafik untuk rentang waktu yang dipilih sebagai bagan batang bertumpuk:

- Rencanakan waktu
- Tunggu waktu
- Komit waktu
- Waktu eksekusi

Mengelola alarm-alarm

Alarm yang Anda buat di konsol CloudWatch Amazon Redshift adalah alarm. Mereka berguna karena membantu Anda membuat keputusan proaktif tentang cluster atau instance tanpa server Anda. Anda dapat menyetel satu atau beberapa alarm pada salah satu metrik yang tercantum dalam [Memantau Amazon Redshift menggunakan metrik CloudWatch](#). Misalnya, menyetel alarm untuk `high CPUUtilization` pada node cluster membantu menunjukkan kapan node terlalu banyak digunakan. Alarm untuk `high DataStorage` akan melacak ruang penyimpanan yang digunakan namespace tanpa server Anda untuk data Anda.

Dari Tindakan, Anda dapat memodifikasi atau menghapus alarm. Anda juga dapat membuat peringatan lonceng atau kendur untuk mengirim peringatan dari CloudWatch Slack atau Amazon Chime dengan menentukan URL webhook Slack atau Amazon Chime.

Di bagian ini, Anda dapat menemukan cara membuat alarm menggunakan konsol Amazon Redshift. Anda dapat membuat alarm menggunakan CloudWatch konsol atau cara lain Anda bekerja dengan metrik, seperti dengan AWS CLI atau AWS SDK.

Untuk membuat CloudWatch alarm dengan konsol Amazon Redshift

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

Jika Anda menggunakan Amazon Redshift Serverless, Pilih Buka Tanpa Server di kanan atas dasbor.

2. Pada menu navigasi, pilih Alarm, lalu pilih Buat alarm.
3. Pada halaman Buat alarm, masukkan properti untuk membuat CloudWatch alarm.
4. Pilih Buat alarm.

Bekerja dengan metrik kinerja di konsol CloudWatch

Saat bekerja dengan metrik Amazon Redshift di CloudWatch konsol, ingatlah beberapa hal:

- Data kinerja kueri dan muat hanya tersedia di konsol Amazon Redshift.
- Beberapa Metrik di CloudWatch memiliki unit yang berbeda dari yang digunakan di konsol Amazon Redshift. Misalnya, `WriteThroughput` ditampilkan dalam GB/s (dibandingkan dengan bytes/s in CloudWatch), yang merupakan unit yang lebih relevan untuk ruang penyimpanan tipikal node.

Saat bekerja dengan metrik Amazon Redshift di CloudWatch konsol, alat baris perintah, atau Amazon SDK, ingatlah konsep ini:

1. Pertama, tentukan dimensi metrik yang akan digunakan. Dimensi adalah pasangan nama-nilai yang membantu Anda mengidentifikasi metrik secara unik. Dimensi untuk Amazon Redshift adalah `ClusterIdentifier` dan `NodeID`. Di CloudWatch konsol, Redshift Node tampilan Redshift Cluster dan disediakan untuk dengan mudah memilih dimensi cluster dan node-spesifik. Untuk informasi selengkapnya tentang dimensi, lihat [Dimensi](#) dalam Panduan CloudWatch Pengembang.
2. Kemudian, tentukan nama metrik, seperti `ReadIOPS`.

Tabel berikut merangkum jenis dimensi metrik Amazon Redshift yang tersedia untuk Anda. Bergantung pada metrik, data tersedia dalam interval 1 menit atau 5 menit tanpa biaya. Untuk informasi selengkapnya, lihat [Metrik Pergeseran Merah Amazon](#).

CloudWatch namespace	Dimensi	Deskripsi
AWS/Redshift	NodeID	Filter meminta data yang spesifik untuk node cluster. NodeID adalah “Leader”, “Shared”, atau “Compute-N” di mana N adalah 0, 1,... untuk jumlah node dalam cluster. “Shared” berarti bahwa cluster hanya memiliki satu node, yaitu node pemimpin dan node komputasi digabungkan.
	ClusterIdentifier	Filter meminta data yang khusus untuk cluster. Metrik yang khusus untuk cluster meliputi <code>HealthStatus</code> , <code>MaintenanceMode</code> , dan <code>DatabaseConnections</code> . Metrik umum untuk dimensi ini (misalnya <code>ReadIOPS</code>) yang juga merupakan metrik node mewakili agregat data metrik node. Berhati-hatilah dalam menafsirkan metrik ini karena mereka menggabungkan perilaku pemimpin dan node komputasi.

Bekerja dengan metrik gateway dan volume mirip dengan bekerja dengan metrik layanan lainnya. Banyak tugas umum diuraikan dalam CloudWatch dokumentasi, termasuk yang berikut:

- [Lihat metrik yang tersedia](#)
- [Dapatkan statistik untuk metrik](#)
- [Membuat CloudWatch alarm](#)

Acara Amazon Redshift

Topik

- [Ikhtisar acara cluster](#)
- [Bekerja dengan Amazon Simple Notification Service](#)
- [Berlangganan notifikasi acara klaster Amazon Redshift](#)
- [Melihat peristiwa cluster menggunakan konsol](#)
- [Melihat peristiwa klaster menggunakan API Amazon Redshift AWS CLI dan Amazon](#)
- [Mengelola notifikasi acara klaster](#)
- [Pemberitahuan acara Amazon Redshift](#)
- [Pemberitahuan acara Amazon Redshift Tanpa Server dengan Amazon EventBridge](#)
- [Pemberitahuan acara integrasi nol-ETL dengan Amazon EventBridge](#)

Ikhtisar acara cluster

Amazon Redshift melacak peristiwa cluster dan menyimpan informasi tentangnya selama beberapa minggu di akun Anda. AWS Untuk setiap peristiwa, Amazon Redshift melaporkan informasi seperti tanggal peristiwa terjadi, deskripsi, sumber peristiwa (misalnya, cluster, grup parameter, atau snapshot), dan ID sumber.

Amazon Redshift memberikan pemberitahuan sebelumnya untuk beberapa acara. Peristiwa ini memiliki kategori `acrapending`. Misalnya, kami mengirim pemberitahuan terlebih dahulu jika pembaruan perangkat keras diperlukan untuk salah satu node di cluster Anda. Anda dapat berlangganan acara yang tertunda sama seperti acara Amazon Redshift lainnya. Untuk informasi selengkapnya, lihat [Berlangganan notifikasi acara klaster Amazon Redshift](#).

Anda dapat menggunakan Amazon Redshift Management Console, Amazon Redshift API, atau SDK untuk mendapatkan AWS informasi peristiwa. Anda dapat memperoleh daftar semua acara, atau Anda dapat menerapkan filter, seperti durasi acara atau tanggal mulai dan berakhir, untuk mendapatkan informasi acara untuk periode tertentu.

Anda juga dapat memperoleh peristiwa yang dihasilkan oleh jenis sumber tertentu, seperti peristiwa cluster atau peristiwa grup parameter. Kolom Sumber menunjukkan nama sumber daya dan jenis sumber daya yang memicu tindakan yang diberikan.

Anda dapat membuat langganan notifikasi acara Amazon Redshift yang menentukan satu set filter peristiwa. Saat terjadi peristiwa yang sesuai dengan kriteria filter, Amazon Redshift menggunakan Layanan Pemberitahuan Sederhana Amazon untuk secara aktif memberi tahu Anda bahwa peristiwa tersebut telah terjadi.

Untuk daftar peristiwa Amazon Redshift menurut jenis dan kategori sumber, lihat [the section called “Kategori acara Amazon Redshift dan pesan acara”](#)

Bekerja dengan Amazon Simple Notification Service

Amazon Redshift menggunakan Amazon Simple Notification Service (Amazon SNS) untuk mengkomunikasikan notifikasi peristiwa Amazon Redshift. Anda mengaktifkan notifikasi dengan membuat langganan acara Amazon Redshift. Di langganan Amazon Redshift, Anda menentukan satu set filter untuk acara Amazon Redshift dan topik Amazon SNS. Setiap kali terjadi peristiwa yang cocok dengan kriteria filter, Amazon Redshift menerbitkan pesan notifikasi ke topik Amazon SNS. Amazon SNS kemudian mengirimkan pesan ke konsumen Amazon SNS yang memiliki langganan Amazon SNS untuk topik tersebut. Pesan yang dikirim ke konsumen Amazon SNS dapat dalam bentuk apa pun yang didukung oleh Amazon SNS untuk AWS suatu Wilayah, seperti email, pesan teks, atau panggilan ke titik akhir HTTP. Misalnya, semua Wilayah mendukung pemberitahuan email, tetapi pemberitahuan SMS hanya dapat dibuat di Wilayah AS Timur (Virginia N.).

Note

Saat ini, Anda hanya dapat membuat langganan acara ke topik standar Amazon SNS (bukan ke topik FIFO Amazon SNS). Untuk informasi selengkapnya, lihat [Sumber peristiwa Amazon SNS di Panduan](#) Pengembang Layanan Pemberitahuan Sederhana Amazon.

Saat Anda membuat langganan pemberitahuan acara, Anda menentukan satu atau beberapa filter acara. Amazon Redshift mengirimkan pemberitahuan melalui langganan setiap kali terjadi peristiwa yang cocok dengan semua kriteria filter. Kriteria filter mencakup jenis sumber (seperti cluster atau snapshot), ID sumber (seperti nama cluster atau snapshot), kategori peristiwa (seperti Monitoring atau Security), dan tingkat keparahan peristiwa (seperti INFO atau ERROR).

Anda dapat dengan mudah mematikan notifikasi tanpa menghapus langganan dengan menyetel tombol radio yang diaktifkan ke No dalam AWS Management Console atau dengan mengatur `Enabled` parameter untuk `false` menggunakan Amazon Redshift CLI atau API.

Penagihan untuk notifikasi acara Amazon Redshift dilakukan melalui Amazon Simple Notification Service (Amazon SNS). Biaya Amazon SNS berlaku saat menggunakan pemberitahuan acara; untuk informasi lebih lanjut tentang penagihan Amazon SNS, buka harga Amazon Simple Notification [Service](#).

Anda juga dapat melihat peristiwa Amazon Redshift yang telah terjadi dengan menggunakan konsol manajemen. Untuk informasi selengkapnya, lihat [Acara Amazon Redshift](#).

Berlangganan notifikasi acara klaster Amazon Redshift

Anda dapat membuat langganan notifikasi peristiwa Amazon Redshift sehingga Anda dapat diberi tahu saat peristiwa terjadi untuk klaster, snapshot, grup keamanan, atau grup parameter tertentu. Cara termudah untuk membuat langganan adalah dengan konsol Amazon SNS. Untuk informasi tentang membuat topik Amazon SNS dan berlangganan itu, lihat [Mulai dengan Amazon SNS](#).

Anda dapat membuat langganan notifikasi peristiwa Amazon Redshift sehingga Anda dapat diberi tahu saat peristiwa terjadi untuk klaster, snapshot, grup keamanan, atau grup parameter tertentu. Cara termudah untuk membuat langganan adalah dengan AWS Management Console. Jika memilih untuk membuat langganan pemberitahuan peristiwa menggunakan CLI atau API, Anda harus membuat topik Amazon Simple Notification Service dan berlangganan topik tersebut dengan konsol Amazon SNS atau Amazon SNS API. Anda juga perlu mempertahankan Nama Sumber Daya Amazon (ARN) topik karena digunakan saat mengirimkan perintah CLI atau tindakan API. Untuk informasi tentang membuat topik Amazon SNS dan berlangganan itu, lihat [Mulai dengan Amazon SNS](#).

Langganan acara Amazon Redshift dapat menentukan kriteria acara ini:

- Jenis sumber, nilainya adalah cluster, snapshot, parameter-group, dan security-groups.
- ID sumber daya, seperti `my-cluster-1` atau `my-snapshot-20130823`. ID harus untuk sumber daya di AWS Wilayah yang sama dengan langganan acara.
- Kategori acara, nilainya adalah Konfigurasi, Manajemen, Pemantauan, Keamanan, dan Pending
- Tingkat keparahan peristiwa, nilainya INFO atau ERROR.

Kriteria peristiwa dapat ditentukan secara independen, kecuali bahwa Anda harus menentukan jenis sumber sebelum Anda dapat menentukan ID sumber di konsol. Misalnya, Anda dapat menentukan kategori acara tanpa harus menentukan jenis sumber, ID sumber, atau tingkat keparahan. Meskipun Anda dapat menentukan ID sumber untuk sumber daya yang bukan dari jenis yang ditentukan dalam

tipe sumber, tidak ada pemberitahuan yang akan dikirim untuk peristiwa dari sumber daya tersebut. Misalnya, jika Anda menentukan jenis sumber kluster dan ID grup keamanan, tidak ada peristiwa yang dimunculkan oleh grup keamanan tersebut yang akan cocok dengan kriteria filter tipe sumber, sehingga tidak ada pemberitahuan yang akan dikirim untuk peristiwa tersebut.

Amazon Redshift mengirimkan pemberitahuan untuk acara apa pun yang cocok dengan semua kriteria yang ditentukan dalam langganan. Beberapa contoh rangkaian acara yang dikembalikan:

- Langganan menentukan jenis sumber cluster, ID sumber my-cluster-1, kategori Monitoring, dan tingkat keparahan ERROR. Langganan akan mengirimkan pemberitahuan hanya untuk memantau peristiwa dengan tingkat keparahan ERROR dari my-cluster-1.
- Langganan menentukan jenis sumber cluster, kategori Konfigurasi, dan tingkat keparahan INFO. Langganan akan mengirimkan pemberitahuan untuk peristiwa konfigurasi dengan tingkat keparahan INFO dari kluster Amazon Redshift mana pun di AWS akun.
- Langganan menentukan kategori Konfigurasi, dan tingkat keparahan INFO. Langganan akan mengirimkan pemberitahuan untuk peristiwa konfigurasi dengan tingkat keparahan INFO dari sumber daya Amazon Redshift apa pun di AWS akun.
- Langganan menentukan tingkat keparahan ERROR. Langganan akan mengirim pemberitahuan untuk semua acara dengan tingkat keparahan ERROR dari sumber daya Amazon Redshift di AWS akun.

Jika Anda menghapus atau mengganti nama objek yang namanya direferensikan sebagai ID sumber dalam langganan yang ada, langganan akan tetap aktif, tetapi tidak akan memiliki acara untuk diteruskan dari objek tersebut. Jika nanti Anda membuat objek baru dengan nama yang sama seperti yang direferensikan di ID sumber langganan, langganan akan mulai mengirim pemberitahuan untuk acara dari objek baru.

Amazon Redshift menerbitkan pemberitahuan acara ke topik Amazon SNS, yang diidentifikasi oleh Nama Sumber Daya Amazon (ARN). Saat membuat langganan acara menggunakan konsol Amazon Redshift, Anda dapat menentukan topik Amazon SNS yang ada, atau meminta konsol membuat topik saat membuat langganan. Semua pemberitahuan acara Amazon Redshift yang dikirim ke topik Amazon SNS pada gilirannya dikirimkan ke semua konsumen Amazon SNS yang berlangganan topik itu. Gunakan konsol Amazon SNS untuk membuat perubahan pada topik Amazon SNS, seperti menambahkan atau menghapus langganan konsumen ke topik tersebut. Untuk informasi selengkapnya tentang membuat dan berlangganan topik Amazon SNS, buka [Memulai dengan Amazon Simple Notification Service](#).

Bagian berikut mencantumkan semua kategori dan acara yang dapat Anda beri tahu. Ini juga memberikan informasi tentang berlangganan dan bekerja dengan langganan acara Amazon Redshift.

Melihat peristiwa cluster menggunakan konsol

Untuk melihat peristiwa

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Acara.

Melihat peristiwa klaster menggunakan API Amazon Redshift AWS CLI dan Amazon

Anda dapat menggunakan operasi Amazon Redshift CLI berikut untuk melihat peristiwa.

- [describe-events](#)

Amazon Redshift menyediakan API berikut untuk melihat peristiwa.

- [DescribeEvents](#)

Mengelola notifikasi acara klaster

Anda dapat membuat langganan notifikasi acara Amazon Simple Notification Service (Amazon SNS) untuk mengirim notifikasi saat peristiwa terjadi untuk cluster Amazon Redshift, snapshot, grup keamanan, atau grup parameter tertentu. Pemberitahuan ini dikirim ke topik SNS, yang pada gilirannya mengirimkan pesan ke konsumen SNS yang berlangganan topik tersebut. Pesan SNS kepada konsumen dapat dalam bentuk pemberitahuan apa pun yang didukung oleh Amazon SNS untuk AWS suatu Wilayah, seperti email, pesan teks, atau panggilan ke titik akhir HTTP. Misalnya, semua wilayah mendukung pemberitahuan email, tetapi pemberitahuan SMS hanya dapat dibuat di Wilayah AS Timur (Virginia N.). Untuk informasi selengkapnya, lihat [Pemberitahuan acara Amazon Redshift](#).

Mengelola notifikasi peristiwa klaster menggunakan konsol Amazon Redshift

Membuat langganan pemberitahuan acara

Untuk membuat langganan acara

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Acara.
3. Pilih tab Berlangganan acara, lalu pilih Buat langganan acara.
4. Masukkan properti langganan acara Anda, seperti nama, jenis sumber, kategori, dan tingkat keparahan. Anda juga dapat mengaktifkan topik Amazon SNS untuk mendapatkan pemberitahuan tentang acara.
5. Pilih Buat langganan acara untuk membuat langganan Anda.

Mengelola notifikasi peristiwa klaster menggunakan AWS CLI API Amazon Redshift dan Amazon

Anda dapat menggunakan operasi Amazon Redshift CLI berikut untuk mengelola notifikasi peristiwa cluster.

- [create-event-subscription](#)
- [delete-event-subscription](#)
- [describe-event-categories](#)
- [describe-event-subscriptions](#)
- [describe-events](#)
- [modify-event-subscription](#)

Anda dapat menggunakan tindakan Amazon Redshift API berikut untuk mengelola pemberitahuan peristiwa.

- [CreateEventSubscription](#)
- [DeleteEventSubscription](#)

- [DescribeEventCategories](#)
- [DescribeEventSubscriptions](#)
- [DescribeEvents](#)
- [ModifyEventSubscription](#)

Untuk informasi selengkapnya tentang notifikasi acara Amazon Redshift, lihat [Pemberitahuan acara Amazon Redshift](#)

Pemberitahuan acara Amazon Redshift

Kategori acara Amazon Redshift dan pesan acara

Bagian ini menunjukkan ID peristiwa dan kategori untuk setiap jenis sumber Amazon Redshift.

Tabel berikut menunjukkan kategori acara dan daftar peristiwa ketika cluster adalah jenis sumber.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Konfigurasi	REDSFT-EV ENT-1000	INFO	Grup parameter [nama grup parameter] diperbarui pada [waktu]. Jika Anda hanya mengubah parameter dinamis, cluster terkait sedang dimodifikasi sekarang. Jika Anda mengubah parameter statis, semua pembaruan, termasuk parameter dinamis, akan diterapkan saat Anda me-reboot cluster terkait.
Konfigurasi	REDSHIFT- EVENT-1001	INFO	Cluster Amazon Redshift [nama cluster] Anda telah dimodifikasi untuk menggunakan grup parameter [nama grup parameter] pada [waktu].
Konfigurasi	ACARA PERGESERAN MERAH-1500	ERROR	VPC Amazon [nama VPC] tidak ada. Perubahan konfigurasi Anda untuk klaster [nama klaster] tidak diterapkan. Silakan

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
			kunjungi AWS Management Console untuk memperbaiki masalah.
Konfigurasi	REDSFT-EV ENT-1501	ERROR	Subnet pelanggan [nama subnet] yang Anda tentukan untuk Amazon VPC [nama VPC] tidak ada atau tidak valid. Perubahan konfigurasi Anda untuk klaster [nama klaster] tidak diterapkan. Silakan kunjungi AWS Management Console untuk memperbaiki masalah.
Konfigurasi	ACARA PERGESERAN MERAH-1502	ERROR	Subnet dalam grup subnet cluster [nama grup subnet] tidak memiliki alamat IP yang tersedia. Cluster [nama cluster] tidak dapat dibuat.
Konfigurasi	ACARA PERGESERAN MERAH-1503	ERROR	VPC Amazon [nama VPC] tidak memiliki gateway internet yang melekat padanya. Perubahan konfigurasi Anda untuk klaster [nama klaster] tidak diterapkan. Silakan kunjungi AWS Management Console untuk memperbaiki masalah.
Konfigurasi	REDSFT-EV ENT-1504	ERROR	HSM untuk klaster [nama cluster] tidak dapat dijangkau.
Konfigurasi	ACARA PERGESERAN MERAH-1505	ERROR	HSM untuk klaster [nama cluster] tidak dapat didaftarkan. Coba konfigurasi yang berbeda.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Konfigurasi	REDSFT-EV ENT-1506	ERROR	Amazon Redshift melampaui batas elastis network interface akun Anda. Hapus hingga [jumlah maksimum antarmuka jaringan elastis] antarmuka jaringan elastis atau minta peningkatan batas jumlah antarmuka jaringan per AWS Wilayah dengan EC2.
Konfigurasi	REDSFT-EV ENT-1509	ERROR	<p>Cluster Amazon Redshift [nama cluster] tidak dapat dibuat karena batas titik akhir VPC akun Anda telah tercapai. Hapus titik akhir VPC yang tidak digunakan atau minta peningkatan batas titik akhir VPC.</p> <p>Untuk informasi selengkapnya, lihat Titik akhir VPC di Panduan Pengguna Amazon VPC.</p>
Konfigurasi	ACARA PERGESERAN MERAH-1510	ERROR	<p>Kami telah mendeteksi bahwa upaya untuk memuat data sampel di klaster Amazon Redshift [nama cluster] Anda tidak berhasil. Untuk memuat data sampel, pertama-tama konfigurasi VPC Anda agar memiliki akses ke bucket Amazon S3, lalu buat cluster baru dan muat data sampel.</p> <p>Untuk informasi selengkapnya, lihat Mengaktifkan perutean VPC yang disempurnakan di Panduan Manajemen Pergeseran Merah Amazon.</p>
Konfigurasi	ACARA PERGESERAN MERAH-1511	ERROR	Cluster Amazon Redshift [nama klaster] tidak dapat dibuat karena Anda melebihi batas alamat IP Elastis akun Anda. Hapus alamat IP Elastis yang tidak digunakan atau minta peningkatan batas dengan Amazon EC2.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Manajemen	ACARA PERGESERAN MERAH-2000	INFO	Cluster Amazon Redshift Anda: [nama cluster] telah dibuat dan siap digunakan.
Manajemen	ACARA PERGESERAN MERAH-2001	INFO	Cluster Amazon Redshift [nama cluster] Anda telah dihapus pada [waktu]. Cuplikan terakhir [adalah/tidak] disimpan.
Manajemen	ACARA PERGESERAN MERAH-2002	INFO	Grup keamanan VPC untuk klaster [nama cluster] diperbarui pada [waktu di UTC].
Manajemen	ACARA PERGESERAN MERAH-2003	INFO	Pemeliharaan dimulai pada cluster [nama cluster] pada [waktu di UTC].
Manajemen	ACARA PERGESERAN MERAH-2004	INFO	Pemeliharaan pada cluster [nama cluster] selesai pada [waktu di UTC].
Manajemen	ACARA PERGESERAN MERAH-2006	INFO	Pengubahan ukuran cluster [nama cluster] dimulai pada [waktu di UTC]. Cluster dalam mode read-only.
Manajemen	ACARA PERGESERAN MERAH-2007	INFO	Permintaan pengubahan ukuran untuk klaster [nama cluster] telah diakui.
Manajemen	ACARA PERGESERAN MERAH-2008	INFO	Operasi pemulihan Anda untuk membuat snapshot [nama klaster] klaster Amazon Redshift baru [nama snapshot] dimulai pada [waktu]. Untuk memantau kemajuan pemulihan, silakan kunjungi AWS Management Console.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Manajemen	ACARA PERGESERAN MERAH-2013	INFO	Cluster Amazon Redshift Anda [nama cluster] diganti namanya pada [waktu].
Manajemen	ACARA PERGESERAN MERAH-2014	INFO	Permintaan pemulihan tabel untuk klaster Amazon Redshift [nama cluster] telah diterima.
Manajemen	ACARA PERGESERAN MERAH-2015	INFO	Pemulihan tabel dibatalkan untuk klaster Amazon Redshift [nama cluster] pada [waktu].
Manajemen	ACARA PERGESERAN MERAH-2016	INFO	Penggantian klaster Amazon Redshift Anda [nama cluster] dimulai pada [waktu].
Manajemen	ACARA PERGESERAN MERAH-2017	INFO	Pemeliharaan yang dimulai oleh pelanggan dimulai di klaster Amazon Redshift [nama klaster] Anda pada [waktu]. Cluster mungkin tidak tersedia selama pemeliharaan.
Manajemen	ACARA PERGESERAN MERAH-2018	INFO	Pemeliharaan yang dimulai oleh pelanggan diselesaikan di klaster Amazon Redshift [nama klaster] Anda pada [waktu].
Manajemen	ACARA PERGESERAN MERAH-2019	ERROR	Pemeliharaan yang dimulai oleh pelanggan gagal di klaster Amazon Redshift [nama klaster] Anda pada [waktu]. Mengembalikan cluster kembali ke keadaan semula.
Manajemen	ACARA PERGESERAN MERAH-2020	INFO	Lagu [nama klaster] klaster Amazon Redshift Anda telah dimodifikasi dari [dari trek] menjadi [untuk melacak].

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Manajemen	ACARA PERGESERAN MERAH-2021	ERROR	[Operasi] klaster Amazon Redshift [nama cluster] tidak berhasil saat memperoleh kapasitas dari kumpulan kapasitas kami. Kami bekerja untuk memperoleh kapasitas tetapi untuk saat ini, kami telah membatalkan permintaan Anda. Hapus cluster ini dan coba lagi nanti.
Manajemen	ACARA PERGESERAN MERAH-2022	ERROR	[Operasi] klaster Amazon Redshift [nama cluster] tidak berhasil saat memperoleh kapasitas dari kumpulan kapasitas kami. Kami bekerja untuk memperoleh kapasitas tetapi untuk saat ini, kami telah membatalkan permintaan Anda. Kapasitas tersedia di [Availability Zone alternatif]. Hapus klaster ini dan coba lagi di Availability Zone alternatif.
Manajemen	ACARA PERGESERAN MERAH-2023	ERROR	Kami telah mendeteksi kegagalan perangkat keras pada cluster Amazon Redshift tunggal Anda [nama klaster], yang mungkin mengakibatkan kueri gagal atau ketersediaan klaster yang terputus-putus. Mengganti cluster tidak berhasil saat memperoleh kapasitas dari kumpulan kapasitas kami. Anda perlu memulihkan cluster baru dari snapshot. Hapus klaster ini, pilih snapshot terbaru yang tersedia, dan pulihkan cluster baru dari snapshot itu. Ini akan secara otomatis memberi Anda perangkat keras yang sehat.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Manajemen	ACARA PERGESERAN MERAH-2024	ERROR	Kami telah mendeteksi kegagalan perangkat keras pada cluster Amazon Redshift tunggal Anda [nama klaster], yang mungkin mengakibatkan kueri gagal atau ketersediaan klaster yang terputus-putus. Mengganti cluster tidak berhasil saat memperoleh kapasitas dari kumpulan kapasitas kami. Kapasitas tersedia di Availability Zone: [alternatif Availability Zones]. Hapus klaster ini, pilih snapshot terbaru yang tersedia, dan pulihkan cluster baru dari snapshot itu. Ini akan secara otomatis memberi Anda perangkat keras yang sehat.
Manajemen	ACARA PERGESERAN MERAH-3011	INFO	Pengubahan ukuran elastis untuk cluster Amazon Redshift '[nama cluster]' dimulai pada [waktu]. Kami akan menahan koneksi database selama mengubah ukuran. Beberapa kueri dan koneksi dapat dihentikan atau habis waktu selama operasi ini.
Manajemen	ACARA PERGESERAN MERAH-3012	INFO	Kami telah menerima permintaan perubahan ukuran elastis untuk cluster '[nama cluster]' yang dimulai pada [waktu]. Kami akan memberikan pemberitahuan acara saat mengubah ukuran dimulai.
Tertunda	ACARA PERGESERAN MERAH-2025	INFO	Database Anda untuk cluster <cluster name> akan diperbarui antara <start time> dan <end time>. Cluster Anda tidak akan dapat diakses. Rencanakan sesuai.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Tertunda	ACARA PERGESERAN MERAH-2026	INFO	Cluster Anda <cluster name> akan diperbarui antara <start time> dan <end time>. Cluster Anda tidak akan dapat diakses. Rencanakan sesuai.
Memantau	ACARA PERGESERAN MERAH-2050	INFO	Masalah perangkat keras terdeteksi di kluster Amazon Redshift [nama cluster]. Permintaan penggantian dimulai pada [waktu].
Memantau	REDSFT-EV ENT-3000	INFO	Cluster Amazon Redshift [nama cluster] Anda di-boot ulang pada [waktu].
Memantau	ACARA PERGESERAN MERAH-3001	INFO	Node di kluster Amazon Redshift Anda: [nama cluster] secara otomatis diganti pada [waktu], dan kluster Anda beroperasi secara normal.
Memantau	REDSFT-EV ENT-3002	INFO	Pengubahan ukuran untuk kluster Amazon Redshift [nama kluster] Anda sudah lengkap dan kluster Anda tersedia untuk dibaca dan ditulis. Pengubahan ukuran dimulai pada [waktu] dan membutuhkan [jam] jam untuk menyelesaikannya.
Memantau	REDSFT-EV ENT-3003	INFO	Cluster Amazon Redshift [nama cluster] berhasil dibuat dari snapshot [nama snapshot] dan tersedia untuk digunakan.
Memantau	REDSFT-EV ENT-3007	INFO	Snapshot Amazon Redshift Anda [nama snapshot] berhasil disalin dari [AWS Wilayah sumber] ke [AWS Wilayah tujuan] pada [waktu].
Memantau	REDSFT-EV ENT-3008	INFO	Pemulihan tabel dimulai untuk kluster Amazon Redshift [nama cluster] pada [waktu].

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Memantau	REDSFT-EV ENT-3009	INFO	Pemulihan tabel berhasil diselesaikan untuk kluster Amazon Redshift [nama cluster] pada [waktu].
Memantau	REDSFT-EV ENT-3010	ERROR	Pemulihan tabel gagal untuk kluster Amazon Redshift [nama kluster] pada [waktu].
Memantau	ACARA PERGESERAN MERAH-3013	ERROR	Operasi pengubahan ukuran elastis yang diminta untuk kluster Amazon Redshift [nama cluster] gagal pada [waktu] karena [alasan].
Memantau	ACARA PERGESERAN MERAH-3014	INFO	Amazon Redshift me-reboot cluster [nama cluster] pada [waktu].
Memantau	REDSFT-EV ENT-3500	ERROR	Pengubahan ukuran untuk kluster Amazon Redshift [nama cluster] gagal. Pengubahan ukuran akan dicoba ulang secara otomatis dalam beberapa menit.
Memantau	REDSFT-EV ENT-3501	ERROR	Operasi pemulihan Anda untuk membuat kluster Amazon Redshift [nama kluster] dari snapshot [nama snapshot] gagal pada [waktu]. Silakan coba lagi operasi Anda.
Memantau	REDSFT-EV ENT-3504	ERROR	Bucket Amazon S3 [nama bucket] tidak valid untuk pencatatan kluster [nama cluster].
Memantau	REDSFT-EV ENT-3505	ERROR	Bucket Amazon S3 [nama bucket] tidak memiliki kebijakan IAM yang benar untuk kluster [nama cluster].
Memantau	REDSFT-EV ENT-3506	ERROR	Bucket Amazon S3 [nama ember] tidak ada. Pencatatan tidak dapat dilanjutkan untuk kluster [nama kluster].

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Memantau	REDSFT-EV ENT-3507	ERROR	Cluster Amazon Redshift [nama cluster] tidak dapat dibuat menggunakan EIP [alamat IP]. EIP ini sudah digunakan.
Memantau	REDSFT-EV ENT-3508	ERROR	Cluster Amazon Redshift [nama cluster] tidak dapat dibuat menggunakan EIP [alamat IP]. EIP tidak dapat ditemukan.
Memantau	REDSFT-EV ENT-3509	ERROR	Salinan snapshot lintas wilayah tidak diaktifkan untuk klaster [nama cluster].
Memantau	ACARA PERGESERAN MERAH-3510	ERROR	Pemulihan tabel gagal dimulai untuk klaster Amazon Redshift [nama cluster] pada [waktu]. Alasan: [alasan].
Memantau	ACARA PERGESERAN MERAH-3511	ERROR	Pemulihan tabel gagal untuk klaster Amazon Redshift [nama klaster] pada [waktu].
Memantau	ACARA PERGESERAN MERAH-3512	ERROR	Cluster Amazon Redshift [nama cluster] gagal karena masalah perangkat keras. Cluster sedang dipulihkan secara otomatis dari snapshot terbaru [nama snapshot] yang dibuat pada [waktu].
Memantau	ACARA PERGESERAN MERAH-3513	ERROR	Cluster Amazon Redshift [nama cluster] gagal karena masalah perangkat keras. Cluster sedang dipulihkan secara otomatis dari snapshot terbaru [nama snapshot] yang dibuat pada [waktu]. Setiap perubahan database yang dilakukan setelah waktu ini perlu dikirimkan kembali.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Memantau	ACARA PERGESERAN MERAH-3514	ERROR	Cluster Amazon Redshift [nama cluster] gagal karena masalah perangkat keras. Cluster ditempatkan dalam status kegagalan perangkat keras. Harap hapus cluster dan pulihkan dari snapshot terbaru [nama snapshot] yang dibuat pada [waktu].
Memantau	REDSFT-EV ENT-3515	ERROR	Cluster Amazon Redshift [nama cluster] gagal karena masalah perangkat keras. Cluster ditempatkan dalam status kegagalan perangkat keras. Harap hapus cluster dan pulihkan dari snapshot terbaru [nama snapshot] yang dibuat pada [waktu]. Setiap perubahan database yang dilakukan setelah waktu ini perlu dikirimkan kembali.
Memantau	ACARA PERGESERAN MERAH-3516	ERROR	Cluster Amazon Redshift [nama cluster] telah gagal karena masalah perangkat keras dan tidak ada cadangan untuk cluster. Cluster ditempatkan dalam status kegagalan perangkat keras dan dapat dihapus.
Memantau	REDSHIFT-ACT-3519	INFO	Cluster [nama cluster] mulai dimulai ulang pada [waktu].
Memantau	REDSFT-EV ENT-3520	INFO	Cluster [nama cluster] selesai restart pada [waktu].
Memantau	ACARA PERGESERAN MERAH-3521	INFO	Kami mendeteksi masalah konektivitas pada cluster '[nama cluster]'. Pemeriksaan diagnostik otomatis telah dimulai pada [waktu].

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Memantau	ACARA PERGESERAN MERAH-3522	INFO	Tindakan pemulihan pada klaster '[nama cluster]' gagal pada [waktu]. Tim Amazon Redshift sedang mengerjakan solusi.
Memantau	ACARA PERGESERAN MERAH-3533	ERROR	Pengubahan ukuran cluster pada '[nama cluster]' dibatalkan pada [waktu]. Operasi dibatalkan karena [alasan]. [tindakan yang diperlukan].
Memantau	ACARA PERGESERAN MERAH-3534	INFO	Pengubahan ukuran elastis untuk cluster Amazon Redshift '[nama cluster]' selesai pada [waktu]. Cluster sekarang tersedia untuk operasi baca dan tulis saat kami mentransfer data. Beberapa pertanyaan mungkin membutuhkan waktu lebih lama untuk diselesaikan hingga transfer data selesai.
Memantau	ACARA PERGESERAN MERAH-3537	INFO	Transfer data cluster '[nama cluster]' selesai pada [waktu di UTC].
Memantau	ACARA PERGESERAN MERAH-3600	INFO	Operasi pengubahan ukuran yang diminta untuk cluster Amazon Redshift '[nama cluster]' dibatalkan di masa lalu. Rollback selesai pada [waktu].
Tertunda	ACARA PERGESERAN MERAH-3601	INFO	Sebuah node pada cluster Anda <cluster name> akan diganti antara <start time> dan <end time>. Anda tidak dapat menunda pemeliharaan ini. Rencanakan sesuai.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Tertunda	REDSFT-EV ENT-3602	INFO	Sebuah node pada cluster Anda <cluster name>dijadwalkan untuk diganti antara <start time>dan<end time>. Cluster Anda tidak akan dapat diakses. Rencanakan sesuai.
Manajemen	ACARA PERGESERAN MERAH-3603	INFO	Operasi pemulihan untuk membuat klaster [nama cluster] dari snapshot [nama snapshot] gagal karena kesalahan internal. Cluster ditempatkan dalam status pemulihan yang tidak kompatibel dan dapat dihapus. Cobalah untuk mengembalikan snapshot ke dalam cluster dengan konfigurasi yang berbeda.
Manajemen	ACARA PERGESERAN MERAH-3614	INFO	Tindakan terjadwal [nama tindakan terjadwal] dibuat pada [waktu di UTC]. Doa pertama dijadwalkan pada [waktu di UTC].
Manajemen	REDSFT-EV ENT-3615	INFO	Tindakan terjadwal [nama tindakan terjadwal] dijadwalkan pada [waktu di UTC].
Memantau	ACARA PERGESERAN MERAH-3616	INFO	Tindakan terjadwal [nama tindakan terjadwal] pada [waktu di UTC] selesai dengan status 'SUCCEDED'.
Memantau	ACARA PERGESERAN MERAH-3617	ERROR	Tindakan terjadwal [nama tindakan terjadwal] dilewati pada [waktu di UTC] karena penundaan.
Memantau	ACARA PERGESERAN MERAH-3618	INFO	Operasi jeda cluster [nama cluster] dimulai pada [waktu UTC]. Jeda Dimulai
Memantau	REDSFT-EV ENT-3619	INFO	Cluster Amazon Redshift [nama cluster] berhasil dijeda pada [waktu UTC].

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Manajemen	REDSFT-EV ENT-3626	INFO	Tindakan terjadwal [nama tindakan terjadwal] dimodifikasi pada [waktu di UTC]. Doa pertama dijadwalkan pada [waktu di UTC].
Manajemen	REDSFT-EV ENT-3627	INFO	Tindakan terjadwal [nama tindakan terjadwal] telah dihapus pada [waktu di UTC].
Memantau	REDSFT-EV ENT-3628	ERROR	Tindakan terjadwal [nama tindakan terjadwal] pada [waktu di UTC] selesai dengan status 'GAGAL'.
Manajemen	ACARA PERGESERAN MERAH-3629	INFO	Amazon Redshift [nama cluster] telah menerima permintaan relokasi Anda. Saat relokasi Availability Zone selesai, Amazon Redshift mengirimkan pemberitahuan acara.
Manajemen	REDSFT-EV ENT-3630	INFO	Cluster Amazon Redshift [nama cluster] berhasil dipindahkan dari [zona ketersediaan] ke [zona ketersediaan]. Anda dapat menggunakan cluster sekarang.
Manajemen	ACARA PERGESERAN MERAH-3631	INFO	Amazon Redshift berhasil memindahkan kluster Amazon Redshift [nama kluster] Anda dari [zona ketersediaan] ke [zona ketersediaan] untuk pemulihan.
Manajemen	REDSFT-EV ENT-3632	INFO	Amazon Redshift telah menonaktifkan sementara relokasi kluster untuk kluster Amazon Redshift [nama cluster] karena perubahan konfigurasi. Coba relokasi cluster lagi nanti.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Memantau	ACARA PERGESERAN MERAH-3658	ERROR	Migrasi EC2-klasik ke EC2-VPC gagal untuk cluster Redshift [id cluster].
Memantau	ACARA PERGESERAN MERAH-3659	INFO	Migrasi EC2-klasik ke EC2-VPC berhasil untuk cluster Redshift [id cluster].
Memantau	ACARA PERGESERAN MERAH-3660	INFO	Cluster ditempatkan dalam status kegagalan perangkat keras. Harap hapus kluster EC2-Classic dan pulihkan ke cluster EC2-VPC dari snapshot terbaru [nama snapshot] yang dibuat pada [waktu di UTC].
Manajemen	ACARA PERGESERAN MERAH-3666	INFO	Amazon Redshift Multi-AZ cluster [nama cluster] telah mendeteksi kegagalan pada [waktu di UTC] dan memicu pemulihan otomatis.
Manajemen	ACARA PERGESERAN MERAH-3667	INFO	Amazon Redshift Multi-AZ cluster [nama cluster] berhasil dipulihkan pada [waktu di UTC] dan tersedia untuk digunakan di [zona ketersediaan pertama]. Komputasi sekunder di AZ lain akan segera tersedia.
Memantau	ACARA PERGESERAN MERAH-3668	ERROR	Cluster Amazon Redshift Multi-AZ [nama cluster] gagal pulih pada [waktu di UTC].
Manajemen	REDSFT-EV ENT-3669	INFO	Amazon Redshift Multi-AZ cluster [nama cluster] berhasil dipulihkan pada [waktu di UTC] dan tersedia untuk digunakan dengan sumber daya komputasi dari [zona ketersediaan pertama] dan [zona ketersediaan kedua].

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Manajemen	ACARA PERGESERAN MERAH-3670	INFO	Pemeliharaan di klaster Amazon Redshift [nama klaster] selesai pada [waktu di UTC] dan tersedia untuk digunakan dengan sumber daya komputasi di [zona ketersediaan pertama]. Komputasi sekunder di AZ lain akan segera tersedia.
Manajemen	REDSFT-EV ENT-3671	INFO	Ubah ukuran pada klaster Amazon Redshift [nama cluster] selesai pada [waktu di UTC] dan tersedia untuk digunakan di [zona ketersediaan pertama]. Komputasi sekunder di AZ lain akan segera tersedia.
Manajemen	REDSFT-EV ENT-3672	INFO	Amazon Redshift Multi-AZ cluster [nama cluster] telah mendeteksi kegagalan di [zona ketersediaan kedua] pada [waktu di UTC] dan memicu pemulihan otomatis.
Manajemen	REDSFT-EV ENT-3673	INFO	Operasi untuk mengaktifkan Multi-AZ untuk klaster Amazon Redshift [nama cluster] telah dimulai pada [waktu di UTC].
Manajemen	ACARA PERGESERAN MERAH-3674	INFO	Operasi untuk mengaktifkan Multi-AZ untuk klaster Amazon Redshift [nama cluster] telah berhasil diselesaikan pada [waktu di UTC].
Memantau	ACARA PERGESERAN MERAH-3675	ERROR	Operasi untuk mengaktifkan Multi-AZ untuk klaster Amazon Redshift [nama cluster] telah gagal pada [waktu di UTC].
Manajemen	ACARA PERGESERAN MERAH-3676	INFO	Operasi untuk menonaktifkan Multi-AZ untuk klaster Amazon Redshift Multi-AZ [nama cluster] Anda telah dimulai pada [waktu di UTC].

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Manajemen	REDSFT-EV ENT-3677	INFO	Operasi untuk menonaktifkan Multi-AZ untuk kluster Amazon Redshift [nama cluster] Anda telah berhasil diselesaikan pada [waktu di UTC].
Memantau	ACARA PERGESERAN MERAH-3678	ERROR	Operasi untuk menonaktifkan Multi-AZ untuk kluster Amazon Redshift [nama cluster] Anda telah gagal pada [waktu di UTC].
Konfigurasi	ACARA PERGESERAN MERAH-3679	INFO	Port cluster Amazon Redshift [nama cluster] berhasil dimodifikasi.
Konfigurasi	REDSFT-EV ENT-3680	ERROR	Amazon Redshift tidak dapat membuat kluster [nama kluster] karena Service Linked Role (SLR) yang diperlukan untuk operasi ini tidak dapat diakses. Coba buat lagi dari konsol Amazon Redshift. Amazon Redshift akan membuat SLR secara otomatis.
Memantau	ACARA PERGESERAN MERAH-3684	ERROR	Bucket Amazon S3 [nama bucket] Anda telah dienkripsi dengan kunci yang tidak dikenal atau tidak dapat diakses. AWS KMS Ubah enkripsi bucket Amazon S3 Anda.
Manajemen	REDSFT-EV ENT-3685	ERROR	Operasi pemulihan pada cluster [nama cluster] gagal karena tidak memiliki cukup ruang disk yang tersedia. Operasi sedang diputar kembali. Coba pulihkan ke cluster dengan konfigurasi yang berbeda.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Manajemen	ACARA PERGESERAN MERAH-3686	ERROR	Operasi pengubahan ukuran pada klaster [nama cluster] gagal karena tidak memiliki cukup ruang disk yang tersedia. Operasi sedang diputar kembali. Coba ubah ukuran ke cluster dengan konfigurasi yang berbeda.
Keamanan	REDSFT-EV ENT-4000	INFO	Kredensi admin Anda untuk klaster Amazon Redshift Anda: [nama klaster] diperbarui pada [waktu].
Keamanan	REDSFT-EV ENT-4001	INFO	Grup keamanan [nama grup keamanan] dimodifikasi pada [waktu]. Perubahan akan terjadi untuk semua cluster terkait secara otomatis.
Keamanan	REDSFT-EV ENT-4500	ERROR	Grup keamanan [nama grup keamanan] yang Anda berikan tidak valid. Perubahan konfigurasi Anda untuk klaster [nama klaster] tidak diterapkan. Silakan kunjungi AWS Management Console untuk memperbaiki masalah.
Keamanan	REDSFT-EV ENT-4501	ERROR	Grup keamanan [nama grup keamanan] yang ditentukan dalam Grup Keamanan Cluster [nama grup keamanan klaster] tidak dapat ditemukan. Otorisasi tidak dapat diselesaikan.
Keamanan	REDSFT-EV ENT-4502	ERROR	Kredensi admin untuk klaster Amazon Redshift [nama klaster] gagal diperbarui pada [waktu] karena aktivitas bersamaan. Biarkan beban kerja saat ini menyelesaikan atau mengurangi beban kerja aktif dan kemudian coba lagi operasi.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Keamanan	PERUBAHAN-PERISTIWA-4503	ERROR	Amazon Redshift tidak dapat mengakses rahasia untuk kluster [nama cluster] Anda.
Keamanan	PERUBAHAN-PERISTIWA-4504	ERROR	Amazon Redshift tidak dapat mengakses kunci KMS [kunci KMS] yang digunakan untuk mengenkripsi rahasia kredensi admin untuk kluster [nama cluster] Anda.
Keamanan	PERUBAHAN-PERISTIWA-4505	ERROR	Amazon Redshift tidak dapat memutar rahasia untuk kluster [nama cluster] Anda karena ada operasi yang sedang berlangsung di cluster.
Keamanan	PERUBAHAN-PERISTIWA-4506	ERROR	Cluster Amazon Redshift [nama cluster] Anda dijeda. Amazon Redshift tidak dapat memutar rahasia cluster yang dijeda.

Tabel berikut menunjukkan kategori kejadian dan daftar kejadian saat grup parameter merupakan jenis sumber.

Kategori dan peristiwa untuk tipe sumber grup parameter

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Konfigurasi	REDSHIFT-EVENT-1002	INFO	Parameter [nama parameter] diperbarui dari [value] ke [value] pada [time].
Konfigurasi	REDSHIFT-EVENT-1003	INFO	Grup parameter cluster [nama grup] telah dibuat.
Konfigurasi	REDSHIFT-EVENT-1004	INFO	Grup parameter cluster [nama grup] telah dihapus.

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Konfigurasi	REDSHIFT-EVENT-1005	INFO	Grup parameter cluster [name] diperbarui pada [waktu]. Jika Anda hanya mengubah parameter dinamis, cluster terkait sedang dimodifikasi sekarang. Jika Anda mengubah parameter statis, semua pembaruan, termasuk parameter dinamis, akan diterapkan saat Anda me-reboot cluster terkait.

Tabel berikut menunjukkan kategori acara dan daftar peristiwa ketika grup keamanan adalah tipe sumber.

Kategori dan peristiwa untuk jenis sumber grup keamanan

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Keamanan	REDSFT-EV-ENT-4002	INFO	Grup keamanan klaster [nama grup] telah dibuat.
Keamanan	REDSFT-EV-ENT-4003	INFO	Grup keamanan klaster [nama grup] telah dihapus.
Keamanan	REDSFT-EV-ENT-4004	INFO	Grup keamanan cluster [nama grup] diubah pada [waktu]. Perubahan akan diterapkan secara otomatis ke semua cluster terkait.

Tabel berikut menunjukkan kategori acara dan daftar peristiwa ketika snapshot adalah jenis sumber.

Kategori dan acara untuk jenis sumber snapshot

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
Manajemen	ACARA PERGESERAN MERAH-2009	INFO	Snapshot pengguna [nama snapshot] untuk Amazon Redshift Cluster [nama cluster] dimulai pada [waktu]. Untuk memantau kemajuan snapshot, silakan kunjungi. AWS Management Console
Manajemen	REDSHIFT-EVENT-2010	INFO	Snapshot pengguna [nama snapshot] untuk klaster Amazon Redshift [nama klaster] dibatalkan pada [waktu].
Manajemen	ACARA PERGESERAN MERAH-2011	INFO	Snapshot pengguna [nama snapshot] untuk klaster Amazon Redshift [nama cluster] telah dihapus pada [waktu].
Manajemen	ACARA PERGESERAN MERAH-2012	INFO	Snapshot terakhir [nama snapshot] untuk cluster Amazon Redshift [nama cluster] dimulai pada [waktu].
Memantau	ACARA PERGESERAN MERAH-3004	INFO	Snapshot pengguna [nama snapshot] untuk klaster Amazon Redshift [nama klaster] berhasil diselesaikan pada [waktu].
Memantau	ACARA PERGESERAN MERAH-3005	INFO	Cuplikan terakhir [nama] untuk klaster Amazon Redshift [nama] berhasil diselesaikan pada [waktu].
Memantau	ACARA PERGESERAN MERAH-3006	INFO	Snapshot terakhir [nama snapshot] untuk cluster Amazon Redshift [nama cluster] dibatalkan pada [waktu].
Memantau	REDSFT-EV ENT-3502	ERROR	Snapshot terakhir [nama snapshot] untuk klaster Amazon Redshift [nama cluster] gagal pada [waktu]. Tim sedang menyelidiki

Kategori Amazon Redshift	ID peristiwa	Tingkat keparahan peristiwa	Deskripsi
			ki masalah ini. Silakan kunjungi AWS Management Console untuk mencoba kembali operasi.
Memantau	REDSFT-EV ENT-3503	ERROR	Snapshot pengguna [nama snapshot] untuk klaster Amazon Redshift [nama klaster] gagal pada [waktu]. Tim sedang menyelidiki masalah ini. Silakan kunjungi AWS Management Console untuk mencoba kembali operasi.

Pemberitahuan acara Amazon Redshift Tanpa Server dengan Amazon EventBridge

Amazon Redshift Serverless menggunakan EventBridge Amazon untuk mengelola pemberitahuan acara agar up-to-date Anda tetap memperhatikan perubahan di gudang data Anda. Amazon EventBridge adalah layanan bus acara tanpa server yang dapat Anda gunakan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. Dalam hal ini, sumber acara adalah Amazon Redshift. Peristiwa, yang memantau perubahan di lingkungan, dikirim ke EventBridge gudang data Amazon Redshift Anda secara otomatis. Acara disampaikan dalam waktu nyaris nyata.

Kemampuan EventBridge termasuk menyediakan lingkungan bagi Anda untuk menulis aturan acara, yang dapat menentukan tindakan yang harus diambil untuk acara tertentu. Anda juga dapat mengatur target, yang merupakan sumber daya yang EventBridge dapat mengirim acara ke. Target dapat mencakup tujuan API, grup CloudWatch log Amazon, dan lainnya. Untuk informasi selengkapnya tentang aturan, lihat [EventBridge Aturan Amazon](#). Untuk informasi selengkapnya tentang target, lihat [EventBridge target Amazon](#).

Acara dapat diklasifikasikan ke dalam tingkat keparahan dan kategori. Filter berikut tersedia:

- Pemfilteran sumber daya - Menerima pesan berdasarkan sumber daya yang terkait dengan peristiwa. Sumber daya termasuk workgroup, snapshot, dan sebagainya.
- Pemfilteran jendela waktu - Cakupan peristiwa dalam periode waktu tertentu.

- Pemfilteran kategori - Menerima pemberitahuan acara untuk semua acara dalam kategori tertentu.

Tabel berikut mencakup peristiwa Amazon Redshift Tanpa Server, dengan metadata tambahan:

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
RateChange	REDSHIFT-SERVERLESS-ACARA-1001	INFO	<time in UTC>Perubahan RPU basis kelompok kerja berhasil diselesaikan di.
RateChange	REDSHIFT-SERVERLESS-ACARA-1002	ERROR	<time in UTC>Perubahan RPU basis grup kerja gagal diselesaikan di.
Memantau	REDSHIFT-SERVERLESS-ACARA-1003	INFO	<endpoint name><time in UTC>Perangkat lunak ini diperbarui di Gudang Data Amazon Redshift Anda di.
Konfigurasi	REDSHIFT-SERVERLESS-ACARA-1011	ERROR	Amazon Redshift Serverless tidak dapat membuat grup kerja [nama grup kerja] karena Service Linked Role (SLR) yang diperlukan untuk operasi ini tidak dapat diakses. Coba buat lagi di konsol

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
			Amazon Redshift. Amazon Redshift akan membuat SLR secara otomatis.
Memantau	REDSHIFT-SERVERLESS-ACARA-1029	ERROR	Perubahan RPU basis grup kerja gagal diselesaikan pada [waktu di UTC] karena tidak memiliki cukup ruang disk yang tersedia. Coba lagi dengan konfigurasi yang berbeda.
Memantau	REDSHIFT-SERVERLESS-ACARA-1500	ERROR	Workgroup <workgroup name>tidak dapat dibuat atau diperbarui karena Anda melebihi batas alamat IP Elastis akun Anda. Hapus alamat IP Elastis yang tidak digunakan atau minta peningkatan batas dengan Amazon EC2.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Memantau	REDSHIFT-SERVERLESS-ACARA-1501	ERROR	Subnet <subnet id>tidak memiliki alamat IP yang tersedia. Ini akan mencegah jenis kueri berikut berjalan dengan sukses di workgroup<workgroup name>: EMR, kueri federasi, SALIN/BONGKAR dari Amazon EC2. Untuk memperbaiki masalah ini, kosongkan IP di subnet Anda dengan menghapus ENI.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Memantau	REDSHIFT-SERVERLESS-ACARA-1502	ERROR	Subnet <subnet id>tidak memiliki alamat IP yang tersedia. <workgroup name>Ini akan mencegah EMR Amazon, kueri federasi Redshift, Redshift COPY/ UNLOAD, jenis kueri Redshift ML agar tidak berhasil berjalan di workgroup . Untuk memperbaiki masalah ini, kosongkan IP di subnet Anda dengan menghapus antarmuka jaringan elastis (ENI) yang tidak digunakan.
Manajemen	REDSHIFT-SERVERLESS-ACARA-1008	INFO	Workgroup Amazon Redshift Anda <workgroup name>telah dibuat dan siap digunakan.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Manajemen	REDSHIFT-SERVERLESS-ACARA-1009	INFO	<time in UTC>Workgroup Amazon Redshift Anda <workgroup name>telah dihapus di.
Memantau	REDSHIFT-SERVERLESS-ACARA-1000	INFO	<time in UTC>Snapshot <snapshot name>berhasil diselesaikan di.
Manajemen	REDSHIFT-SERVERLESS-ACARA-1004	INFO	<time in UTC>Pulihkan dari snapshot di namespace <namespace name>berhasil diselesaikan di.
Manajemen	REDSHIFT-SERVERLESS-ACARA-1005	ERROR	<namespace name><time in UTC>Pulihkan dari snapshot di namespace gagal di.
Manajemen	REDSHIFT-SERVERLESS-ACARA-1006	INFO	<time in UTC>Pulihkan dari titik pemulihan pada namespace yang <namespace name>berhasil diselesaikan di.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Manajemen	REDSHIFT-SERVERLESS-ACARA-1007	INFO	<time in UTC>Pemulihan dari titik pemulihan pada namespace <namespace name>gagal di.
Keamanan	REDSHIFT-SERVERLESS-ACARA-1012	ERROR	<namespace name>Amazon Redshift tidak dapat mengakses rahasia untuk namespace Anda.
Keamanan	REDSHIFT-SERVERLESS-ACARA-1013	ERROR	<namespace name>Amazon Redshift tidak dapat mengakses kunci KMS yang digunakan untuk mengenkripsi rahasia kredensial admin untuk namespace Anda.
Keamanan	REDSHIFT-SERVERLESS-ACARA-1014	ERROR	Amazon Redshift tidak dapat memutar rahasia untuk namespace Anda <namespace name>karena ada operasi yang sedang berlangsung di workgroup.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Keamanan	REDSHIFT-SERVERLESS-ACARA-1015	ERROR	Namespace Anda <namespace name>tidak memiliki workgroup yang melekat padanya. Amazon Redshift hanya dapat memutar rahasia untuk ruang nama dengan grup kerja yang melekat padanya.
Keamanan	REDSHIFT-SERVERLESS-ACARA-1016	INFO	<namespace name><time in UTC>Kredensi admin diperbarui untuk namespace Anda di.

Pemberitahuan acara integrasi nol-ETL dengan Amazon EventBridge

Integrasi nol-ETL menggunakan Amazon EventBridge untuk mengelola pemberitahuan acara agar Anda tetap memperhatikan perubahan dalam integrasi up-to-date Anda. Amazon EventBridge adalah layanan bus acara tanpa server yang dapat Anda gunakan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. Dalam hal ini, sumber acara adalah Amazon Redshift. Peristiwa, yang memantau perubahan di lingkungan, dikirim ke EventBridge gudang data Amazon Redshift Anda secara otomatis. Acara disampaikan dalam waktu dekat.

EventBridge menyediakan lingkungan bagi Anda untuk menulis aturan acara, yang dapat menentukan tindakan yang akan diambil untuk acara tertentu. Anda juga dapat mengatur target, yang merupakan sumber daya yang EventBridge dapat mengirim acara ke. Target dapat mencakup tujuan

API, grup CloudWatch log Amazon, dan lainnya. Untuk informasi selengkapnya tentang aturan, lihat [EventBridge Aturan Amazon](#). Untuk informasi selengkapnya tentang target, lihat [EventBridge target Amazon](#).

Acara dapat diklasifikasikan ke dalam tingkat keparahan dan kategori. Filter berikut tersedia:

- Pemfilteran sumber daya — Menerima pesan berdasarkan sumber daya yang terkait dengan peristiwa tersebut. Sumber daya termasuk workgroup atau snapshot.
- Pemfilteran jendela waktu - Cakupan peristiwa dalam periode waktu tertentu.
- Pemfilteran kategori - Menerima pemberitahuan acara untuk semua acara dalam kategori tertentu.

Tabel berikut mencakup peristiwa integrasi nol-ETL, dengan metadata tambahan:

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0000	INFO	Integrasi nol-ETL <integration name>telah dibuat dan sekarang AKTIF.
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0001	INFO	<integration name><time in UTC>Integrasi nol-ETL telah dihapus di.
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0002	INFO	<integration name><time in UTC>Memulai penghapusan integrasi nol-ETL di.
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0003	INFO	Integrasi nol-ETL <integration name>adalah menyinkronkan data

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
			transaksional ke gudang data target.
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0004	WARNING	Satu atau beberapa tabel tidak memiliki kunci utama dan tidak dapat disinkronkan. Ambil cadangan di Amazon RDS, jatuhkan tabel ini, dan buat ulang mengikuti praktik terbaik Amazon Redshift untuk mendesain tabel.
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0005	WARNING	Satu atau beberapa tabel tidak dapat disinkronkan karena berisi tipe atau panjang data yang tidak didukung. Perbaiki tabel dan coba lagi. Untuk tipe data yang tidak didukung, lihat Tipe data yang tidak didukung .
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0006	ERROR	Tidak dapat membuat integrasi. Hapus dan buat ulang integrasi.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0007	ERROR	Tidak dapat memuat data karena kegagalan internal. Hapus dan buat ulang integrasi.
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0008	ERROR	Otorisasi gagal karena izin telah dicabut dari cluster DB cluster Aurora DB sumber. Hapus dan buat ulang integrasi.
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0009	ERROR	Tidak dapat mengirim data ke Amazon Redshift karena jumlah tabel dan skema melebihi batas Amazon Redshift. Hapus dan buat ulang integrasi.
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0012	ERROR	Pemulihan dari titik pemulihan dipanggil pada namespace tanpa server tujuan. Hapus dan buat ulang integrasi.
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0013	INFO	<integration name>Integrasi nol-ETL sekarang AKTIF.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Pemantauan	PERUBAHAN-INTEGRASI-PERISTIWA-0014	ERROR	Integrasi <integration name>gagal karena tidak dapat dimodifikasi karena kesalahan internal. Hapus dan buat ulang integrasi . Jika kesalahan berlanjut, hubungi AWS Support.
Operasi	PERUBAHAN-INTEGRASI-PERISTIWA-0015	INFO	<schema.name>Perubahan DDL <DDL Change>telah diterapkan ke tabel.
Operasi	PERUBAHAN-INTEGRASI-PERISTIWA-0016	INFO	<copy of request arguments>Integrasi nol-ETL Anda <integration name>memproses permintaan modifikasi dengan argumen berikut:.
Operasi	PERUBAHAN-INTEGRASI-PERISTIWA-0017	INFO	<integration name>Modifikasi Anda untuk integrasi nol-ETL telah diterapkan.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Operasi	PERUBAHAN-INTEGRASI-PERISTIWA-0018	WARNING	Target cluster Amazon Redshift sedang dijeda. Tunggu cluster dijeda dan kemudian lanjutkan untuk melanjutkan streaming data.
Operasi	PERUBAHAN-INTEGRASI-PERISTIWA-0019	WARNING	Target cluster Amazon Redshift sedang dijeda. Lanjutkan cluster untuk melanjutkan streaming data.
Operasi	PERUBAHAN-INTEGRASI-PERISTIWA-0020	WARNING	Target cluster Amazon Redshift sedang dilanjutkan. Tunggu cluster aktif untuk melanjutkan streaming data.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Konfigurasi	PERGESERAN MERAH-INTEGRASI-PERISTIWA-1000	ERROR	Satu atau lebih parameter pada sumber Aurora DB cluster DB cluster DB salah dikonfigurasi. Perbaiki grup parameter dan reboot cluster untuk menerapkan perubahan, lalu buat ulang integrasi.
Konfigurasi	PERGESERAN MERAH-INTEGRASI-PERISTIWA-1001	ERROR	Integrasi gagal karena nilai parameter <code>enable_case_sensitive_identifier</code> salah. Tetapkan nilai ke <code>true</code> untuk cluster DB cluster Aurora DB sumber, lalu hapus dan buat ulang integrasi.
Konfigurasi	PERGESERAN MERAH-INTEGRASI-PERISTIWA-1002	ERROR	Integrasi gagal karena nilai parameter <code>cdc_insert_enabled</code> salah. Tetapkan nilai ke <code>true</code> untuk cluster DB cluster Aurora DB sumber, lalu hapus dan buat ulang integrasi.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Konfigurasi	PERGESERAN MERAH-INTEGRASI-PERISTIWA-1003	ERROR	Parameter <code>binlog_format</code> dalam kelompok parameter cluster DB sumber harus disetel ke ROW. Perbaiki grup parameter dan reboot cluster untuk menerapkan perubahan, lalu buat ulang integrasi.
Konfigurasi	PERGESERAN MERAH-INTEGRASI-PERISTIWA-1004	ERROR	Tidak dapat memuat data karena parameter cluster <code>binlog_transaction_compression</code> diaktifkan. Setel nilai parameter ke OFF dan reboot instance writer untuk menerapkan perubahan, lalu buat ulang integrasi.

Kategori Amazon Redshift	ID Peristiwa Eksternal	Tingkat Keparahan Acara	Deskripsi Pesan
Konfigurasi	PERGESERAN MERAH-INTEGRASI-PERISTIWA-1005	ERROR	Tidak dapat memuat data karena parameter cluster <code>binlog_row_value_options</code> disetel ke <code>PARTIAL_JSON</code> , yang tidak didukung. Perbaiki grup parameter dan reboot instance penulis untuk menerapkan perubahan, lalu buat ulang integrasi.
Konfigurasi	PERGESERAN MERAH-INTEGRASI-PERISTIWA-1006	WARNING	Tidak dapat mengurai filter integrasi. Perbaiki sintaks filter.

Kuota dan batas di Amazon Redshift

Amazon Redshift memiliki kuota yang membatasi penggunaan beberapa sumber daya di AWS akun Anda per Wilayah. AWS Ada nilai default untuk setiap kuota dan beberapa kuota dapat disesuaikan. Untuk kuota yang dapat disesuaikan, Anda dapat meminta peningkatan untuk AWS akun Anda di AWS Wilayah dengan mengirimkan Formulir Peningkatan Batas Pergeseran Merah [Amazon](#).

Kuota untuk objek Amazon Redshift

Amazon Redshift memiliki kuota yang membatasi penggunaan beberapa jenis objek. Ada nilai default untuk masing-masing.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
AWS akun yang dapat Anda otorisasi untuk memulihkan snapshot per snapshot	20	Tidak	Jumlah maksimum AWS akun yang dapat Anda otorisasi untuk memulihkan snapshot, per snapshot.
AWS akun yang dapat Anda otorisasi untuk memulihkan snapshot per AWS KMS key	100	Tidak	Jumlah maksimum AWS akun yang dapat Anda otorisasi untuk memulihkan snapshot, per kunci KMS. Artinya, jika Anda memiliki 10 snapshot yang dienkripsi dengan satu kunci KMS, maka Anda dapat mengotorisasi 10 AWS akun untuk memulihkan setiap snapshot, atau kombinasi lain yang menambahkan hingga 100 akun dan tidak melebihi 20 akun untuk setiap snapshot.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Peran IAM cluster untuk Amazon Redshift untuk mengakses layanan lain AWS	50 ¹	Tidak	Jumlah maksimum peran IAM yang dapat Anda kaitkan dengan klaster untuk mengotorisasi Amazon Redshift untuk mengakses layanan AWS lain bagi pengguna yang memiliki peran klaster dan IAM. ¹ Kuota adalah 10 sebagai berikut Wilayah AWS: us-iso-east -1, -1, us-iso-west us-isob-east -1.
Tingkat konkurensi (slot kueri) untuk semua antrian WLM manual yang ditentukan pengguna	50	Tidak	Slot kueri maksimum untuk semua antrian yang ditentukan pengguna yang ditentukan oleh manajemen beban kerja manual.
Cluster penskalaan konkurensi	10	Ya	Jumlah maksimum cluster penskalaan konkurensi.
Node DC2 dalam sebuah cluster	128	Ya	Jumlah maksimum node DC2 yang dapat Anda alokasikan ke cluster. Untuk informasi selengkapnya tentang batas node untuk setiap jenis node, lihat Cluster dan node di Amazon Redshift .
Langganan kejadian	20	Ya	Jumlah maksimum langganan acara untuk akun ini di AWS Wilayah saat ini.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Simpul	200	Ya	Jumlah maksimum node di semua instance database untuk akun ini di AWS Wilayah saat ini.
Grup parameter	20	Tidak	Jumlah maksimum grup parameter untuk akun ini di AWS Wilayah saat ini.
Node RA3 dalam sebuah cluster	128	Ya	Jumlah maksimum node RA3 yang dapat Anda alokasikan ke cluster. Untuk informasi selengkapnya tentang batas node untuk setiap jenis node, lihat Cluster dan node di Amazon Redshift .
Titik akhir VPC yang dikelola Redshift terhubung ke klaster	30	Ya	Jumlah maksimum titik akhir VPC yang dikelola RedShift yang dapat Anda sambungkan ke cluster. Untuk informasi selengkapnya tentang titik akhir VPC yang dikelola RedShift, lihat. Bekerja dengan titik akhir VPC yang dikelola Redshift
Penerima hibah untuk cluster yang diakses melalui titik akhir VPC yang dikelola RedShift	5	Ya	Jumlah maksimum penerima hibah yang dapat diotorisasi oleh pemilik klaster untuk membuat titik akhir VPC yang dikelola RedShift untuk sebuah cluster. Untuk informasi selengkapnya tentang titik akhir VPC yang dikelola RedShift, lihat. Bekerja dengan titik akhir VPC yang dikelola Redshift

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Titik akhir VPC yang dikelola Redshift per otorisasi	5	Ya	Jumlah maksimum titik akhir VPC yang dikelola RedShift yang dapat Anda buat per otorisasi. Untuk informasi selengkapnya tentang titik akhir VPC yang dikelola RedShift, lihat. Bekerja dengan titik akhir VPC yang dikelola Redshift
Simpul terpesan	200	Ya	Jumlah maksimum node yang dicadangkan untuk akun ini di AWS Wilayah saat ini.
Skema di setiap database per cluster	9,900	Tidak	Jumlah maksimum skema yang dapat Anda buat di setiap database, per cluster. Namun, pg_temp_* skema tidak diperhitungkan dalam kuota ini.
Grup keamanan	20	Ya	Jumlah maksimum grup keamanan untuk akun ini di AWS Wilayah saat ini.
Ukuran baris tunggal saat memuat dengan COPY	4	Tidak	Ukuran maksimum (dalam MB) dari satu baris saat memuat dengan menggunakan perintah COPY.
Snapshot	700	Ya	Jumlah maksimum snapshot pengguna untuk akun ini di AWS Wilayah saat ini.
Grup subnet	20	Ya	Jumlah maksimum grup subnet untuk akun ini di AWS Wilayah saat ini.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Subnet dalam grup subnet	20	Ya	Jumlah maksimum subnet untuk grup subnet.
Tabel untuk tipe node large cluster	9,900	Tidak	Jumlah maksimum tabel untuk tipe node cluster besar. Batas ini mencakup tabel permanen, tabel sementara, tabel datashare, dan tampilan terwujud. Tabel eksternal dihitung sebagai tabel sementara. Tabel sementara mencakup tabel sementara yang ditentukan pengguna dan tabel sementara yang dibuat oleh Amazon Redshift selama pemrosesan kueri atau pemeliharaan sistem. Tampilan dan tabel sistem tidak termasuk dalam batas ini.
Tabel untuk tipe node xlarge cluster	9,900	Tidak	Jumlah maksimum tabel untuk tipe node xlarge cluster. Batas ini mencakup tabel permanen, tabel sementara, tabel datashare, dan tampilan terwujud. Tabel eksternal dihitung sebagai tabel sementara. Tabel sementara mencakup tabel sementara yang ditentukan pengguna dan tabel sementara yang dibuat oleh Amazon Redshift selama pemrosesan kueri atau pemeliharaan sistem. Tampilan dan tabel sistem tidak termasuk dalam batas ini.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Tabel untuk tipe node x1plus cluster dengan cluster single-node.	9,900	Tidak	Jumlah maksimum tabel untuk tipe node x1plus cluster dengan cluster single-node. Batas ini mencakup tabel permanen, tabel sementara, tabel datashare, dan tampilan terwujud. Tabel eksternal dihitung sebagai tabel sementara. Tabel sementara mencakup tabel sementara yang ditentukan pengguna dan tabel sementara yang dibuat oleh Amazon Redshift selama pemrosesan kueri atau pemeliharaan sistem. Tampilan dan tabel sistem tidak termasuk dalam batas ini.
Tabel untuk tipe node x1plus cluster dengan cluster multiple-node.	20.000	Tidak	Jumlah maksimum tabel untuk tipe node x1plus cluster dengan cluster multiple-node. Batas ini mencakup tabel permanen, tabel sementara, tabel datashare, dan tampilan terwujud. Tabel eksternal dihitung sebagai tabel sementara. Tabel sementara mencakup tabel sementara yang ditentukan pengguna dan tabel sementara yang dibuat oleh Amazon Redshift selama pemrosesan kueri atau pemeliharaan sistem. Tampilan dan tabel sistem tidak termasuk dalam batas ini.
Tabel untuk tipe node 4xlarge cluster	200.000	Tidak	Jumlah maksimum tabel untuk tipe node 4xlarge cluster. Batas ini mencakup tabel permanen, tabel sementara, tabel datashare, dan tampilan terwujud. Tabel eksternal dihitung sebagai tabel sementara. Tabel sementara mencakup tabel sementara yang ditentukan pengguna dan tabel sementara yang dibuat oleh Amazon Redshift selama pemrosesan kueri atau pemeliharaan sistem. Tampilan dan tabel sistem tidak termasuk dalam batas ini.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Tabel untuk tipe node 8xlarge cluster	200.000	Tidak	Jumlah maksimum tabel untuk tipe node 8xlarge cluster. Batas ini mencakup tabel permanen, tabel sementara, tabel datashare, dan tampilan terwujud. Tabel eksternal dihitung sebagai tabel sementara. Tabel sementara mencakup tabel sementara yang ditentukan pengguna dan tabel sementara yang dibuat oleh Amazon Redshift selama pemrosesan kueri atau pemeliharaan sistem. Tampilan dan tabel sistem tidak termasuk dalam batas ini.
Tabel untuk tipe node 16xlarge cluster	200.000	Tidak	Jumlah maksimum tabel untuk tipe node 16xlarge cluster. Batas ini mencakup tabel permanen, tabel sementara, tabel datashare, dan tampilan terwujud. Tabel eksternal dihitung sebagai tabel sementara. Tabel sementara mencakup tabel sementara yang ditentukan pengguna dan tabel sementara yang dibuat oleh Amazon Redshift selama pemrosesan kueri atau pemeliharaan sistem. Tampilan dan tabel sistem tidak termasuk dalam batas ini.
Jumlah database	60	Tidak	Jumlah maksimum database yang diizinkan dalam cluster Amazon Redshift. Ini tidak termasuk database yang dibuat dari datashares.
Batas waktu untuk sesi idle atau tidak aktif	4 jam	Tidak	Pengaturan ini berlaku untuk cluster. Untuk informasi tentang menyetel nilai batas waktu sesi siaga bagi pengguna, lihat MENGUBAH PENGGUNA di Panduan Pengembang Database Amazon Redshift. Pengaturan pengguna lebih diutamakan daripada pengaturan cluster.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Timeout untuk transaksi idle	6 jam	Tidak	Periode maksimum tidak aktif untuk transaksi terbuka sebelum Amazon Redshift mengakhiri sesi yang terkait dengan transaksi. Pengaturan ini lebih diutamakan daripada setelan batas waktu idle yang ditentukan pengguna. Ini berlaku untuk cluster.
Prosedur tersimpan dalam database	10.000	Tidak	Jumlah maksimum prosedur yang disimpan. Lihat Batas dan perbedaan untuk dukungan prosedur tersimpan untuk batasan lainnya.
Jumlah maksimum koneksi untuk node RA3	2.000	Tidak	Jumlah maksimum koneksi ke cluster RA3. (Ini berlaku khusus untuk tipe node ra3.xlplus, ra3.4xlarge dan ra3.16xlarge.) Koneksi maksimum yang diizinkan bervariasi menurut jenis node.
Jumlah maksimum koneksi untuk node DC2	Bervariasi	Tidak	Jumlah maksimum koneksi ke cluster dc2.large adalah 500. Jumlah maksimum koneksi untuk cluster dc2.8xlarge adalah 2000.
Jumlah peran Amazon Redshift dalam sebuah cluster	1.000	Ya	Jumlah maksimum peran Amazon Redshift yang dapat Anda buat per cluster. Untuk informasi selengkapnya tentang peran kontrol akses berbasis peran (RBAC), lihat Kontrol akses berbasis peran (RBAC) di Panduan Pengembang Database Amazon Redshift

Kuota untuk objek Amazon Redshift Tanpa Server

Amazon Redshift memiliki kuota yang membatasi penggunaan beberapa jenis objek di instans Amazon Redshift Tanpa Server Anda. Ada nilai default untuk masing-masing.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Jumlah database	100	Tidak	Jumlah maksimum database yang diizinkan di namespace Amazon Redshift Tanpa Server. Ini tidak termasuk database yang dibuat dari datashares.
Jumlah skema	9,900	Tidak	Jumlah maksimum skema yang diizinkan dalam instance Amazon Redshift Tanpa Server.
Jumlah tabel	200.000	Tidak	Jumlah maksimum tabel yang diizinkan dalam instance Amazon Redshift Tanpa Server.
Batas waktu untuk sesi idle atau tidak aktif	1 jam	Tidak	Untuk informasi tentang menyetel nilai batas waktu sesi siaga bagi pengguna, lihat MENGUBAH PENGGUNA di Panduan Pengembang Database Amazon Redshift. Pengaturan pengguna diutamakan.
Batas waktu untuk kueri yang sedang berjalan	86,399 detik (24 jam)	Tidak	Waktu maksimum untuk kueri yang berjalan sebelum Amazon Redshift mengakhirinya.
Timeout untuk transaksi idle	6 jam	Tidak	Periode maksimum tidak aktif untuk transaksi terbuka sebelum Amazon Redshift Serverless mengakhiri sesi yang terkait dengan transaksi. Pengaturan ini lebih diutamakan daripada setelan batas waktu idle yang ditentukan pengguna.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Jumlah koneksi maksimum	2000	Tidak	Jumlah maksimum koneksi yang diizinkan untuk terhubung ke workgroup.
Jumlah kelompok kerja	25	Ya	Jumlah kelompok kerja yang didukung.
Jumlah ruang nama	25	Ya	Jumlah ruang nama yang didukung.
Jumlah peran Amazon Redshift dalam workgroup	1.000	Ya	Jumlah maksimum peran Amazon Redshift yang dapat Anda buat per workgroup. Untuk informasi selengkapnya tentang peran kontrol akses berbasis peran (RBAC), lihat Kontrol akses berbasis peran (RBAC) di Panduan Pengembang Database Amazon Redshift

Untuk informasi selengkapnya tentang bagaimana penagihan Amazon Redshift Tanpa Server dipengaruhi oleh konfigurasi batas waktu, lihat. [Penagihan untuk Amazon Redshift Tanpa Server](#)

Kuota untuk Amazon Redshift Data API

Amazon Redshift memiliki kuota yang membatasi penggunaan Redshift Data API. Ada nilai default untuk masing-masing. Untuk informasi selengkapnya tentang Amazon Redshift Data API, lihat. [Menggunakan API Data Amazon Redshift](#)

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Transaksi per detik (TPS) untuk API BatchExecuteStatement	20	Tidak	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling.
Transaksi per detik (TPS) untuk API CancelStatement	3	Tidak	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling.
Transaksi per detik (TPS) untuk API DescribeStatement	100	Tidak	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling.
Transaksi per detik (TPS) untuk API DescribeTable	3	Tidak	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling.
Transaksi per detik (TPS) untuk API	30	Tidak	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
ExecuteStatement			
Transaksi per detik (TPS) untuk API GetStatementResult	20	Tidak	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling.
Transaksi per detik (TPS) untuk API ListDatabases	3	Tidak	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling.
Transaksi per detik (TPS) untuk API ListSchemas	3	Tidak	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling.
Transaksi per detik (TPS) untuk API ListStatements	3	Tidak	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Transaksi per detik (TPS) untuk API ListTables	3	Tidak	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling.

Kuota untuk objek editor kueri v2

Amazon Redshift memiliki kuota yang membatasi penggunaan beberapa jenis objek di editor kueri Amazon Redshift v2 Anda. Ada nilai default untuk masing-masing.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Koneksi	500	Ya	Jumlah maksimum koneksi yang dapat Anda buat menggunakan editor kueri v2 di akun ini di Wilayah saat ini.
Prinsipal aktif per akun	50	Ya	Jumlah maksimum prinsipal simultan yang dapat menggunakan editor kueri v2 di akun ini di Wilayah saat ini.
Kueri tersimpan	2.500	Ya	Jumlah maksimum kueri tersimpan yang dapat Anda buat menggunakan editor kueri v2 di akun ini di Wilayah saat ini.
Versi kueri	20	Ya	Jumlah maksimum versi per kueri yang dapat Anda buat menggunakan editor kueri v2 di akun ini di Wilayah saat ini.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Bagan tersimpan	500	Ya	Jumlah maksimum bagan tersimpan yang dapat Anda buat menggunakan editor kueri v2 di akun ini di Wilayah saat ini.
Baris diambil per kueri	100.000	Tidak	Jumlah maksimum baris yang diambil per kueri oleh editor kueri v2 di akun ini di Wilayah saat ini.
Ukuran data diambil per kueri	5	Tidak	Ukuran maksimum, dalam megabyte, dari data yang diambil per kueri oleh editor kueri v2 di akun ini di Wilayah saat ini.
Koneksi soket simultan per prinsipal	10	Ya	Jumlah maksimum koneksi soket simultan ke editor kueri v2 yang dapat dibuat oleh satu prinsipal di Wilayah saat ini. Evaluasi apakah akan meningkatkan kuota ini jika Anda menerima kesalahan bahwa koneksi soket Anda melebihi batas.
Koneksi soket simultan per akun	250	Ya	Jumlah maksimum koneksi soket simultan ke editor kueri v2 yang dapat dibuat oleh semua prinsipal di akun di Wilayah saat ini. Evaluasi apakah akan meningkatkan kuota ini jika Anda menerima kesalahan bahwa koneksi soket Anda melebihi batas.

Nama kuota	AWS nilai default	Dapat disesuaikan	Deskripsi
Koneksi bersamaan maksimum	3	Tidak	Koneksi database maksimum per pengguna (termasuk sesi terisolasi). Nilai ini dapat diatur dari 1-10 oleh administrator editor kueri v2 di Pengaturan akun. Jika Anda mencapai batas yang ditetapkan oleh administrator Anda, pertimbangkan untuk menggunakan sesi bersama alih-alih sesi terisolasi saat menjalankan SQL Anda. Untuk informasi selengkapnya tentang koneksi, lihat Membuka editor kueri v2 . Untuk informasi selengkapnya tentang menetapkan batas, lihat Mengubah pengaturan akun .

Kuota dan batas untuk objek Amazon Redshift Spectrum

Amazon Redshift Spectrum memiliki kuota dan batasan berikut:

- Jumlah maksimum database per AWS akun saat menggunakan file AWS Glue Data Catalog. Untuk nilai ini, lihat [kuota AWS Glue layanan](#) di. Referensi Umum Amazon Web Services
- Jumlah maksimum tabel per database saat menggunakan file AWS Glue Data Catalog. Untuk nilai ini, lihat [kuota AWS Glue layanan](#) di. Referensi Umum Amazon Web Services
- Jumlah maksimum partisi per tabel saat menggunakan file AWS Glue Data Catalog. Untuk nilai ini, lihat [kuota AWS Glue layanan](#) di. Referensi Umum Amazon Web Services
- Jumlah maksimum partisi per AWS akun saat menggunakan file AWS Glue Data Catalog. Untuk nilai ini, lihat [kuota AWS Glue layanan](#) di. Referensi Umum Amazon Web Services
- Jumlah maksimum kolom untuk tabel eksternal saat menggunakan AWS Glue Data Catalog, 1.597 saat pseudocolumns diaktifkan, dan 1.600 saat pseudocolumns tidak diaktifkan.
- Ukuran maksimum nilai string dalam file ION atau JSON saat menggunakan AWS Glue Data Catalog adalah 16 KB. String dapat dipotong jika Anda mencapai batas ini.
- Anda dapat menambahkan maksimal 100 partisi menggunakan pernyataan ALTER TABLE tunggal.
- Semua data S3 harus berada di AWS Wilayah yang sama dengan cluster Amazon Redshift.

- [Stempel waktu dalam ION dan JSON harus menggunakan format ISO8601.](#)
- Kompresi eksternal file ORC tidak didukung.
- Text, OpenCSV, dan Regex SerDes tidak mendukung pembatas oktal yang lebih besar dari '\ 177'.
- Anda harus menentukan predikat pada kolom partisi untuk menghindari pembacaan dari semua partisi.

Misalnya, filter predikat berikut pada kolom `ship_dtm`, tetapi tidak menerapkan filter ke kolom `ship_yyyymm` partisi:

```
WHERE ship_dtm > '2018-04-01'.
```

Untuk melewati partisi yang tidak dibutuhkan, Anda perlu menambahkan predikat. `WHERE ship_yyyymm = '201804'` Predikat ini membatasi operasi baca ke `\ship_yyyymm=201804\` partisi.

Batasan ini tidak berlaku untuk metastore Apache Hive.

Kendala penamaan

Tabel berikut menjelaskan batasan penamaan dalam Amazon Redshift.

Pengidentifikasi kluster	<ul style="list-style-type: none"> • Sebuah identifier cluster harus berisi hanya karakter huruf kecil. • Pengidentifikasi ini harus berisi 1-63 karakter alfanumerik atau tanda hubung. • Karakter pertamanya harus berupa huruf. • Pengidentifikasi ini tidak boleh diakhiri dengan tanda hubung atau mengandung dua tanda hubung berturut-turut. • Itu harus unik untuk semua cluster dalam AWS akun.
Nama basis data	<ul style="list-style-type: none"> • Nama database harus berisi 1-64 karakter alfanumerik.

	<ul style="list-style-type: none">• Itu harus berisi hanya huruf kecil.• Itu tidak bisa menjadi kata yang dicadangkan. Untuk daftar kata yang dicadangkan, lihat Kata-kata yang dicadangkan di Panduan Pengembang Database Amazon Redshift.
Nama titik akhir dari titik akhir VPC yang dikelola RedShift	<ul style="list-style-type: none">• Nama endpoint harus berisi 1—30 karakter.• Karakter yang valid adalah A-Z, a-z, 0-9, dan tanda hubung (-).• Karakter pertama harus berupa huruf.• Nama tidak dapat berisi dua tanda hubung berturut-turut atau diakhiri dengan tanda hubung.
Nama pengguna admin	<ul style="list-style-type: none">• Nama pengguna admin harus hanya berisi karakter huruf kecil.• Itu harus berisi 1-128 karakter alfanumerik.• Karakter pertamanya harus berupa huruf.• Itu tidak bisa menjadi kata yang dicadangkan. Untuk daftar kata yang dicadangkan, lihat Kata-kata yang dicadangkan di Panduan Pengembang Database Amazon Redshift.

Kata sandi admin	<ul style="list-style-type: none">• Kata sandi admin harus berisi 8-64 karakter.• Itu harus berisi setidaknya satu huruf besar.• Itu harus berisi setidaknya satu huruf kecil.• Itu harus berisi satu nomor.• <p>Ini dapat menggunakan karakter ASCII apa pun dengan kode ASCII 33—126, kecuali '(kutipan tunggal), "(kutipan ganda), \, /, atau @.</p>
Nama grup parameter	<ul style="list-style-type: none">• Nama grup parameter harus berisi 1-255 karakter alfanumerik atau tanda hubung.• Itu harus berisi hanya karakter huruf kecil.• Karakter pertama harus berupa huruf.• Pengidentifikasi ini tidak boleh diakhiri dengan tanda hubung atau mengandung dua tanda hubung berturut-turut.
Nama grup keamanan klaster	<ul style="list-style-type: none">• Nama grup keamanan klaster harus berisi tidak lebih dari 255 karakter alfanumerik atau tanda hubung.• Itu harus berisi hanya karakter huruf kecil.• Itu tidak harus Default.• Ini harus unik untuk semua grup keamanan yang dibuat oleh AWS akun Anda.

Nama grup subnet	<ul style="list-style-type: none">• Nama grup subnet harus berisi tidak lebih dari 255 karakter alfanumerik atau tanda hubung.• Itu harus berisi hanya karakter huruf kecil.• Itu tidak harus Default.• Ini harus unik untuk semua grup subnet yang dibuat oleh AWS akun Anda.
Pengidentifikasi snapshot cluster	<ul style="list-style-type: none">• Pengidentifikasi snapshot cluster harus berisi tidak lebih dari 255 karakter alfanumerik atau tanda hubung.• Itu harus berisi hanya karakter huruf kecil.• Itu tidak harus Default.• Itu harus unik untuk semua pengidentifikasi snapshot yang dibuat oleh akun Anda AWS .

Menandai sumber daya di Amazon Redshift

Topik

- [Ikhtisar penandaan](#)
- [Mengelola tag sumber daya menggunakan konsol](#)
- [Mengelola tag menggunakan Amazon Redshift API](#)

Ikhtisar penandaan

Dalam AWS, tag adalah label yang ditentukan pengguna yang terdiri dari pasangan nilai kunci. Amazon Redshift mendukung penandaan untuk memberikan metadata tentang sumber daya secara sekilas, dan untuk mengkategorikan laporan penagihan berdasarkan alokasi biaya. Untuk menggunakan tag untuk alokasi biaya, Anda harus terlebih dahulu mengaktifkan tag tersebut di AWS Billing and Cost Management layanan. Untuk informasi selengkapnya tentang menyiapkan dan menggunakan tag untuk tujuan penagihan, lihat [Menggunakan tag alokasi biaya untuk laporan penagihan khusus dan Menyiapkan laporan alokasi biaya bulanan Anda](#).

Tag tidak diperlukan untuk sumber daya di Amazon Redshift, tetapi tag membantu memberikan konteks. Anda mungkin ingin menandai sumber daya dengan metadata tentang pusat biaya, nama proyek, dan informasi terkait lainnya yang terkait dengan sumber daya. Misalnya, Anda ingin melacak sumber daya mana yang termasuk dalam lingkungan pengujian dan lingkungan produksi. Anda dapat membuat kunci bernama `environment` dan memberikan nilai `test` atau `production` untuk mengidentifikasi sumber daya yang digunakan di setiap lingkungan. Jika Anda menggunakan penandaan di AWS layanan lain atau memiliki kategori standar untuk bisnis Anda, kami sarankan Anda membuat pasangan nilai kunci yang sama untuk sumber daya di Amazon Redshift untuk konsistensi.

Tag disimpan untuk sumber daya setelah Anda mengubah ukuran klaster, dan setelah Anda memulihkan snapshot klaster dalam wilayah yang sama. Namun, tag tidak dipertahankan jika Anda menyalin snapshot ke wilayah lain, jadi Anda harus membuat ulang tag di wilayah baru. Jika Anda menghapus sumber daya, tag terkait akan dihapus.

Setiap sumber daya memiliki satu set tag, yang merupakan kumpulan dari satu atau beberapa tag yang ditetapkan ke sumber daya. Setiap sumber daya dapat memiliki hingga 50 tag per set tag. Anda dapat menambahkan tag saat membuat sumber daya dan setelah sumber daya dibuat. Anda dapat menambahkan tag ke jenis sumber daya berikut di Amazon Redshift:

- CIDR/IP
- Klaster
- Grup keamanan klaster
- Aturan masuknya grup keamanan klaster
- Grup keamanan Amazon EC2
- Koneksi modul keamanan perangkat keras (HSM)
- Sertifikat klien HSM
- Grup parameter
- Snapshot
- Grup subnet

Untuk menggunakan penandaan dari konsol Amazon Redshift, pengguna Anda dapat melampirkan kebijakan terkelola AWS. `AmazonRedshiftFullAccess` Untuk contoh kebijakan IAM dengan izin penandaan terbatas yang dapat Anda lampirkan ke pengguna konsol Amazon Redshift, lihat. [Contoh 7: Izinkan pengguna menandai sumber daya dengan konsol Amazon Redshift](#) Untuk informasi selengkapnya tentang penandaan, lihat [Apa itu AWS Resource Groups?](#) .

Persyaratan penandaan

Tag memiliki persyaratan sebagai berikut:

- Kunci tidak dapat diawali dengan `aws :`.
- Kunci harus unik per set tag.
- Kunci harus antara 1 dan 128 karakter yang diizinkan.
- Nilai harus antara 0 dan 256 karakter yang diizinkan.
- Nilai tidak harus unik per set tag.
- Karakter yang diizinkan untuk kunci dan nilai adalah huruf Unicode, digit, spasi putih, dan salah satu simbol berikut: `._:/= + - @`.
- Kunci dan nilai peka huruf besar dan kecil.

Mengelola tag sumber daya menggunakan konsol

Untuk mengelola tag di sumber daya Amazon Redshift Anda

1. [Masuk ke AWS Management Console dan buka konsol Amazon Redshift di https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Pada menu navigasi, pilih Konfigurasi, lalu pilih Kelola tag.
3. Masukkan pilihan Anda untuk sumber daya dan pilih tag mana yang akan ditambahkan, dimodifikasi, atau dihapus. Kemudian pilih Kelola tag sumber daya yang Anda pilih.

Sumber daya yang dapat Anda tag termasuk cluster, grup parameter, grup subnet, sertifikat klien HSM, koneksi HSM, dan snapshot.

4. Pada halaman navigasi Kelola tag, pilih Tinjau dan terapkan perubahan tag, lalu pilih Terapkan untuk menyimpan perubahan Anda.

Mengelola tag menggunakan Amazon Redshift API

Anda dapat menggunakan AWS CLI operasi berikut untuk mengelola tag di Amazon Redshift.

- [create-tags](#)
- [delete-tags](#)
- [describe-tags](#)

Anda dapat menggunakan operasi Amazon Redshift API berikut untuk mengelola tag:

- [CreateTags](#)
- [DeleteTags](#)
- [DescribeTags](#)
- [Tag](#)
- [TaggedResource](#)

Selain itu, Anda dapat menggunakan operasi Amazon Redshift API berikut untuk mengelola dan melihat tag untuk sumber daya tertentu:

- [CreateCluster](#)

- [CreateClusterParameterGroup](#)
- [CreateClusterSecurityGroup](#)
- [CreateClusterSnapshot](#)
- [CreateClusterSubnetGroup](#)
- [CreateHsmClientCertificate](#)
- [CreateHsmConfiguration](#)
- [DescribeClusters](#)
- [DescribeClusterParameterGroups](#)
- [DescribeClusterSecurityGroups](#)
- [DescribeClusterSnapshots](#)
- [DescribeClusterSubnetGroups](#)
- [DescribeHsmClientCertificates](#)
- [DescribeHsmConfigurations](#)

Versi cluster untuk Amazon Redshift

Amazon Redshift secara teratur merilis versi cluster. Cluster Amazon Redshift Anda ditambal selama jendela pemeliharaan sistem Anda. Waktu tambalan tergantung pada pengaturan jendela Anda Wilayah AWS dan pemeliharaan. Anda dapat melihat atau mengubah pengaturan jendela pemeliharaan dari konsol Amazon Redshift. Untuk informasi lebih lanjut tentang pemeliharaan, lihat [Pemeliharaan cluster](#).

Anda dapat melihat versi cluster cluster Anda di konsol Amazon Redshift pada tab Maintenance pada detail cluster. Atau Anda dapat melihat versi cluster di output dari perintah SQL:

```
SELECT version();
```

Topik

- [Patch Pergeseran Merah Amazon 181](#)
- [Patch Pergeseran Merah Amazon 180](#)
- [Patch Pergeseran Merah Amazon 179](#)
- [Patch Pergeseran Merah Amazon 178](#)
- [Patch Pergeseran Merah Amazon 177](#)
- [Patch Pergeseran Merah Amazon 176](#)
- [Patch Pergeseran Merah Amazon 175](#)
- [Patch Pergeseran Merah Amazon 174](#)
- [Patch Pergeseran Merah Amazon 173](#)
- [Patch Pergeseran Merah Amazon 172](#)
- [Patch Pergeseran Merah Amazon 171](#)
- [Patch Pergeseran Merah Amazon 170](#)
- [Patch Pergeseran Merah Amazon 169](#)
- [Patch Pergeseran Merah Amazon 168](#)

Patch Pergeseran Merah Amazon 181

Versi cluster di tambalan ini:

- 1.0.69497 - Amazon Redshift Versi Tanpa Server - Dirilis pada 18 Juni 2024

- 1.0.69451 - Versi trek saat ini - Dirilis pada 18 Juni 2024
- 1.0.69076 - Amazon Redshift Versi Tanpa Server - Dirilis pada 14 Juni 2024
- 1.0.69065 - Versi trek saat ini - Dirilis pada 14 Juni 2024
- 1.0.68555 - Amazon Redshift Versi Tanpa Server - Dirilis pada 31 Mei 2024
- 1.0.68540 - Versi trek saat ini - Dirilis pada 31 Mei 2024
- 1.0.68328 - Amazon Redshift Versi Tanpa Server - Dirilis pada 23 Mei 2024
- 1.0.68205 - Versi trek saat ini - Dirilis pada 23 Mei 2024
- 1.0.67796 - Amazon Redshift Versi Tanpa Server - Dirilis pada 15 Mei 2024
- 1.0.67788 - Versi trek saat ini - Dirilis pada 15 Mei 2024
- 1.0.67308 - Amazon Redshift Versi Tanpa Server - Dirilis pada 1 Mei 2024
- 1.0.67305 - Versi trek saat ini - Dirilis pada 1 Mei 2024

Fitur dan peningkatan baru di tambalan ini

- Memperkenalkan dukungan untuk mengubah kunci distribusi dan mengurutkan kunci tampilan yang terwujud.
- Memperkenalkan dukungan untuk fungsi 'lower_attribute_names ()' dan 'upper_attribute_names ()' yang memodifikasi kasus nama atribut untuk nilai objek SUPER.
- Memperbaiki masalah di CREATE TABLE LIKE saat menggunakan kolom identitas. Sebelumnya, tabel baru akan mewarisi pengenal dari tabel sumber. Ini menyebabkan masalah jika tabel sumber kemudian dijatuhkan, karena pengenal akan menjadi tidak valid di tabel baru.
- Memperbaiki masalah yang mencegah beberapa tabel eksternal ditampilkan di SVV_ALL_TABLES.
- Meningkatkan waktu bootstrap cluster, dan mempercepat inisialisasi kueri untuk beban kerja bersamaan yang tinggi.
- Memperbaiki masalah dengan kueri federasi yang menyebabkan kesalahan saat meneruskan fungsi split_part () ke sumber federasi ke RDS dan Aurora MySQL
- Mendukung perubahan yang dimulai pengguna pada kunci distribusi melalui ALTER TABLE... ALTER DISTYLE KEY DISTYLE perintah pada cluster penskalaan konkurensi yang disediakan dan komputasi penskalaan otomatis tanpa server.
- Mendukung tampilan terwujud yang disegarkan secara manual yang melibatkan agregasi pada penskalaan konkurensi yang disediakan dan komputasi penskalaan otomatis tanpa server.
- Menambahkan dukungan untuk Zero-ETL untuk menangani catatan hingga 16 MB dalam ukuran dan untuk mendukung nilai SUPER hingga 16 MB.

- Meningkatkan pesan kesalahan selama sinkronisasi awal di nol-ETL dari Aurora MySQL dengan memberikan rincian tambahan seperti skema dan nama tabel.
- Memperkenalkan dukungan untuk penandaan dengan Amazon Redshift MLCREATE MODEL. Dengan peningkatan ini, Anda sekarang dapat menandai SageMaker sumber daya Amazon yang digunakan oleh Amazon Redshift ML. Penandaan membantu Anda mengelola, mengidentifikasi, mengatur, mencari, dan memfilter sumber daya.
- Meningkatkan kinerja kueri yang melibatkan fungsi yang ditentukan pengguna Lambda (UDF) dengan mengoptimalkan pemrosesan data dengan. AWS Lambda
- Mengurangi pemanfaatan memori selama konsumsi data dalam tabel yang diurutkan dari cluster yang diubah ukurannya secara elastis dan tanpa server.
- Menambahkan dukungan untuk baris baru (\n) di kolom dalam tampilan SYS_QUERY_HISTORY dan untuk kolom query_text dalam tampilan SYS_QUERY_TEXT. text

Patch Pergeseran Merah Amazon 180

Versi cluster di tambalan ini:

- 1.0.68870 - Versi trailing track - Dirilis pada 3 Juni 2024
- 1.0.68520 - Versi trailing track - Dirilis pada 28 Mei 2024
- 1.0.67699 - Versi trailing track - Dirilis pada 15 Mei 2024
- 1.0.66960 - Versi trailing track - Dirilis pada 21 April 2024
- 1.0.66954 - Versi trek saat ini - Dirilis pada 21 April 2024
- 1.0.66276 - Versi trek saat ini - Dirilis pada 12 April 2024
- 1.0.66290 - Amazon Redshift Versi Tanpa Server - Dirilis pada 10 April 2024
- 1.0.63590 - Versi trek saat ini - Dirilis pada 19 Februari 2024
- 1.0.63567 - Amazon Redshift Versi Tanpa Server - Dirilis pada 16 Februari 2024
- 1.0.63282 - Amazon Redshift Versi Tanpa Server - Dirilis pada 13 Februari 2024
- 1.0.63269 - Versi trek saat ini - Dirilis pada 13 Februari 2024
- 1.0.63215 - Amazon Redshift Versi Tanpa Server - Dirilis pada 12 Februari 2024
- 1.0.63205 - Versi trek saat ini - Dirilis pada 12 Februari 2024
- 1.0.63030 - Amazon Redshift Versi Tanpa Server - Dirilis pada 7 Februari 2024
- 1.0.62913 - Versi trek saat ini - Dirilis pada 7 Februari 2024

- 1.0.62922 - Amazon Redshift Versi Tanpa Server - Dirilis pada 5 Februari 2024
- 1.0.62878 - Versi trek saat ini - Dirilis pada 5 Februari 2024
- 1.0.62698 - Amazon Redshift Versi Tanpa Server - Dirilis pada 31 Januari 2024
- 1.0.62614 - Versi trek saat ini - Dirilis pada 31 Januari 2024
- 1.0.61687 - Amazon Redshift Versi Tanpa Server - Dirilis pada 5 Januari 2024
- 1.0.61678 - Versi trek saat ini - Dirilis pada 5 Januari 2024
- 1.0.61567 - Amazon Redshift Versi Tanpa Server - Dirilis pada 31 Desember 2023
- 1.0.61559 - Versi trek saat ini - Dirilis pada 31 Desember 2023
- 1.0.61430 - Amazon Redshift Versi Tanpa Server - Dirilis pada 29 Desember 2023
- 1.0.61395 - Versi trek saat ini - Dirilis pada 29 Desember 2023

Fitur dan peningkatan baru di tambalan ini

- Mengubah `CURRENT_USER` agar tidak lagi memotong nama pengguna yang dikembalikan menjadi 64 karakter.
- Menambahkan kemampuan untuk menerapkan kebijakan penyembunyian data pada tampilan standar dan tampilan pengikatan akhir.
- Menambahkan kemampuan untuk menerapkan masking data dinamis (DDM) ke atribut skalar di kolom tipe data SUPER.
- Menambahkan fungsi SQL `OBJECT_TRANSFORM`. Untuk informasi selengkapnya, lihat [fungsi `OBJECT_TRANSFORM` di Panduan Pengembang Database Amazon Redshift](#).
- Menambahkan kemampuan untuk menerapkan kontrol akses AWS Lake Formation berbutir halus ke data bersarang Anda, dan kueri dengan analitik data lake Amazon Redshift.
- Menambahkan tipe data INTERVAL.
- Menambahkan `CONTINUE_HANDLER`, yang merupakan jenis handler pengecualian yang mengontrol aliran prosedur yang disimpan. Dengan menggunakannya, Anda dapat menangkap dan menangani pengecualian tanpa mengakhiri blok pernyataan yang ada.
- Menambahkan kemampuan untuk menentukan izin pada lingkup (skema atau database) selain objek individu. Hal ini memungkinkan pengguna dan peran untuk diberikan izin pada semua objek saat ini dan masa depan dalam lingkup.
- Menambahkan kemampuan untuk membuat database dari datashare dengan izin yang memungkinkan administrator sisi konsumen memberikan izin individu pada objek database bersama kepada pengguna dan peran sisi konsumen.

- Menambahkan dukungan untuk tipe data pengembalian SUPER dari model BYOM jarak jauh. Ini memperluas jangkauan model yang diterima untuk memasukkan SageMaker model dengan format pengembalian yang lebih kompleks.
- Mengubah fungsi eksternal untuk sekarang secara implisit melemparkan angka dengan atau tanpa bagian pecahan ke tipe data numerik kolom. Untuk kolom int2, int4, dan int8, angka dengan digit pecahan diterima dengan memotong kecuali jumlahnya di luar jangkauan. Untuk kolom float4 dan float8, angka diterima tanpa digit fraksional.
- Menambahkan tiga fungsi spasial yang bekerja dengan sistem grid pengindeksan geospasial hierarkis H3: H3_FromLong Lat, H3_, dan H3_Polyfill. FromPoint

Patch Pergeseran Merah Amazon 179

Versi cluster di tambalan ini:

- 1.0.62317 - Amazon Redshift Versi Tanpa Server - Dirilis pada 29 Januari 2024
- 1.0.62312 - Versi trailing track - Dirilis pada 29 Januari 2024
- 1.0.61631 - Amazon Redshift Versi Tanpa Server - Dirilis pada 5 Januari 2024
- 1.0.61626 - Versi trek saat ini - Dirilis pada 5 Januari 2024
- 1.0.61191 - Versi trek saat ini - Dirilis pada 16 Desember 2023
- 1.0.61150 - Amazon Redshift Versi Tanpa Server - Dirilis pada 16 Desember 2023
- 1.0.60982 - Amazon Redshift Versi Tanpa Server - Dirilis pada 13 Desember 2023
- 1.0.60854 - Versi trek saat ini - Dirilis pada 10 Desember 2023
- 1.0.60354 - Amazon Redshift Versi Tanpa Server - Dirilis pada 22 November 2023
- 1.0.60353 - Versi trek saat ini - Dirilis pada 21 November 2023
- 1.0.60293 - Amazon Redshift Versi Tanpa Server - Dirilis pada 21 November 2023
- 1.0.60292 - Versi trek saat ini - Dirilis pada 22 November 2023
- 1.0.60161 - Amazon Redshift Versi Tanpa Server - Dirilis pada 18 November 2023
- 1.0.60140 - Versi trek saat ini - Dirilis pada 18 November 2023
- 1.0.60139 - Amazon Redshift Versi Tanpa Server - Dirilis pada 18 November 2023
- 1.0.59947 - Amazon Redshift Versi Tanpa Server - Dirilis pada 16 November 2023
- 1.0.59945 - Versi trek saat ini - Dirilis pada 16 November 2023

- 1.0.59118 - Amazon Redshift Versi Tanpa Server - Dirilis pada 9 November 2023
- 1.0.59117 - Versi trek saat ini - Dirilis pada 9 November 2023

Fitur dan peningkatan baru di tambalan ini

- Menambahkan dukungan sehingga pengguna federasi dengan izin yang sesuai dapat melihat keamanan tingkat baris dan tampilan sistem masking data dinamis, termasuk:
 - SVV_ATTACHED_MASKING_POLICY
 - SVV_MASKING_POLICY
 - SVV_RLS_ATTACHED_POLICY
 - SVV_RLS_POLICY
 - SVV_RLS_RELASI
- Menambahkan fungsionalitas sedemikian rupa sehingga kueri yang hanya berisi fungsi skalar di klausa FROM sekarang menghasilkan kesalahan.
- Menambahkan pernyataan CREATE TABLE AS (CTAS) dengan fungsionalitas tabel target permanen ke cluster penskalaan konkurensi. Cluster penskalaan konkurensi sekarang mendukung lebih banyak kueri.
- Menambahkan tabel sistem berikut untuk melacak status redistribusi tabel setelah menjalankan perubahan ukuran klasik pada cluster RA3:
 - Tabel sistem SYS_RESTORE_STATE menunjukkan kemajuan redistribusi tingkat tabel.
 - Tabel sistem SYS_RESTORE_LOG menunjukkan throughput historis redistribusi data.
- Meningkatkan kecondongan irisan meminimalkan pada tabel EVEN setelah menjalankan perubahan ukuran klasik pada tipe node RA3. Ini juga berlaku untuk menambal 178 cluster yang menjalankan perubahan ukuran klasik.
- Menambahkan dukungan untuk UNLOAD dengan EXTENSION pada cluster penskalaan konkurensi.
- Meningkatkan kinerja untuk kueri yang berisi \wedge UDF masuk HashJoins dan NestLoop bergabung.
- Meningkatkan kinerja Elastic Resize pada tipe node RA3.
- Meningkatkan kinerja untuk kueri berbagi data.
- Meningkatkan kinerja kueri analisis yang dimulai secara manual dalam klaster penyediaan yang diubah ukurannya elastis dan grup kerja tanpa server.
- Meningkatkan kinerja kueri WLM auto dengan prediksi sumber daya yang lebih baik dalam manajemen beban kerja.

- Menghapus fungsionalitas peluncuran cluster ke VPC penyewaan khusus. Perubahan ini tidak memengaruhi penyewaan instans EC2 apa pun di VPC. Anda dapat memodifikasi penyewaan VPC Anda ke default dengan `modify-vpc-tenancy` AWS CLI perintah.
- Penyegaran manual tampilan terwujud sekarang didukung pada kluster penskalaan konkurensi yang disediakan dan komputasi penskalaan otomatis tanpa server.
- Menambahkan dukungan untuk literal INTERVAL ke fungsi EXTRACT. Misalnya, `EXTRACT('hours' from Interval '50 hours')` pengembalian 2 karena 50 jam ditafsirkan sebagai 2 hari dan 2 jam, dan komponen jam 2 diekstraksi.

Patch Pergeseran Merah Amazon 178

Versi cluster di tambalan ini:

- 1.0.63327 - Versi trek saat ini - Dirilis pada 9 Februari 2024
- 1.0.63313 - Versi trailing track - Dirilis pada 9 Februari 2024
- 1.0.60977 - Versi trailing track - Dirilis pada 15 Desember 2023
- 1.0.59596 - Versi trek saat ini - Dirilis pada 9 November 2023
- 1.0.58593 - Amazon Redshift Versi Tanpa Server - Dirilis pada 23 Oktober 2023
- 1.0.58558 - Versi trek saat ini - Dirilis pada 23 Oktober 2023
- 1.0.57864 - Versi trek saat ini - Dirilis pada 12 Oktober 2023
- 1.0.57850 - Amazon Redshift Versi Tanpa Server - Dirilis pada 12 Oktober 2023
- 1.0.56952 - Versi trek saat ini - Dirilis pada 25 September 2023
- 1.0.56970 - Amazon Redshift Versi Tanpa Server - Dirilis pada 25 September 2023

Fitur dan peningkatan baru di tambalan ini

- Amazon Redshift sekarang telah meningkatkan kinerja kueri berbagi data dengan mempercepat penyegaran metadata pada instance konsumen sementara perubahan data bersamaan terjadi pada instance produsen.
- Menambahkan dukungan untuk penyegaran otomatis dan inkremental tampilan terwujud di instans konsumen berbagi data Amazon Redshift saat tabel dasar tampilan terwujud merujuk ke data bersama.

- Menambahkan dukungan untuk menyimpan objek besar hingga 16 MB dalam tipe data SUPER. Saat menelan dari file sumber JSON, PARQUET, TEXT, dan CSV, Anda dapat memuat data atau dokumen semi-terstruktur sebagai nilai dalam tipe data SUPER, hingga 16 MB.
- Menambahkan dukungan untuk pengubahan ukuran elastis untuk penskalaan ke dan dari cluster Amazon Redshift RA3 simpul tunggal.
- Cluster Amazon Redshift RA3 node tunggal sekarang dapat memperoleh manfaat dari peningkatan enkripsi, mengurangi waktu enkripsi secara keseluruhan dan meningkatkan ketersediaan gudang data selama proses enkripsi.
- Meningkatkan dukungan untuk kueri saat membuka sarang dan melepaskan data yang disimpan dalam tipe data SUPER.
- Meningkatkan kinerja menyegarkan tampilan terwujud dengan tipe data SUPER.
- Menambahkan dukungan untuk menggabungkan literal INTERVAL dengan fungsi ANY_VALUE.
- Streaming ingestion sekarang mendukung perintah SQL baru berikut untuk membersihkan data streaming: `DELETE FROM streaming_materialized_views WHERE <where filter clause>`
- Fungsi DECODE menggantikan nilai tertentu dengan nilai spesifik lain atau nilai default, tergantung pada hasil dari kondisi kesetaraan. DECODE sekarang membutuhkan tiga parameter berikut:
 - ekspresi
 - pencarian
 - result
- Menambahkan fungsionalitas ke prosedur tersimpan untuk memungkinkan penangkapan kesalahan konversi tipe data overflow data, dan penanganan di dalam blok penanganan pengecualian.
- Anda sekarang akan menerima kesalahan saat menanyakan keamanan tingkat baris atau hubungan yang dilindungi masking data dinamis jika Anda mengubah `enable_case_sensitive_identifier` menjadi berbeda dari pengaturan default sesi. Selain itu, konfigurasi berikut akan diblokir ketika kebijakan keamanan tingkat baris atau masking data dinamis diterapkan di klaster yang disediakan atau namespace tanpa server:

```
ALTER USER <current_user> SET case-sensitive identifier.
```
- Perintah MERGE sekarang mendukung sintaks yang disederhanakan yang hanya membutuhkan target dan tabel sumber. Untuk informasi selengkapnya, lihat [MENGGABUNGKAN di Panduan Pengembang Database Amazon Redshift](#).

- Menambahkan dukungan untuk melampirkan kebijakan masking data dinamis yang identik ke beberapa pengguna atau peran dengan prioritas yang sama, atau tanpa menentukan prioritas.
- Anda sekarang dapat menentukan COLLATION saat menambahkan kolom baru melalui ALTER TABLE ADD COLUMN.
- Memperbaiki masalah yang menunda penegakan aturan QMR pada kluster penskalaan konkurensi dan Amazon Redshift Tanpa Server.
- Amazon Redshift Federated Query telah memperluas dukungan pushdown untuk zona waktu dengan stempel waktu di Amazon RDS untuk PostgreSQL dan Amazon Aurora PostgreSQL.
- Anda sekarang dapat menggunakan Amazon RDS untuk MySQL dan Aurora MySQL nama database MySQL dimulai dengan digit dengan kueri federasi.
- Menambahkan tampilan SYS_ANALYZE_HISTORY, yang berisi rincian catatan untuk operasi ANALISIS.
- Menambahkan tampilan SYS_ANALYZE_COMPRESSION_HISTORY, yang berisi detail catatan untuk operasi analisis kompresi selama perintah COPY atau ANALYZE COMPRESSION.
- Menambahkan tampilan SYS_SESSION_HISTORY, yang berisi detail rekaman yang terkait dengan sesi aktif, historis, dan dimulai ulang.
- Menambahkan tampilan SYS_TRANSACTION_HISTORY, yang berisi rincian catatan yang terkait dengan analisis tingkat transaksi yang menyediakan waktu yang dihabiskan untuk komit, jumlah datasha blok yang berkomitmen, dan tingkat isolasi.
- Menambahkan tampilan SVV_REDSHIFT_SCHEMA_QUOTA, yang berisi catatan yang terkait dengan kuota dan penggunaan disk saat ini untuk setiap skema dalam database.
- Menambahkan tampilan SYS_PROCEDURE_CALL, yang berisi catatan yang terkait dengan panggilan prosedur tersimpan, termasuk waktu mulai, waktu akhir, status panggilan prosedur tersimpan, dan hierarki panggilan untuk panggilan prosedur tersimpan bersarang.
- Menambahkan tampilan SYS_CROSS_REGION_DATASHARING_USAGE, yang berisi catatan yang terkait dengan pelacakan penggunaan berbagi data lintas wilayah.
- Menambahkan tampilan SYS_PROCEDURE_MESSAGES, yang berisi catatan yang terkait dengan informasi pelacakan tentang pesan prosedur tersimpan yang dicatat.
- Menambahkan tampilan SYS_UDF_LOG, yang berisi catatan yang terkait dengan melacak pesan log sistem dari panggilan fungsi, kesalahan, peringatan, atau jejak yang ditentukan pengguna bila berlaku.
- Menambahkan kolom baru IS_RECURSIVE, IS_NESTED, S3LIST_TIME, dan GET_PARTITION_TIME ke SYS_EXTERNAL_QUERY_DETAIL.

- Menambahkan MaxRPU, pengaturan kontrol biaya komputasi baru untuk Redshift Serverless. Dengan MaxRPU, Anda dapat secara opsional menentukan ambang batas komputasi atas untuk mengontrol biaya gudang data pada titik waktu yang berbeda dengan memilih tingkat komputasi maksimum yang dapat diskalakan Redshift Serverless per grup kerja.
- Mengoreksi output dari INTERVAL literal dengan string interval numerik. Misalnya, interval yang menentukan sebagai INTERVAL '1' YEAR sekarang kembali 1 YEAR bukan. "00:00:00 Selain itu, output dari literal INTERVAL terpotong ke komponen INTERVAL terkecil yang ditentukan. Misalnya, INTERVAL '1 day 1 hour 1 minute 1.123 seconds' HOUR TO MINUTE terpotong menjadi. 1 day 01:01:00

Patch Pergeseran Merah Amazon 177

Versi cluster di tambalan ini:

- 1.0.57922 - Versi trailing track - Dirilis pada 12 Oktober 2023
- 1.0.57799 - Amazon Redshift Versi Tanpa Server - Dirilis pada 10 Oktober 2023
- 1.0.57798 - Versi trek saat ini - Dirilis pada 10 Oktober 2023
- 1.0.57085 - Versi trailing track - Dirilis pada 26 September 2023
- 1.0.56899 - Amazon Redshift Versi Tanpa Server - Dirilis pada 21 September 2023
- 1.0.56754 - Versi trek saat ini - Dirilis pada 21 September 2023
- 1.0.56242 - Versi trek saat ini - Dirilis pada 11 September 2023
- 1.0.55539 - Amazon Redshift Versi Tanpa Server - Dirilis pada 28 Agustus 2023
- 1.0.55524 - Versi trek saat ini - Dirilis pada 28 Agustus 2023
- 1.0.54899 - Versi trek saat ini - Dirilis pada 15 Agustus 2023
- 1.0.54899 - Versi trek saat ini - Dirilis pada 14 Agustus 2023
- 1.0.54899 - Versi trek saat ini - Dirilis pada 15 Agustus 2023
- 1.0.54239 - Versi trek saat ini - Dirilis pada 3 Agustus 2023
- 1.0.54321 - Amazon Redshift Versi Tanpa Server - Dirilis pada 3 Agustus 2023

Fitur dan peningkatan baru di tambalan ini

- Menambahkan tampilan `SYS_MV_STATE`, yang berisi baris untuk setiap transisi status dari tampilan terwujud. `SYS_MV_STATE` dapat digunakan untuk pemantauan penyegaran MV untuk instans yang disediakan Amazon Redshift Serverless dan Amazon Redshift.
- Menambahkan tampilan `SYS_USERLOG`, yang mencatat detail untuk perubahan pada pengguna database untuk Buat pengguna, Jatuhkan pengguna, Ubah pengguna (ganti nama), Ubah pengguna (ubah properti).
- Menambahkan tampilan `SYS_COPY_REPLACEMENTS`, yang menampilkan log yang mencatat ketika karakter UTF-8 yang tidak valid digantikan oleh perintah `COPY` dengan opsi `ACCEPTINVCHARS`.
- Menambahkan tampilan `SYS_SPATIAL_SIMPLIFY`, yang berisi informasi tentang objek geometri spasial yang disederhanakan menggunakan perintah `COPY`.
- Menambahkan tampilan `SYS_VACUUM_HISTORY`, yang dapat Anda gunakan untuk melihat detail dan hasil operasi `VACUUM`.
- Menambahkan tampilan `SYS_SCHEMA_QUOTA_VIOLATIONS` untuk merekam kejadian, stempel waktu, `XID`, dan informasi berguna lainnya saat kuota skema terlampaui.
- Menambahkan tampilan `SYS_RESTORE_STATE`, yang dapat Anda gunakan memantau kemajuan redistribusi setiap tabel di cluster selama pengubahan ukuran klasik asinkron.
- Menambahkan tampilan `SYS_EXTERNAL_QUERY_ERROR` yang mengembalikan informasi tentang kesalahan pemindaian Redshift Spectrum.
- Menambahkan parameter tag ke perintah `CREATE MODEL`, sehingga Anda sekarang dapat melacak biaya pelatihan dengan pekerjaan pelatihan autopilot.
- Menambahkan nama domain khusus (`CNAME`) untuk kluster Amazon Redshift.
- Menambahkan dukungan pratinjau untuk Apache Iceberg, memungkinkan pelanggan menjalankan kueri analitik pada tabel Apache Iceberg dalam Amazon Redshift.
- Menambahkan dukungan untuk menggunakan peran pengguna dengan grup parameter dalam manajemen beban kerja (`WLM`).
- Menambahkan dukungan untuk pemasangan otomatis AWS Glue Data Catalog, sehingga memudahkan pelanggan untuk menjalankan kueri di danau data mereka.
- Menambahkan fungsionalitas sedemikian rupa sehingga menggunakan fungsi pengelompokan tanpa klausa `GROUP BY` atau menggunakan operasi pengelompokan dalam klausa `WHERE` menghasilkan kesalahan.

- Menambahkan fungsionalitas ke prosedur tersimpan untuk memungkinkan penangkapan pembagian dengan nol kesalahan dan penanganan di dalam blok penanganan pengecualian.
- Memperbaiki bug yang mencegah kueri menggunakan penskalaan konkurensi untuk menulis data ke tabel saat tabel sumber adalah tabel berbagi data.
- Memperbaiki identifier case-sensitive yang didokumentasikan di `enable_case_sensitive_identifier` untuk sekarang bekerja dengan pernyataan MERGE.
- Memperbaiki bug yang kueri pada fungsi `pg_get_late_binding_view_cols ()` mungkin diabaikan sesekali. Anda sekarang selalu dapat membatalkan pertanyaan tersebut.
- Meningkatkan kinerja untuk kueri berbagi data yang berjalan pada konsumen saat menjalankan pekerjaan vakum pada produsen.
- Meningkatkan kinerja untuk berbagi data dan kueri penskalaan konkurensi, terutama dengan perubahan data bersamaan pada produsen atau saat pembongkaran ke instance penskalaan konkurensi yang dilampirkan ke konsumen.

Patch Pergeseran Merah Amazon 176

Versi cluster di tambalan ini:

- 1.0.56738 - Versi trailing track - dirilis pada 21 September 2023
- 1.0.55837 - Versi trailing track - dirilis pada 11 September 2023
- 1.0.54776 - Versi trek saat ini - dirilis pada 15 Agustus 2023
- 1.0.54052 - Versi trek saat ini - Dirilis pada 26 Juli 2023
- 1.0.53642 - Amazon Redshift Versi Tanpa Server - Dirilis pada 20 Juli 2023
- 1.0.53301 - Versi trek saat ini - Dirilis pada 20 Juli 2023
- 1.0.52943 - Amazon Redshift Versi Tanpa Server - Dirilis pada 7 Juli 2023
- 1.0.52931 - Versi trek saat ini - Dirilis pada 7 Juli 2023
- 1.0.52194 - Amazon Redshift Versi Tanpa Server - Dirilis pada 21 Juni 2023
- 1.0.51986 - Versi trek saat ini - Dirilis pada 16 Juni 2023
- 1.0.51594 - Versi trek saat ini - Dirilis pada 9 Juni 2023

Fitur dan peningkatan baru di tambalan ini

- Peningkatan penanganan kesalahan saat menulis GROUP BY () untuk kumpulan pengelompokan kosong. Ini diabaikan sebelumnya dan sekarang mengembalikan kesalahan parser.
- Peningkatan kinerja untuk menyegarkan tampilan terwujud secara bertahap dengan kolom SUPER.
- ALTER TABLE <target_tbl>APPEND FROM <streaming_mv>— (ATA) Perintah SQL sekarang mendukung pemindahan semua catatan dari streaming materialized view (MV) sebagai sumber, selain tabel sebagai sumber, ke tabel target. Dukungan untuk ATA pada streaming MV memungkinkan pengguna untuk dengan cepat membersihkan semua catatan dalam MV streaming dengan memindahkannya ke tabel lain untuk mengelola pertumbuhan data.
- TRUNCATE <streaming_mv>— Perintah SQL sekarang mendukung pemotongan semua catatan dalam tampilan terwujud streaming (MV), selain tabel. TRUNCATE menghapus semua catatan di MV streaming, sambil membiarkan struktur MV streaming tetap utuh. Menjalankan TRUNCATE pada streaming MV memungkinkan pelanggan untuk dengan cepat membersihkan semua catatan dalam streaming MV untuk mengelola pertumbuhan data.
- Menambahkan fungsionalitas untuk klausa QUALIFY ke perintah SELECT.
- Dukungan pembelajaran mesin Redshift untuk peramalan deret waktu dengan mengintegrasikan dengan Amazon Forecast.
- AWS Glue Data Catalog pemasangan otomatis didukung untuk menyederhanakan kueri data lake tanpa langkah tambahan untuk membuat referensi skema eksternal.
- Mengubah kebijakan RLS sekarang didukung. Lihat dokumentasi untuk detail selengkapnya di [KEBIJAKAN ALTER RLS](#).
- Lambda UDF sekarang mendukung parameter volatilitas fungsi STABLE dalam pernyataan CREATE FUNCTION. Ketika parameter STABLE digunakan dalam pernyataan CREATE FUNCTION dan Lambda UDF dipanggil beberapa kali, dengan argumen yang sama, jumlah yang diharapkan dari pemanggilan fungsi Lambda UDF berkurang. Kategori volatilitas fungsi STABLE dijelaskan secara lebih rinci dalam [parameter CREATE FUNCTION](#).
- Beberapa peningkatan kinerja Lambda UDF. Secara khusus, peningkatan dukungan batch rekaman saat menanyakan tabel yang dilindungi oleh kebijakan keamanan tingkat baris (RLS).
- Pengurangan waktu enkripsi keseluruhan untuk cluster Amazon Redshift RA3 dan peningkatan ketersediaan gudang data selama enkripsi. Untuk informasi selengkapnya, lihat [Enkripsi basis data Amazon Redshift](#).
- Tampilan sistem baru SYS_MV_REFRESH_HISTORY telah ditambahkan ke Redshift. Tampilan SYS_MV_REFRESH_HISTORY berisi baris untuk aktivitas penyegaran tampilan terwujud.

Menggunakan SYS_MV_REFRESH_HISTORY, Anda dapat memeriksa riwayat penyegaran tampilan terwujud. SYS_MV_REFRESH_HISTORY dapat dilihat oleh semua pengguna. Pengguna super dapat melihat semua baris; pengguna biasa hanya dapat melihat data mereka sendiri.

Sebuah kolom baru SPILLED_BLOCK_LOCAL_DISK telah ditambahkan ke tampilan sistem SYS_QUERY_DETAIL. Kolom baru SPILLED_BLOCK_LOCAL_DISK membantu pelanggan untuk menentukan blok tumpah ke disk lokal. Anda dapat menggunakan SYS_QUERY_DETAIL untuk melihat detail kueri pada tingkat langkah. SYS_QUERY_DETAIL terlihat oleh semua pengguna. Pengguna super dapat melihat semua baris; pengguna biasa hanya dapat melihat metadata yang dapat mereka akses.

- Tampilan sistem baru, SYS_QUERY_TEXT, telah ditambahkan ke Amazon Redshift Tanpa Server dan Amazon Redshift yang disediakan. [Tampilan SYS_QUERY_TEXT mirip dengan SVL_STATEMENTTEXT untuk cluster yang disediakan.](#) Gunakan sequence kolom dalam tampilan SYS_QUERY_TEXT untuk mendapatkan teks pernyataan SQL lengkap.

Patch Pergeseran Merah Amazon 175

Versi cluster di tambalan ini:

- 1.0.53064 - Versi trek saat ini - Dirilis pada 7 Juli 2023
- 1.0.51973 - Versi trek saat ini - Dirilis pada 16 Juni 2023
- 1.0.51781 - Versi trek saat ini - Dirilis pada 10 Juni 2023
- 1.0.51314 - Amazon Redshift Versi Tanpa Server - Dirilis pada 3 Juni 2023
- 1.0.51304 - Versi trek saat ini - Dirilis pada 2 Juni 2023
- 1.0.50708 - Versi Track saat ini - Dirilis pada 19 Mei 2023
- 1.0.50300 - Versi trek saat ini - Dirilis pada 8 Mei 2023
- 1.0.49710 - Amazon Redshift Versi Tanpa Server - Dirilis pada 28 April 2023
- 1.0.49676 - Versi trek saat ini - Dirilis pada 28 April 2023

Fitur dan peningkatan baru di tambalan ini

- Perbaiki bug minor.
- Penyerapan streaming Amazon Redshift sekarang mendukung konsumsi streaming lintas wilayah di mana topik sumber Anda (Amazon Kinesis Data Streams KDS) atau Amazon Managed

Streaming for Apache Kafka (MSK) dapat ditemukan di wilayah yang AWS berbeda dari wilayah tempat gudang data Amazon Redshift Anda berada. AWS Dokumentasi di [Memulai dengan konsumsi streaming dari Amazon Kinesis Data Streams](#) telah direvisi dan menjelaskan bagaimana kata kunci REGION digunakan.

- Penyesuaian musim panas Mesir.
- Peningkatan waktu keseluruhan untuk enkripsi cluster RA3.

Patch Pergeseran Merah Amazon 174

1.0.51296 - Dirilis pada 2 Juni 2023

Lepaskan ke trailing track. Tidak ada catatan rilis.

1.0.50468 - Dirilis pada 12 Mei 2023

Rilis pemeliharaan. Tidak ada catatan rilis.

1.0.49780, 1.0.49868, dan 1.0.49997 - Dirilis pada 28 April 2023

Catatan rilis untuk versi ini:

- Peningkatan dukungan batching untuk Lambda UDF.
- Batching tambahan untuk Lambda UDF.
- Perintah MERGE SQL baru untuk menerapkan perubahan data sumber ke tabel Amazon Redshift.
- Kemampuan masking data dinamis baru untuk menyederhanakan proses perlindungan data sensitif di gudang data Amazon Redshift.
- Kontrol akses terpusat baru untuk berbagi data dengan Lake Formation yang memungkinkan mengelola hibah izin, melihat kontrol akses, dan mengaudit izin pada tabel dan tampilan di database Amazon Redshift menggunakan Lake Formation API dan Konsol. AWS
- Penyesuaian musim panas Mesir.

1.0.49087 - Dirilis pada 12 April 2023

Rilis pemeliharaan. Tidak ada catatan rilis.

1.0.48805 - Dirilis pada 5 April 2023

Catatan rilis untuk versi ini:

- Amazon Redshift memperkenalkan peningkatan kinerja tambahan untuk kueri string-heavy menggunakan BYTEDICT, pengkodean kompresi baru di Amazon Redshift yang mempercepat pemrosesan data berbasis string antara 5x hingga 63x dibandingkan dengan pengkodean kompresi alternatif seperti LZO atau ZSTD. Untuk informasi selengkapnya tentang fitur ini, lihat [Pengkodean Byte-dictionary](#) di Panduan Pengembang Database Amazon Redshift.

1.0.48004 - Dirilis pada 17 Maret 2023

Rilis pemeliharaan. Tidak ada catatan rilis.

1.0.47470 - Dirilis pada 11 Maret 2023

Catatan rilis untuk versi ini:

- Meningkatkan kinerja kueri `padapg_catalog.svv_table_info`. Juga menambahkan kolom baru `create_time`. Saat membuat tabel, kolom ini menyimpan stempel tanggal/waktu di UTC.
- Menambahkan dukungan untuk menentukan batas waktu tingkat sesi pada kueri federasi.

Patch Pergeseran Merah Amazon 173

1.0.49788 - Dirilis pada 28 April 2023

Catatan rilis untuk versi ini:

- Penyesuaian musim panas Mesir.

1.0.49074 - Dirilis pada 12 April 2023

Catatan rilis untuk versi ini:

- Konfigurasi zona waktu diperbarui ke rilis perpustakaan IANA 2022g.

1.0.48766 - Dirilis pada 5 April 2023

Rilis pemeliharaan. Tidak ada catatan rilis.

1.0.48714 - Dirilis pada 5 April 2023

Rilis pemeliharaan. Tidak ada catatan rilis.

1.0.48022 - Dirilis pada 17 Maret 2023

Rilis pemeliharaan. Tidak ada catatan rilis.

1.0.47357 - Dirilis pada 7 Maret 2023

Rilis pemeliharaan. Tidak ada catatan rilis.

1.0.46987 - Dirilis pada 24 Februari 2023

Rilis pemeliharaan. Tidak ada catatan rilis.

1.0.46806 - Dirilis pada 18 Februari 2023

Rilis pemeliharaan. Tidak ada catatan rilis.

1.0.46607 - Dirilis pada 13 Februari 2023

Catatan rilis untuk versi ini:

- Kami sekarang secara otomatis mengonversi tabel dengan secara manual mengatur kunci sortir interleaved ke kunci sortir majemuk jika gaya distribusinya telah disetel ke `DISTSTYLE KEY`, untuk meningkatkan kinerja tabel ini. Ini dilakukan pada saat memulihkan snapshot ke Amazon Redshift Serverless.

1.0.45698 - Dirilis pada 20 Januari 2023

Catatan rilis untuk versi ini:

- Menambahkan parameter ekstensi file ke perintah `UNLOAD`, sehingga ekstensi file secara otomatis ditambahkan ke nama file.

- Mendukung perlindungan objek yang dilindungi RLS secara default saat menambahkannya ke datashare atau jika mereka sudah menjadi bagian dari datashare. Administrator sekarang dapat mematikan RLS untuk datashares untuk memungkinkan konsumen mengakses objek yang dilindungi.
- Menambahkan tabel sistem baru untuk pemantauan:SVV_ML_MODEL_INFO,SVV_MV_DEPENDENCY, danSYS_LOAD_DETAIL. Juga menambahkan kolom data_skewness dan time_skewness ke tabel sistemSYS_QUERY_DETAIL.

Patch Pergeseran Merah Amazon 172

Versi cluster di tambalan ini:

- 1.0.46534 - Dirilis pada 18 Februari 2023
- 1.0.46523 - Dirilis pada 13 Februari 2023
- 1.0.46206 - Dirilis pada 1 Februari 2023
- 1.0.45603 - Dirilis pada 20 Januari 2023
- 1.0.44924 — Dirilis pada 19 Desember 2022
- 1.0.44903 — Dirilis pada 18 Desember 2022
- 1.0.44540 — Dirilis pada 13 Desember 2022
- 1.0.44126 — Dirilis pada 23 November 2022
- 1.0.43980 — Dirilis pada 17 November 2022

Fitur dan peningkatan baru di tambalan ini

- Tabel yang dibuat oleh CTAS adalah AUTO secara default.
- Menambahkan dukungan untuk keamanan tingkat baris (RLS) pada tampilan terwujud.
- Meningkatkan batas waktu S3 untuk meningkatkan berbagi data lintas wilayah.
- Menambahkan fungsi spasial baruST_GeomFromGeohash.
- Meningkatkan pemilihan otomatis kunci distribusi dari kunci primer komposit untuk meningkatkan out-of-the-box kinerja.
- Menambahkan kunci primer otomatis ke kunci distribusi untuk tabel dengan kunci primer komposit, meningkatkan out-of-the-box kinerja.

- Meningkatkan penskalaan konkurensi untuk memungkinkan lebih banyak kueri untuk diskalakan bahkan saat data berubah.
- Meningkatkan kinerja kueri berbagi data.
- Menambahkan metrik probabilitas Machine Learning untuk model klasifikasi.
- Menambahkan tabel sistem baru untuk pemantauan:SVV_USER_INFO,SVV_MV_INFO,SYS_CONNECTION_LOG,SYS_DATASHARE_USAGE_PRODUCED danSYS_DATASHARE_CHANGE_LOG.
- Menambahkan dukungan untuk menanyakan kolom VARBYTE di tabel eksternal untuk jenis file Parquet dan ORC.

Patch Pergeseran Merah Amazon 171

Versi cluster di tambalan ini:

- 1.0.43931 — Dirilis pada 16 November 2022
- 1.0.43551 — Dirilis pada 5 November 2022
- 1.0.43331 — Dirilis pada 29 September 2022
- 1.0.43029 — Dirilis pada 26 September 2022

Fitur dan peningkatan baru di tambalan ini

- Dukungan CONNECT BY: Menambahkan dukungan untuk konstruksi CONNECT BY SQL, memungkinkan Anda secara rekursif menanyakan data hierarkis di gudang data Anda berdasarkan hubungan induk-anak dalam kumpulan data tersebut.

Patch Pergeseran Merah Amazon 170

Versi cluster di tambalan ini:

- 1.0.43922 — Dirilis pada 21 November 2022
- 1.0.43573 — Dirilis pada 7 November 2022
- 1.0.41881 — Dirilis pada 20 September 2022
- 1.0.41465 — Dirilis pada 7 September 2022
- 1.0.40325 — Dirilis pada 27 Juli 2022

Fitur dan peningkatan baru di tambalan ini

- ST_GeomfromGeo JSON: Membangun objek geometri spasial Amazon Redshift dari VARCHAR dalam representasi GeoJSON.

Patch Pergeseran Merah Amazon 169

Versi cluster di tambalan ini:

- 1.0.41050 — Dirilis pada 7 September 2022
- 1.0.40083 — Dirilis pada 16 Juli 2022
- 1.0.39734 — Dirilis pada 7 Juli 2022
- 1.0.39380 — Dirilis pada 23 Juni 2022
- 1.0.39251 — Dirilis pada 15 Juni 2022
- 1.0.39009 — Dirilis pada 8 Juni 2022

Fitur dan peningkatan baru di tambalan ini

- Menambahkan peran sebagai parameter untuk perintah Alter Default Privileges untuk mendukung Kontrol Akses berbasis peran.
- Menambahkan parameter ACCEPTINVCHARS untuk mendukung penggantian karakter UTF-8 yang tidak valid saat menyalin dari file Parquet dan ORC.
- Menambahkan fungsi OBJECT (k, v) untuk membangun objek SUPER dari pasangan kunci dan nilai.

Patch Pergeseran Merah Amazon 168

Versi cluster di tambalan ini:

- 1.0.38698 — Dirilis pada 25 Mei 2022
- 1.0.38551 — Dirilis pada 20 Mei 2022
- 1.0.38463 — Dirilis pada 18 Mei 2022
- 1.0.38361 — Dirilis pada 13 Mei 2022
- 1.0.38199 — Dirilis pada 9 Mei 2022

- 1.0.38112 — Dirilis pada 6 Mei 2022
- 1.0.37684 — Dirilis pada 20 April 2022

Fitur dan peningkatan baru di tambalan ini

- Menambahkan dukungan untuk tipe model Linear Learner di Amazon Redshift ML.
- Menambahkan opsi SNAPSHOT untuk tingkat isolasi transaksi SQL.
- Menambahkan `farmhashFingerprint64` sebagai algoritma hashing baru untuk VARBYTE dan VARCHAR data.
- Mendukung fungsi AVG dalam penyegaran inkremental tampilan terwujud.
- Mendukung sub-kueri berkorelasi pada tabel eksternal di Redshift Spectrum.
- Untuk meningkatkan kinerja out-of-the-box kueri, Amazon Redshift secara otomatis memilih kunci utama kolom tunggal untuk tabel tertentu sebagai kunci distribusi.

Contoh kode untuk Amazon Redshift menggunakan SDK AWS

Contoh kode berikut menunjukkan cara menggunakan Amazon Redshift dengan AWS perangkat pengembangan perangkat lunak (SDK).

Tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Meskipun tindakan menunjukkan cara memanggil fungsi layanan individual, Anda dapat melihat tindakan dalam konteks pada skenario terkait dan contoh lintas layanan.

Skenario adalah contoh kode yang menunjukkan cara menyelesaikan tugas tertentu dengan memanggil beberapa fungsi dalam layanan yang sama.

Contoh lintas layanan adalah contoh aplikasi yang bekerja di beberapa Layanan AWS.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Memulai

Halo Amazon Redshift

Contoh kode berikut menunjukkan cara memulai menggunakan Amazon Redshift.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```
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()));
    }
}
```

- Untuk detail API, lihat [DescribeClusters](#) di AWS SDK for Java 2.x Referensi API.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```
import boto3

def hello_redshift(redshift_client):
    """
    Use the AWS SDK for Python (Boto3) to create an Amazon Redshift client and
    list
    the clusters in your account. This list might be empty if you haven't created
    any clusters.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param redshift_client: A Boto3 Redshift Client object.
    """
    print("Hello, Redshift! Let's list your clusters:")
    paginator = redshift_client.get_paginator("describe_clusters")
    clusters = []
    for page in paginator.paginate():
        clusters.extend(page["Clusters"])

    print(f"{len(clusters)} cluster(s) were found.")

    for cluster in clusters:
        print(f" {cluster['ClusterIdentifier']}")

if __name__ == "__main__":
    hello_redshift(boto3.client("redshift"))
```

- Untuk detail API, lihat [DescribeClusters](#) in AWS SDK for Python (Boto3) Referensi API.

Contoh kode

- [Tindakan untuk Amazon Redshift menggunakan SDK AWS](#)
 - [Gunakan CreateCluster dengan AWS SDK atau CLI](#)
 - [Gunakan CreateTable dengan AWS SDK atau CLI](#)
 - [Gunakan DeleteCluster dengan AWS SDK atau CLI](#)
 - [Gunakan DescribeClusters dengan AWS SDK atau CLI](#)
 - [Gunakan DescribeStatement dengan AWS SDK atau CLI](#)

- [Gunakan GetStatementResult dengan AWS SDK atau CLI](#)
- [Gunakan Insert dengan AWS SDK atau CLI](#)
- [Gunakan ModifyCluster dengan AWS SDK atau CLI](#)
- [Gunakan Query dengan AWS SDK atau CLI](#)
- [Skenario untuk Amazon Redshift menggunakan SDK AWS](#)
 - [Memulai tabel, item, dan kueri Amazon Redshift](#)
- [Contoh lintas layanan untuk Amazon AWS Redshift menggunakan SDK](#)
 - [Buat pelacak item Amazon Redshift](#)

Tindakan untuk Amazon Redshift menggunakan SDK AWS

Contoh kode berikut menunjukkan cara melakukan tindakan Amazon Redshift individual dengan AWS SDK. Kutipan ini menyebut Amazon Redshift API dan merupakan kutipan kode dari program yang lebih besar yang harus dijalankan dalam konteks. Setiap contoh menyertakan tautan ke GitHub, di mana Anda dapat menemukan instruksi untuk mengatur dan menjalankan kode.

Contoh berikut hanya mencakup tindakan yang paling umum digunakan. Untuk daftar lengkapnya, lihat Referensi [API Amazon Redshift](#).

Contoh

- [Gunakan CreateCluster dengan AWS SDK atau CLI](#)
- [Gunakan CreateTable dengan AWS SDK atau CLI](#)
- [Gunakan DeleteCluster dengan AWS SDK atau CLI](#)
- [Gunakan DescribeClusters dengan AWS SDK atau CLI](#)
- [Gunakan DescribeStatement dengan AWS SDK atau CLI](#)
- [Gunakan GetStatementResult dengan AWS SDK atau CLI](#)
- [Gunakan Insert dengan AWS SDK atau CLI](#)
- [Gunakan ModifyCluster dengan AWS SDK atau CLI](#)
- [Gunakan Query dengan AWS SDK atau CLI](#)

Gunakan **CreateCluster** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `CreateCluster`.

CLI

AWS CLI

Buat Cluster dengan ParametersThis contoh Minimal membuat cluster dengan set minimal parameter. Secara default, output dalam format JSON.Command:

```
aws redshift create-cluster --node-type dw.hs1.xlarge --number-of-nodes 2 --
master-username adminuser --master-user-password TopSecret1 --cluster-identifier
mycluster
```

Hasil:

```
{
  "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"
```

```
}  
}
```

- Untuk detail API, lihat [CreateCluster](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Buat 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);  
    }  
}
```

- Untuk detail API, lihat [CreateCluster](#) di Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Buat klien.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Buat 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();

```

- Untuk detail API, lihat [CreateCluster](#) di Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Buat 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}")
    }
}

```

- Untuk detail API, lihat [CreateCluster](#) di AWS SDK untuk referensi API Kotlin.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```

class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client

    def create_cluster(
        self,
        cluster_identifier,

```

```

node_type,
master_username,
master_user_password,
publicly_accessible,
number_of_nodes,
):
    """
    Creates a cluster.

    :param cluster_identifier: The name of the cluster.
    :param node_type: The type of node in the cluster.
    :param master_username: The master username.
    :param master_user_password: The master user password.
    :param publicly_accessible: Whether the cluster is publicly accessible.
    :param number_of_nodes: The number of nodes in the cluster.
    :return: The cluster.
    """

    try:
        cluster = self.client.create_cluster(
            ClusterIdentifier=cluster_identifier,
            NodeType=node_type,
            MasterUsername=master_username,
            MasterUserPassword=master_user_password,
            PubliclyAccessible=publicly_accessible,
            NumberOfNodes=number_of_nodes,
        )
        return cluster
    except ClientError as err:
        logging.error(
            "Couldn't create a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

```

Kode berikut membuat instance objek. RedshiftWrapper

```

client = boto3.client("redshift")
redhifft_wrapper = RedshiftWrapper(client)

```

- Untuk detail API, lihat [CreateCluster](#) di AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **CreateTable** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `CreateTable`.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```
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);
    }
}
```



```
}

```

- Untuk detail API, lihat [CreateTable](#) di Referensi AWS SDK for Java 2.x API.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```
def create_table(self, cluster_id, database, username):
    self.redshift_data_wrapper.execute_statement(
        cluster_idenfier=cluster_id,
        database_name=database,
        user_name=username,
        sql="CREATE TABLE Movies (statement_id INT PRIMARY KEY, title
VARCHAR(100), year INT)",
    )

    print("Table created: Movies")

```

Pemanggilan ExecuteStatement objek pembungkus.

```
class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client

    def execute_statement(

```

```
        self, cluster_identifier, database_name, user_name, sql,
parameter_list=None
    ):
        """
        Executes a SQL statement.

        :param cluster_identifier: The cluster identifier.
        :param database_name: The database name.
        :param user_name: The user's name.
        :param sql: The SQL statement.
        :param parameter_list: The optional SQL statement parameters.
        :return: The SQL statement result.
        """

        try:
            kwargs = {
                "ClusterIdentifier": cluster_identifier,
                "Database": database_name,
                "DbUser": user_name,
                "Sql": sql,
            }
            if parameter_list:
                kwargs["Parameters"] = parameter_list
            response = self.client.execute_statement(**kwargs)
            return response
        except ClientError as err:
            logging.error(
                "Couldn't execute statement. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Kode berikut membuat instance objek. `RedshiftDataWrapper`

```
client = boto3.client("redshift-data")
redshift_data_wrapper = RedshiftDataWrapper(client)
```

- Untuk detail API, lihat [CreateTable](#) di AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **DeleteCluster** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `DeleteCluster`.

CLI

AWS CLI

Hapus Cluster tanpa Snapshot. Ini contoh Final Cluster menghapus cluster, memaksa penghapusan data sehingga tidak ada snapshot cluster akhir yang dibuat. Command:

```
aws redshift delete-cluster --cluster-identifier mycluster --skip-final-cluster-snapshot
```

Menghapus Cluster, Mengizinkan Snapshot. Ini contoh Final Cluster menghapus klaster, tetapi menentukan snapshot. Command cluster akhir:

```
aws redshift delete-cluster --cluster-identifier mycluster --final-cluster-snapshot-identifier myfinalsnapshot
```

- Untuk detail API, lihat [DeleteCluster](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Hapus klaster .

```
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);
    }
}
```

- Untuk detail API, lihat [DeleteCluster](#) di Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Buat klien.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Buat 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();
```

- Untuk detail API, lihat [DeleteCluster](#) di Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Hapus klaster .

```
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}")
    }
}

```

- Untuk detail API, lihat [DeleteCluster](#) di AWS SDK untuk referensi API Kotlin.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```

class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client

    def delete_cluster(self, cluster_identifier):
        """
        Deletes a cluster.

        :param cluster_identifier: The cluster identifier.
        """
        try:
            self.client.delete_cluster(

```

```
        ClusterIdentifier=cluster_identifier,  
        SkipFinalClusterSnapshot=True  
    )  
    except ClientError as err:  
        logging.error(  
            "Couldn't delete a cluster. Here's why: %s: %s",  
            err.response["Error"]["Code"],  
            err.response["Error"]["Message"],  
        )  
        raise
```

Kode berikut membuat instance objek. `RedshiftWrapper`

```
client = boto3.client("redshift")  
redshift_wrapper = RedshiftWrapper(client)
```

- Untuk detail API, lihat [DeleteCluster](#) di AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **DescribeClusters** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `DescribeClusters`.

CLI

AWS CLI

Dapatkan Deskripsi Semua Clusters This contoh mengembalikan deskripsi semua cluster untuk akun. Secara default, output dalam format JSON. Command:

```
aws redshift describe-clusters
```

Hasil:

```
{
```

```

"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"
}
}

```

Anda juga dapat memperoleh informasi yang sama dalam format teks menggunakan `--output text` option.Command:

`--output textOption.command:`

Option.command:


```
aws redshift describe-clusters --output text
```


Hasil:

```
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
```

- Untuk detail API, lihat [DescribeClusters](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Jelaskan 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);
    }
}

```

- Untuk detail API, lihat [DescribeClusters](#) di Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Buat klien.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Jelaskan cluster Anda.

```
// 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();
```

- Untuk detail API, lihat [DescribeClusters](#) di Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Jelaskan 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}")
            }
        }
    }
}
```

- Untuk detail API, lihat [DescribeClusters](#) di AWS SDK untuk referensi API Kotlin.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client

    def describe_clusters(self, cluster_identifier):
        """
        Describes a cluster.

        :param cluster_identifier: The cluster identifier.
        :return: A list of clusters.
        """
        try:
            kwargs = {}
            if cluster_identifier:
                kwargs["ClusterIdentifier"] = cluster_identifier

            paginator = self.client.get_paginator("describe_clusters")
            clusters = []
            for page in paginator.paginate(**kwargs):
                clusters.extend(page["Clusters"])

            return clusters

        except ClientError as err:
            logging.error(
                "Couldn't describe a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Kode berikut membuat instance objek. RedshiftWrapper

```
client = boto3.client("redshift")
redshift_wrapper = RedshiftWrapper(client)
```

- Untuk detail API, lihat [DescribeClusters](#) di AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **DescribeStatement** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `DescribeStatement`.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```
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);
}
}

```

- Untuk detail API, lihat [DescribeStatement](#) di Referensi AWS SDK for Java 2.x API.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```

class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client

    def describe_statement(self, statement_id):
        """

```

```
Describes a SQL statement.

:param statement_id: The SQL statement identifier.
:return: The SQL statement result.
"""
try:
    response = self.client.describe_statement(Id=statement_id)
    return response
except ClientError as err:
    logging.error(
        "Couldn't describe statement. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise
```

Kode berikut membuat instance objek. `RedshiftDataWrapper`

```
client = boto3.client("redshift-data")
redshift_data_wrapper = RedshiftDataWrapper(client)
```

- Untuk detail API, lihat [DescribeStatement](#) di AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan `GetStatementResult` dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetStatementResult`.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Periksa hasil pernyataan.

```
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);
    }
}
```

- Untuk detail API, lihat [GetStatementHasil](#) dalam Referensi AWS SDK for Java 2.x API.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```
class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client

    def get_statement_result(self, statement_id):
        """
        Gets the result of a SQL statement.

        :param statement_id: The SQL statement identifier.
        :return: The SQL statement result.
        """
        try:
            result = {
                "Records": [],
            }
            paginator = self.client.get_paginator("get_statement_result")
            for page in paginator.paginate(Id=statement_id):
                if "ColumnMetadata" not in result:
                    result["ColumnMetadata"] = page["ColumnMetadata"]
                    result["Records"].extend(page["Records"])
            return result
        except ClientError as err:
            logging.error(
                "Couldn't get statement result. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
```

```
)  
raise
```

Kode berikut membuat instance objek. `RedshiftDataWrapper`

```
client = boto3.client("redshift-data")  
redshift_data_wrapper = RedshiftDataWrapper(client)
```

- Untuk detail API, lihat [GetStatementHasil](#) dalam AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **Insert** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `Insert`.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```
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. ");
}
```

- Untuk detail API, lihat [Menyisipkan](#) di Referensi AWS SDK for Java 2.x API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **ModifyCluster** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `ModifyCluster`.

CLI

AWS CLI

Mengaitkan Grup Keamanan dengan ClusterThis contoh menunjukkan cara mengaitkan grup keamanan klaster dengan `Cluster.command` yang ditentukan:

```
aws redshift modify-cluster --cluster-identifier mycluster --cluster-security-groups mysecuritygroup
```

Ubah Jendela Pemeliharaan untuk ClusterThis menunjukkan cara mengubah jendela pemeliharaan pilihan mingguan untuk cluster menjadi jendela minimum empat jam mulai hari Minggu pukul 11:15, dan berakhir Senin pukul 3:15 pagi. Perintah:

```
aws redshift modify-cluster --cluster-identifier mycluster --preferred-maintenance-window Sun:23:15-Mon:03:15
```

Ubah Kata Sandi Master untuk ClusterThis contoh menunjukkan cara mengubah kata sandi master untuk cluster. Command:

```
aws redshift modify-cluster --cluster-identifier mycluster --master-user-password
A1b2c3d4
```

- Untuk detail API, lihat [ModifyCluster](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Memodifikasi 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);
    }
}
```

- Untuk detail API, lihat [ModifyCluster](#) di Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Buat klien.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Memodifikasi 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();
```

- Untuk detail API, lihat [ModifyCluster](#) di Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Memodifikasi 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",
        )
    }
}
```

- Untuk detail API, lihat [ModifyCluster](#) di AWS SDK untuk referensi API Kotlin.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client

    def modify_cluster(self, cluster_identifier, preferred_maintenance_window):
        """
        Modifies a cluster.

        :param cluster_identifier: The cluster identifier.
        :param preferred_maintenance_window: The preferred maintenance window.
        """
        try:
            self.client.modify_cluster(
                ClusterIdentifier=cluster_identifier,
                PreferredMaintenanceWindow=preferred_maintenance_window,
            )
        except ClientError as err:
            logging.error(
                "Couldn't modify a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Kode berikut membuat instance objek. `RedshiftWrapper`

```
client = boto3.client("redshift")
redshift_wrapper = RedshiftWrapper(client)
```

- Untuk detail API, lihat [ModifyCluster](#) di AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **Query** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `Query`.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

Kueri tabel.

```
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 "";
}
```

- Untuk detail API, lihat [Kueri](#) di Referensi API AWS SDK for Java 2.x .

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Skenario untuk Amazon Redshift menggunakan SDK AWS

Contoh kode berikut menunjukkan cara menerapkan skenario umum di Amazon Redshift dengan AWS SDK. Skenario ini menunjukkan cara menyelesaikan tugas tertentu dengan memanggil beberapa fungsi dalam Amazon Redshift. Setiap skenario menyertakan tautan ke GitHub, di mana Anda dapat menemukan petunjuk tentang cara mengatur dan menjalankan kode.

Contoh

- [Memulai tabel, item, dan kueri Amazon Redshift](#)

Memulai tabel, item, dan kueri Amazon Redshift

Contoh kode berikut menunjukkan cara bekerja dengan tabel, item, dan kueri Amazon Redshift.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import com.fasterxml.jackson.core.JsonFactory;
import com.fasterxml.jackson.databind.JsonNode;
import com.fasterxml.jackson.databind.ObjectMapper;
import com.fasterxml.jackson.databind.node.ObjectNode;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.redshift.RedshiftClient;
import software.amazon.awssdk.services.redshift.model.Cluster;
import software.amazon.awssdk.services.redshift.model.CreateClusterRequest;
import software.amazon.awssdk.services.redshift.model.CreateClusterResponse;
import software.amazon.awssdk.services.redshift.model.DeleteClusterRequest;
import software.amazon.awssdk.services.redshift.model.DeleteClusterResponse;
import software.amazon.awssdk.services.redshift.model.DescribeClustersRequest;
import software.amazon.awssdk.services.redshift.model.DescribeClustersResponse;
import software.amazon.awssdk.services.redshift.model.ModifyClusterRequest;
import software.amazon.awssdk.services.redshift.model.ModifyClusterResponse;
import software.amazon.awssdk.services.redshift.model.RedshiftException;
import software.amazon.awssdk.services.redshiftdata.RedshiftDataClient;
import
    software.amazon.awssdk.services.redshiftdata.model.DescribeStatementRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.DescribeStatementResponse;
import
    software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementResponse;
import software.amazon.awssdk.services.redshiftdata.model.Field;
import
    software.amazon.awssdk.services.redshiftdata.model.GetStatementResultRequest;
```

```
import
    software.amazon.awssdk.services.redshiftdata.model.GetStatementResultResponse;
import software.amazon.awssdk.services.redshiftdata.model.ListDatabasesRequest;
import software.amazon.awssdk.services.redshiftdata.model.RedshiftDataException;
import software.amazon.awssdk.services.redshiftdata.model.SqlParameter;
import
    software.amazon.awssdk.services.redshiftdata.paginators.ListDatabasesIterable;
import com.fasterxml.jackson.core.JsonParser;
import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.Iterator;
import java.util.List;
import java.util.Scanner;
import java.util.concurrent.TimeUnit;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
 *
 * This Java example performs these tasks:
 *
 * 1. Prompts the user for a unique cluster ID or use the default value.
 * 2. Creates a Redshift cluster with the specified or default cluster Id value.
 * 3. Waits until the Redshift cluster is available for use.
 * 4. Lists all databases using a pagination API call.
 * 5. Creates a table named "Movies" with fields ID, title, and year.
 * 6. Inserts a specified number of records into the "Movies" table by reading
    the Movies JSON file.
 * 7. Prompts the user for a movie release year.
 * 8. Runs a SQL query to retrieve movies released in the specified year.
 * 9. Modifies the Redshift cluster.
 * 10. Prompts the user for confirmation to delete the Redshift cluster.
 * 11. If confirmed, deletes the specified Redshift cluster.
 */

public class RedshiftScenario {
```

```
public static final String DASHES = new String(new char[80]).replace("\0",
"-");
public static void main(String[] args) throws Exception {
    final String usage = ""

        Usage:
            <jsonFilePath>\s

        Where:
            jsonFilePath - The path to the Movies JSON file (you can locate
that file in ../../../../resources/sample_files/movies.json)
        """;

    if (args.length != 1) {
        System.out.println(usage);
        System.exit(1);
    }

    String jsonFilePath = args[0];
    String userName;
    String userPassword;
    String databaseName = "dev" ;
    Scanner scanner = new Scanner(System.in);

    Region region = Region.US_EAST_1;
    RedshiftClient redshiftClient = RedshiftClient.builder()
        .region(region)
        .build();

    RedshiftDataClient redshiftDataClient = RedshiftDataClient.builder()
        .region(region)
        .build();

    System.out.println(DASHES);
    System.out.println("Welcome to the Amazon Redshift SDK Getting Started
scenario.");
    System.out.println("""
    This Java program demonstrates how to interact with Amazon Redshift by
using the AWS SDK for Java (v2).\s
    Amazon Redshift is a fully managed, petabyte-scale data warehouse service
hosted in the cloud.

    The program's primary functionalities include cluster creation,
verification of cluster readiness,\s
```

list databases, table creation, data population within the table, and execution of SQL statements.

Furthermore, it demonstrates the process of querying data from the Movie table.\s

```
Upon completion of the program, all AWS resources are cleaned up.
""");
```

```
System.out.println("Lets get started...");
System.out.println("Please enter your user name (default is awsuser)");
String user = scanner.nextLine();
userName = user.isEmpty() ? "awsuser" : user;
System.out.println(DASHES);
System.out.println("Please enter your user password (default is
AwsUser1000)");
String userpass = scanner.nextLine();
userPassword = userpass.isEmpty() ? "AwsUser1000" : userpass;
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("A Redshift cluster refers to the collection of
computing resources and storage that work together to process and analyze large
volumes of data.");
System.out.println("Enter a cluster id value (default is redshift-
cluster-movies): ");
String userClusterId = scanner.nextLine();
String clusterId = userClusterId.isEmpty() ? "redshift-cluster-movies" :
userClusterId;
createCluster(redshiftClient, clusterId, userName, userPassword);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Wait until "+clusterId +" is available.");
System.out.print("Press Enter to continue...");
scanner.nextLine();
waitForClusterReady(redshiftClient, clusterId);
System.out.println(DASHES);

System.out.println(DASHES);
String databaseInfo = ""
    When you created $clusteridD, the dev database is created by default
and used in this scenario.\s
```

To create a custom database, you need to have a CREATEDB privilege.\s

```
For more information, see the documentation here: https://docs.aws.amazon.com/redshift/latest/dg/r\_CREATE\_DATABASE.html.
    ""$.replace("${clusteridD}", clusterId);

System.out.println(databaseInfo);
System.out.print("Press Enter to continue...");
scanner.nextLine();
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("List databases in "+clusterId);
System.out.print("Press Enter to continue...");
scanner.nextLine();
listAllDatabases(redshiftDataClient, clusterId, userName, databaseName);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Now you will create a table named Movies.");
System.out.print("Press Enter to continue...");
scanner.nextLine();
createTable(redshiftDataClient, clusterId, databaseName, userName);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Populate the Movies table using the Movies.json
file.");
System.out.println("Specify the number of records you would like to add
to the Movies Table.");
System.out.println("Please enter a value between 50 and 200.");
int numRecords;
do {
    System.out.print("Enter a value: ");
    while (!scanner.hasNextInt()) {
        System.out.println("Invalid input. Please enter a value between
50 and 200.");
        System.out.print("Enter a year: ");
        scanner.next();
    }
    numRecords = scanner.nextInt();
} while (numRecords < 50 || numRecords > 200);
popTable(redshiftDataClient, clusterId, databaseName, userName,
jsonFilePath, numRecords);
System.out.println(DASHES);
```



```
System.out.println(DASHES);
System.out.println("Query the Movies table by year. Enter a value between
2012-2014.");
int movieYear;
do {
    System.out.print("Enter a year: ");
    while (!scanner.hasNextInt()) {
        System.out.println("Invalid input. Please enter a valid year
between 2012 and 2014.");
        System.out.print("Enter a year: ");
        scanner.next();
    }
    movieYear = scanner.nextInt();
    scanner.nextLine();
} while (movieYear < 2012 || movieYear > 2014);

String id = queryMoviesByYear(redshiftDataClient, databaseName, userName,
movieYear, clusterId);
System.out.println("The identifier of the statement is " + id);
checkStatement(redshiftDataClient, id);
getResults(redshiftDataClient, id);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Now you will modify the Redshift cluster.");
System.out.print("Press Enter to continue...");
scanner.nextLine();
modifyCluster(redshiftClient, clusterId);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Would you like to delete the Amazon Redshift cluster?
(y/n)");
String delAns = scanner.nextLine().trim();
if (delAns.equalsIgnoreCase("y")) {
    System.out.println("You selected to delete " +clusterId);
    System.out.print("Press Enter to continue...");
    scanner.nextLine();
    deleteRedshiftCluster(redshiftClient, clusterId);
} else {
    System.out.println("The "+clusterId +" was not deleted");
}
System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("This concludes the Amazon Redshift SDK Getting
Started scenario.");
        System.out.println(DASHES);
    }

    public static void listAllDatabases(RedshiftDataClient redshiftDataClient,
String clusterId, String dbUser, String database) {
        try {
            ListDatabasesRequest databasesRequest =
ListDatabasesRequest.builder()
                .clusterIdentifier(clusterId)
                .dbUser(dbUser)
                .database(database)
                .build();

            ListDatabasesIterable listDatabasesIterable =
redshiftDataClient.listDatabasesPaginator(databasesRequest);
            listDatabasesIterable.stream()
                .flatMap(r -> r.databases().stream())
                .forEach(db -> System.out
                    .println("The database name is : " + db));

        } catch (RedshiftDataException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void deleteRedshiftCluster(RedshiftClient redshiftClient,
String clusterId) {
        try {
            DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
                .clusterIdentifier(clusterId)
                .skipFinalClusterSnapshot(true)
                .build();

            DeleteClusterResponse response =
redshiftClient.deleteCluster(deleteClusterRequest);
            System.out.println("The status is " +
response.cluster().clusterStatus());

        } catch (RedshiftException e) {
```

```
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void popTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName, String fileName, int number)
throws IOException {
    JsonParser parser = new JsonFactory().createParser(new File(fileName));
    com.fasterxml.jackson.databind.JsonNode rootNode = new
ObjectMapper().readTree(parser);
    Iterator<JsonNode> iter = rootNode.iterator();
    ObjectNode currentNode;
    int t = 0;
    while (iter.hasNext()) {
        if (t == number)
            break;
        currentNode = (ObjectNode) iter.next();
        int year = currentNode.get("year").asInt();
        String title = currentNode.get("title").asText();

        // Use SqlParameter to avoid SQL injection.
        List<SqlParameter> parameterList = new ArrayList<>();
        String sqlStatement = "INSERT INTO Movies
VALUES( :id , :title, :year)";

        // Create the parameters.
        SqlParameter idParam = SqlParameter.builder()
            .name("id")
            .value(String.valueOf(t))
            .build();

        SqlParameter titleParam= SqlParameter.builder()
            .name("title")
            .value(title)
            .build();

        SqlParameter yearParam = SqlParameter.builder()
            .name("year")
            .value(String.valueOf(year))
            .build();
        parameterList.add(idParam);
        parameterList.add(titleParam);
        parameterList.add(yearParam);
    }
}
```

```
        try {
            ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
                .clusterIdentifier(clusterId)
                .sql(sqlStatement)
                .database(databaseName)
                .dbUser(userName)
                .parameters(parameterList)
                .build();

            redshiftDataClient.executeStatement(insertStatementRequest);
            System.out.println("Inserted: " + title + " (" + year + ")");
            t++;

        } catch (RedshiftDataException e) {
            System.err.println("Error inserting data: " + e.getMessage());
            System.exit(1);
        }
    }
    System.out.println(t + " records were added to the Movies table. ");
}

public static void checkStatement(RedshiftDataClient redshiftDataClient,
String sqlId) {
    try {
        DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
            .id(sqlId)
            .build();

        String status;
        while (true) {
            DescribeStatementResponse response =
redshiftDataClient.describeStatement(statementRequest);
            status = response.statusAsString();
            System.out.println("..." + status);

            if (status.compareTo("FAILED") == 0 ) {
                System.out.println("The Query Failed. Ending program");
                System.exit(1);
            }

            } else if (status.compareTo("FINISHED") == 0) {
                break;
            }
        }
    }
}
```

```
        }
        TimeUnit.SECONDS.sleep(1);
    }

    System.out.println("The statement is finished!");

} catch (RedshiftDataException | InterruptedException e) {
    System.err.println(e.getMessage());
    System.exit(1);
}
}

public static void modifyCluster(RedshiftClient redshiftClient, String
clusterId) {
    try {
        ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .preferredMaintenanceWindow("wed:07:30-wed:08:00")
            .build();

        ModifyClusterResponse clusterResponse =
redshiftClient.modifyCluster(modifyClusterRequest);
        System.out.println("The modified cluster was successfully modified
and has "
            + clusterResponse.cluster().preferredMaintenanceWindow() + " as
the maintenance window");

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static String queryMoviesByYear(RedshiftDataClient redshiftDataClient,
String database,
String dbUser,
int year,
String clusterId) {

    try {
        String sqlStatement = " SELECT * FROM Movies WHERE year = :year";
        SqlParameter yearParam= SqlParameter.builder()
            .name("year")
```

```
        .value(String.valueOf(year))
        .build();

        ExecuteStatementRequest statementRequest =
ExecuteStatementRequest.builder()
        .clusterIdentifier(clusterId)
        .database(database)
        .dbUser(dbUser)
        .parameters(yearParam)
        .sql(sqlStatement)
        .build();

        ExecuteStatementResponse response =
redshiftDataClient.executeStatement(statementRequest);
        return response.id();

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
}

public static void getResults(RedshiftDataClient redshiftDataClient, String
statementId) {
    try {
        GetStatementResultRequest resultRequest =
GetStatementResultRequest.builder()
        .id(statementId)
        .build();

        // Extract and print the field values using streams.
        GetStatementResultResponse response =
redshiftDataClient.getStatementResult(resultRequest);
        response.records().stream()
            .flatMap(List::stream)
            .map(Field::stringValue)
            .filter(value -> value != null)
            .forEach(value -> System.out.println("The Movie title field is "
+ value));

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

```
    }  
  }  
  
  public static void waitForClusterReady(RedshiftClient redshiftClient, String  
clusterId) {  
    boolean clusterReady = false;  
    String clusterReadyStr;  
    System.out.println("Waiting for cluster to become available. This may  
take a few mins.");  
    try {  
      DescribeClustersRequest clustersRequest =  
DescribeClustersRequest.builder()  
        .clusterIdentifier(clusterId)  
        .build();  
      long startTime = System.currentTimeMillis();  
  
      // Loop until the cluster is ready.  
      while (!clusterReady) {  
        DescribeClustersResponse clusterResponse =  
redshiftClient.describeClusters(clustersRequest);  
        List<Cluster> clusterList = clusterResponse.clusters();  
        for (Cluster cluster : clusterList) {  
          clusterReadyStr = cluster.clusterStatus();  
          if (clusterReadyStr.contains("available"))  
            clusterReady = true;  
          else {  
            long elapsedTimeMillis = System.currentTimeMillis() -  
startTime;  
  
            long elapsedSeconds = elapsedTimeMillis / 1000;  
            long minutes = elapsedSeconds / 60;  
            long seconds = elapsedSeconds % 60;  
  
            System.out.printf("Elapsed Time: %02d:%02d - Waiting for  
cluster... %n", minutes, seconds);  
            TimeUnit.SECONDS.sleep(5);  
          }  
        }  
      }  
  
      long elapsedTimeMillis = System.currentTimeMillis() - startTime;  
      long elapsedSeconds = elapsedTimeMillis / 1000;  
      long minutes = elapsedSeconds / 60;  
      long seconds = elapsedSeconds % 60;
```

```
        System.out.println(String.format("Cluster is available! Total Elapsed
Time: %02d:%02d", minutes, seconds));

    } catch (RedshiftException | InterruptedException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void createTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName) {
    try {
        ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
            .clusterIdentifier(clusterId)
            .dbUser(userName)
            .database(databaseName)
            .sql("CREATE TABLE Movies ("
                + "id INT PRIMARY KEY, "
                + "title VARCHAR(100), "
                + "year INT)")
            .build();

        redshiftDataClient.executeStatement(createTableRequest);
        System.out.println("Table created: Movies");

    } catch (RedshiftDataException e) {
        System.err.println("Error creating table: " + e.getMessage());
        System.exit(1);
    }
}

public static void createCluster(RedshiftClient redshiftClient, String
clusterId, String masterUsername,
                                String masterUserPassword) {
    try {
        CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .masterUsername(masterUsername)
            .masterUserPassword(masterUserPassword)
            .nodeType("ra3.4xlarge")
            .publiclyAccessible(true)
            .numberOfNodes(2)
            .build();
```



```
        CreateClusterResponse clusterResponse =
redshiftClient.createCluster(clusterRequest);
        System.out.println("Created cluster " +
clusterResponse.cluster().clusterIdentifier());

    } catch (RedshiftException e) {

        System.err.println(e.getMessage());
        System.exit(1);
    }
}
}
```

- Untuk detail API, lihat topik berikut di Referensi API AWS SDK for Java 2.x .
 - [CreateCluster](#)
 - [DeskripsiKlusters](#)
 - [DescribePernyataan](#)
 - [ExecuteStatement](#)
 - [mendapatkan StatementResult](#)
 - [daftar DatabasesPaginator](#)
 - [ModifyCluster](#)

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [AWS Repositori Contoh Kode](#).

```
class RedshiftScenario:
    """Runs an interactive scenario that shows how to get started with
    Redshift."""
```

```
def __init__(self, redshift_wrapper, redshift_data_wrapper):
    self.redshift_wrapper = redshift_wrapper
    self.redshift_data_wrapper = redshift_data_wrapper

def redshift_scenario(self, json_file_path):
    database_name = "dev"

    print(DASHES)
    print("Welcome to the Amazon Redshift SDK Getting Started example.")
    print(
        """
This Python program demonstrates how to interact with Amazon Redshift
using the AWS SDK for Python (Boto3).

Amazon Redshift is a fully managed, petabyte-scale data warehouse
service hosted in the cloud.

The program's primary functionalities include cluster creation,
verification of cluster readiness, listing databases, table creation,
populating data within the table, and executing SQL statements.

It also demonstrates querying data from the Movies table.

Upon completion, all AWS resources are cleaned up.
"""
    )
    if not os.path.isfile(json_file_path):
        logging.error(f"The file {json_file_path} does not exist.")
        return

    print("Let's get started...")
    user_name = q.ask("Please enter your user name (default is awsuser):")
    user_name = user_name if user_name else "awsuser"

    print(DASHES)
    user_password = q.ask(
        "Please enter your user password (default is AwsUser1000):"
    )
    user_password = user_password if user_password else "AwsUser1000"

    print(DASHES)
    print(
        """A Redshift cluster refers to the collection of computing resources
and storage that work
```

```
        together to process and analyze large volumes of data."""
    )
    cluster_id = q.ask(
        "Enter a cluster identifier value (default is redshift-cluster-
movies): "
    )
    cluster_id = cluster_id if cluster_id else "redshift-cluster-movies"

    self.redshift_wrapper.create_cluster(
        cluster_id, "ra3.4xlarge", user_name, user_password, True, 2
    )

    print(DASHES)
    print(f"Wait until {cluster_id} is available. This may take a few
minutes...")
    q.ask("Press Enter to continue...")

    self.wait_cluster_available(cluster_id)

    print(DASHES)

    print(
        f"""
When you created {cluster_id}, the dev database is created by default and
used in this scenario.

To create a custom database, you need to have a CREATEDB privilege.
For more information, see the documentation here:
https://docs.aws.amazon.com/redshift/latest/dg/r\_CREATE\_DATABASE.html.
"""
    )
    q.ask("Press Enter to continue...")
    print(DASHES)

    print(DASHES)
    print(f"List databases in {cluster_id}")
    q.ask("Press Enter to continue...")
    databases = self.redshift_data_wrapper.list_databases(
        cluster_id, database_name, user_name
    )
    print(f"The cluster contains {len(databases)} database(s).")
    for database in databases:
        print(f"    Database: {database}")
    print(DASHES)
```

```
print(DASHES)
print("Now you will create a table named Movies.")
q.ask("Press Enter to continue...")

self.create_table(cluster_id, database_name, user_name)

print(DASHES)

print("Populate the Movies table using the Movies.json file.")
print(
    "Specify the number of records you would like to add to the Movies
Table."
)
print("Please enter a value between 50 and 200.")

while True:
    try:
        num_records = int(q.ask("Enter a value: ", q.is_int))
        if 50 <= num_records <= 200:
            break
        else:
            print("Invalid input. Please enter a value between 50 and
200.")
    except ValueError:
        print("Invalid input. Please enter a value between 50 and 200.")

self.populate_table(
    cluster_id, database_name, user_name, json_file_path, num_records
)

print(DASHES)
print("Query the Movies table by year. Enter a value between 2012-2014.")

while True:
    movie_year = int(q.ask("Enter a year: ", q.is_int))
    if 2012 <= movie_year <= 2014:
        break
    else:
        print("Invalid input. Please enter a valid year between 2012 and
2014.")

# Function to query database
sql_id = self.query_movies_by_year(
```

```
        database_name, user_name, movie_year, cluster_id
    )

    print(f"The identifier of the statement is {sql_id}")

    print("Checking statement status...")
    self.wait_statement_finished(sql_id)
    result = self.redshift_data_wrapper.get_statement_result(sql_id)

    self.display_movies(result)

    print(DASHES)

    print(DASHES)
    print("Now you will modify the Redshift cluster.")
    q.ask("Press Enter to continue...")

    preferred_maintenance_window = "wed:07:30-wed:08:00"
    self.redshift_wrapper.modify_cluster(cluster_id,
    preferred_maintenance_window)

    print(DASHES)

    print(DASHES)
    delete = q.ask("Do you want to delete the cluster? (y/n) ", q.is_yesno)

    if delete:
        print(f"You selected to delete {cluster_id}")
        q.ask("Press Enter to continue...")
        self.redshift_wrapper.delete_cluster(cluster_id)
    else:
        print(f"Cluster {cluster_id}cluster_id was not deleted")

    print(DASHES)
    print("This concludes the Amazon Redshift SDK Getting Started scenario.")
    print(DASHES)

    def create_table(self, cluster_id, database, username):
        self.redshift_data_wrapper.execute_statement(
            cluster_identifier=cluster_id,
            database_name=database,
            user_name=username,
            sql="CREATE TABLE Movies (statement_id INT PRIMARY KEY, title
            VARCHAR(100), year INT)",
```

```
)

print("Table created: Movies")

def populate_table(self, cluster_id, database, username, file_name, number):
    with open(file_name) as f:
        data = json.load(f)

    i = 0
    for record in data:
        if i == number:
            break

        statement_id = i
        title = record["title"]
        year = record["year"]
        i = i + 1
        parameters = [
            {"name": "statement_id", "value": str(statement_id)},
            {"name": "title", "value": title},
            {"name": "year", "value": str(year)},
        ]

        self.redshift_data_wrapper.execute_statement(
            cluster_identifier=cluster_id,
            database_name=database,
            user_name=username,
            sql="INSERT INTO Movies VALUES(:statement_id, :title, :year)",
            parameter_list=parameters,
        )

    print(f"{i} records inserted into Movies table")

def wait_cluster_available(self, cluster_id):
    """
    Waits for a cluster to be available.

    :param cluster_id: The cluster identifier.

    Note: The cluster_available waiter can also be used.
    It is not used in this case to allow an elapsed time message.
    """
    cluster_ready = False
```

```
start_time = time.time()

while not cluster_ready:
    time.sleep(30)
    cluster = self.redshift_wrapper.describe_clusters(cluster_id)
    status = cluster[0]["ClusterStatus"]
    if status == "available":
        cluster_ready = True
    elif status != "creating":
        raise Exception(
            f"Cluster {cluster_id} creation failed with status {status}."
        )

    elapsed_seconds = int(round(time.time() - start_time))
    minutes = int(elapsed_seconds // 60)
    seconds = int(elapsed_seconds % 60)

    print(f"Elapsed Time: {minutes}:{seconds:02d} - status {status}...")

    if minutes > 30:
        raise Exception(
            f"Cluster {cluster_id} is not available after 30 minutes."
        )

def query_movies_by_year(self, database, username, year, cluster_id):
    sql = "SELECT * FROM Movies WHERE year = :year"

    params = [{"name": "year", "value": str(year)}]

    response = self.redshift_data_wrapper.execute_statement(
        cluster_identifier=cluster_id,
        database_name=database,
        user_name=username,
        sql=sql,
        parameter_list=params,
    )

    return response["Id"]

@staticmethod
def display_movies(response):
    metadata = response["ColumnMetadata"]
    records = response["Records"]
```

```

    title_column_index = None
    for i in range(len(metadata)):
        if metadata[i]["name"] == "title":
            title_column_index = i
            break

    if title_column_index is None:
        print("No title column found.")
        return

    print(f"Found {len(records)} movie(s).")
    for record in records:
        print(f"    {record[title_column_index]['stringValue']}")

def wait_statement_finished(self, sql_id):
    while True:
        time.sleep(1)
        response = self.redshift_data_wrapper.describe_statement(sql_id)
        status = response["Status"]
        print(f"Statement status is {status}.")

        if status == "FAILED":
            print(f"The query failed because {response['Error']}. Ending
program")
            raise Exception("The Query Failed. Ending program")
        elif status == "FINISHED":
            break

```

Fungsi utama yang menunjukkan implementasi skenario.

```

def main():
    redshift_client = boto3.client("redshift")
    redshift_data_client = boto3.client("redshift-data")
    redshift_wrapper = RedshiftWrapper(redshift_client)
    redshift_data_wrapper = RedshiftDataWrapper(redshift_data_client)
    redshift_scenario = RedshiftScenario(redshift_wrapper, redshift_data_wrapper)
    redshift_scenario.redshift_scenario(
        f"{os.path.dirname(__file__)}/../../resources/sample_files/
movies.json"
    )

```


Fungsi pembungkus yang digunakan dalam skenario.

```
def create_cluster(
    self,
    cluster_identifier,
    node_type,
    master_username,
    master_user_password,
    publicly_accessible,
    number_of_nodes,
):
    """
    Creates a cluster.

    :param cluster_identifier: The name of the cluster.
    :param node_type: The type of node in the cluster.
    :param master_username: The master username.
    :param master_user_password: The master user password.
    :param publicly_accessible: Whether the cluster is publicly accessible.
    :param number_of_nodes: The number of nodes in the cluster.
    :return: The cluster.
    """

    try:
        cluster = self.client.create_cluster(
            ClusterIdentifier=cluster_identifier,
            NodeType=node_type,
            MasterUsername=master_username,
            MasterUserPassword=master_user_password,
            PubliclyAccessible=publicly_accessible,
            NumberOfNodes=number_of_nodes,
        )
        return cluster
    except ClientError as err:
        logging.error(
            "Couldn't create a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
```

```
        raise

def describe_clusters(self, cluster_identifier):
    """
    Describes a cluster.

    :param cluster_identifier: The cluster identifier.
    :return: A list of clusters.
    """
    try:
        kwargs = {}
        if cluster_identifier:
            kwargs["ClusterIdentifier"] = cluster_identifier

        paginator = self.client.get_paginator("describe_clusters")
        clusters = []
        for page in paginator.paginate(**kwargs):
            clusters.extend(page["Clusters"])

        return clusters

    except ClientError as err:
        logging.error(
            "Couldn't describe a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

def execute_statement(
    self, cluster_identifier, database_name, user_name, sql,
    parameter_list=None
):
    """
    Executes a SQL statement.

    :param cluster_identifier: The cluster identifier.
    :param database_name: The database name.
    :param user_name: The user's name.
    :param sql: The SQL statement.
    :param parameter_list: The optional SQL statement parameters.
    :return: The SQL statement result.
```

```
"""

try:
    kwargs = {
        "ClusterIdentifier": cluster_identifier,
        "Database": database_name,
        "DbUser": user_name,
        "Sql": sql,
    }
    if parameter_list:
        kwargs["Parameters"] = parameter_list
    response = self.client.execute_statement(**kwargs)
    return response
except ClientError as err:
    logging.error(
        "Couldn't execute statement. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise

def describe_statement(self, statement_id):
    """
    Describes a SQL statement.

    :param statement_id: The SQL statement identifier.
    :return: The SQL statement result.
    """
    try:
        response = self.client.describe_statement(Id=statement_id)
        return response
    except ClientError as err:
        logging.error(
            "Couldn't describe statement. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

def get_statement_result(self, statement_id):
    """
    Gets the result of a SQL statement.
```

```
:param statement_id: The SQL statement identifier.
:return: The SQL statement result.
"""
try:
    result = {
        "Records": [],
    }
    paginator = self.client.get_paginator("get_statement_result")
    for page in paginator.paginate(Id=statement_id):
        if "ColumnMetadata" not in result:
            result["ColumnMetadata"] = page["ColumnMetadata"]
            result["Records"].extend(page["Records"])
    return result
except ClientError as err:
    logging.error(
        "Couldn't get statement result. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise

def modify_cluster(self, cluster_identifier, preferred_maintenance_window):
    """
    Modifies a cluster.

    :param cluster_identifier: The cluster identifier.
    :param preferred_maintenance_window: The preferred maintenance window.
    """
    try:
        self.client.modify_cluster(
            ClusterIdentifier=cluster_identifier,
            PreferredMaintenanceWindow=preferred_maintenance_window,
        )
    except ClientError as err:
        logging.error(
            "Couldn't modify a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

```
def list_databases(self, cluster_identifier, database_name, database_user):
    """
    Lists databases in a cluster.

    :param cluster_identifier: The cluster identifier.
    :param database_name: The database name.
    :param database_user: The database user.
    :return: The list of databases.
    """
    try:
        paginator = self.client.get_paginator("list_databases")
        databases = []
        for page in paginator.paginate(
            ClusterIdentifier=cluster_identifier,
            Database=database_name,
            DbUser=database_user,
        ):
            databases.extend(page["Databases"])

        return databases
    except ClientError as err:
        logging.error(
            "Couldn't list databases. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

def delete_cluster(self, cluster_identifier):
    """
    Deletes a cluster.

    :param cluster_identifier: The cluster identifier.
    """
    try:
        self.client.delete_cluster(
            ClusterIdentifier=cluster_identifier,
            SkipFinalClusterSnapshot=True
        )
    except ClientError as err:
        logging.error(
            "Couldn't delete a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
```

```
        err.response["Error"]["Message"],
    )
    raise
```

- Untuk detail API, lihat topik berikut ini adalah Referensi API SDK untuk Python (Boto3)AWS
 - [CreateCluster](#)
 - [DeskripsiKlusters](#)
 - [DescribePernyataan](#)
 - [ExecuteStatement](#)
 - [mendapatkan StatementResult](#)
 - [daftar DatabasesPaginator](#)
 - [ModifyCluster](#)

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Contoh lintas layanan untuk Amazon AWS Redshift menggunakan SDK

Contoh aplikasi berikut menggunakan AWS SDK untuk menggabungkan Amazon Redshift dengan yang lain. Layanan AWS Setiap contoh menyertakan tautan ke GitHub, di mana Anda dapat menemukan petunjuk tentang cara mengatur dan menjalankan aplikasi.

Contoh

- [Buat pelacak item Amazon Redshift](#)

Buat pelacak item Amazon Redshift

Contoh kode berikut menunjukkan cara membuat aplikasi web yang melacak dan melaporkan item pekerjaan menggunakan database Amazon Redshift.

Java

SDK untuk Java 2.x

Menunjukkan cara membuat aplikasi web yang melacak dan melaporkan item pekerjaan yang disimpan dalam database Amazon Redshift.

Untuk kode sumber lengkap dan petunjuk tentang cara menyiapkan Spring REST API yang menanyakan data Amazon Redshift dan untuk digunakan oleh aplikasi React, lihat contoh lengkapnya di. [GitHub](#)

Layanan yang digunakan dalam contoh ini

- Amazon Redshift
- Amazon SES

Kotlin

SDK untuk Kotlin

Menunjukkan cara membuat aplikasi web yang melacak dan melaporkan item pekerjaan yang disimpan dalam database Amazon Redshift.

Untuk kode sumber lengkap dan petunjuk tentang cara menyiapkan Spring REST API yang menanyakan data Amazon Redshift dan untuk digunakan oleh aplikasi React, lihat contoh lengkapnya di. [GitHub](#)

Layanan yang digunakan dalam contoh ini

- Amazon Redshift
- Amazon SES

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan layanan ini dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Riwayat dokumen

Note

Untuk deskripsi fitur baru di Amazon Redshift, lihat [Apa yang baru.](#)

Tabel berikut menjelaskan perubahan dokumentasi penting pada Panduan Manajemen Pergeseran Merah Amazon setelah Juni 2018. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Versi API: 2012-12-01

Untuk daftar perubahan pada Panduan Pengembang Database Amazon Redshift, lihat riwayat dokumen Panduan Pengembang Database [Amazon Redshift.](#)

Untuk informasi selengkapnya tentang fitur baru, termasuk daftar perbaikan dan nomor versi kluster terkait untuk setiap rilis, lihat [Riwayat versi cluster.](#)

Perubahan	Deskripsi	Tanggal
Patch Amazon Redshift 181 dirilis.	Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat Amazon Redshift patch 181.	1 Mei 2024
Perbarui kebijakan terkelola editor kueri v2	Pembaruan untuk AmazonRedshiftQueryEditorV2 FullAccess , AmazonRedshiftQueryEditorV2 NoSharing AmazonRedshiftQueryEditorV2	Februari 21, 2024

ReadSharing , dan kebijakan AmazonRedshiftQueryEditorV2 ReadWriteSharing terkelola dengan izin redshift-serverless:ListNamespaces danredshift-serverless:ListWorkgroups .

[Perbarui kebijakan terkelola akses hanya-baca Amazon Redshift](#)

Pembaruan kebijakan AmazonRedshiftReadOnlyAccess terkelola dengan izin redshift:ListRecommendations untuk mencantumkan rekomendasi Amazon Redshift Advisor.

Februari 7, 2024

[Amazon Redshift patch 180 dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 180](#).

Desember 29, 2023

[Patch Amazon Redshift 179
dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 179](#).

9 November 2023

[Perbarui kebijakan terkelola
Amazon Redshift](#)

Pembaruan kebijakan AmazonRedshiftServiceLinkedRolePolicy terkelola dengan izin ec2:AssignIpv6Addresses dan ec2:UnassignIpv6Addresses .

31 Oktober 2023

[Patch Amazon Redshift 178
dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 178](#).

25 September 2023

[Perbarui kebijakan terkelola editor kueri v2](#)

Pembaruan Amazon Redshift Query Editor V2 NoSharing, Amazon Redshift Query Editor V2 ReadSharing, dan kebijakan Amazon Redshift Query Editor V2 ReadWriteSharing terkelola dengan izin sqlworkbench:GetAutocompletionMetadata dan sqlworkbench:GetAutocompletionResource.

16 Agustus 2023

[Perbarui kebijakan terkelola Amazon Redshift](#)

Pembaruan kebijakan Amazon Redshift ServiceLinkedRolePolicy terkelola untuk memberikan izin AWS Secrets Manager untuk membuat dan mengelola rahasia kredensi admin.

Agustus 14, 2023

[Patch Amazon Redshift 177 dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 177](#).

3 Agustus 2023

[Patch Amazon Redshift 176
dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 176](#).

8 Juni 2023

[Amazon Redshift patch 175
dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 175](#).

28 April 2023

[Perbarui kebijakan terkelola
Amazon Redshift](#)

Pembaruan kebijakan AmazonRedshiftServiceLinkedRolePolicy terkelola untuk menghapus izin untuk tindakan terkait jaringan ec2. Ini secara khusus terkait dengan tag Purpose: RedshiftMigrateToVpc resource.

27 April 2023

[Perbarui kebijakan terkelola
Amazon Redshift Data API](#)

Pembaruan kebijakan AmazonRedshiftDataFullAccess terkelola dengan izinredshift: GetClusterCredentialsWithIAM .

April 7, 2023

[Perbarui kebijakan terkelola editor kueri v2](#)

PembaruanAmazonRedshiftQueryEditorV2NoSharing ,AmazonRedshiftQueryEditorV2ReadSharing , dan kebijakan AmazonRedshiftQueryEditorV2ReadWriteSharing terkelola dengan izinsqlworkbench:GetSchemaInference .

21 Maret 2023

[Patch Amazon Redshift 174 dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch](#) 174.

Maret 11, 2023

[Perbarui kebijakan terkelola editor kueri v2](#)

PembaruanAmazonRedshiftQueryEditorV2NoSharing ,AmazonRedshiftQueryEditorV2ReadSharing , dan kebijakan AmazonRedshiftQueryEditorV2ReadWriteSharing terkelola dengan izinsqlworkbench:AssociateNotebookWithTab .

2 Februari 2023

[Patch Amazon Redshift 173
dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 173](#).

20 Januari 2023

[Patch Amazon Redshift 172
dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 172](#).

17 November 2022

[Patch Amazon Redshift 171
dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 171](#).

9 November 2022

[Amazon Redshift patch 170
dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 170](#).

20 Juli 2022

[Patch Amazon Redshift 169
dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 169](#).

Juni 8, 2022

[Patch Amazon Redshift 168
dirilis.](#)

Patch Amazon Redshift baru sedang digunakan. Dibutuhkan beberapa minggu agar versi baru tersedia di semua Amazon Redshift yang didukung. Wilayah AWS Untuk informasi selengkapnya tentang versi ini, lihat [Amazon Redshift patch 168](#).

19 April 2022

[Support untuk profil otentikasi
i dengan driver Amazon
Redshift](#)

Anda sekarang dapat terhubung ke Amazon Redshift dengan profil otentikasi.

2 Agustus 2021

Dukungan untuk titik akhir lintas-VPC untuk Amazon Redshift didukung oleh AWS PrivateLink	Anda sekarang dapat menggunakan titik akhir VPC yang dikelola RedShift dengan Amazon Redshift.	1 April 2021
Dukungan untuk penyempurnaan editor kueri Amazon Redshift	Anda sekarang dapat menggunakan editor kueri dengan perutean VPC yang disempurnakan, waktu menjalankan kueri yang lebih lama, dan lebih banyak jenis node cluster.	17 Februari 2021
Support untuk integrasi konsol dengan mitra	Anda dapat berintegrasi dengan mitra menggunakan konsol Amazon Redshift.	9 Desember 2020
Support untuk kemampuan memindahkan cluster antar Availability Zones	Anda sekarang dapat memindahkan cluster RA3 antara Availability Zones.	9 Desember 2020
Support untuk tipe node ra3.xlplus	Anda sekarang dapat membuat tipe node ra3.xlplus.	9 Desember 2020
Support untuk driver JDBC versi 2.0	Anda sekarang dapat mengkonfigurasi driver JDBC versi 2.0.	5 November 2020
Support untuk Lambda UDF dan tokenisasi	Anda sekarang dapat menulis UDF Lambda untuk mengaktifkan tokenisasi data eksternal.	26 Oktober 2020
Support untuk menjadwalkan menjalankan pernyataan SQL	Anda sekarang dapat menjadwalkan kueri di konsol Amazon Redshift.	22 Oktober 2020

Support untuk API Data untuk Amazon Redshift	Amazon Redshift sekarang dapat diakses menggunakan API Data bawaan. Pembaruan dokumentasi mencakup Referensi API Data Amazon Redshift.	10 September 2020
Dukungan untuk pemantauan kueri konsol Amazon Redshift	Memperbarui panduan untuk menjelaskan grafik pemantauan kueri baru.	7 Mei 2020
Support untuk batas penggunaan	Memperbarui panduan untuk menjelaskan batas penggunaan.	23 April 2020
Otentikasi multi-faktor	Memperbarui panduan untuk menjelaskan dukungan otentikasi multi-faktor.	20 April 2020
Ubah ukuran elastis sekarang mendukung perubahan tipe simpul	Deskripsi perubahan ukuran elastis yang diperbarui.	6 April 2020
Support untuk tipe node ra3.4xlarge dengan penyimpanan terkelola	Memperbarui panduan untuk menyertakan tipe node ra3.4xlarge.	2 April 2020
Support untuk jeda dan lanjutkan	Memperbarui panduan untuk menjelaskan jeda dan melanjutkan operasi cluster.	11 Maret 2020
Support untuk Microsoft Azure AD sebagai penyedia identitas	Memperbarui panduan untuk menjelaskan langkah-langkah untuk menggunakan Microsoft Azure AD sebagai penyedia identitas.	10 Februari 2020

Support untuk tipe node RA3	Memperbarui panduan untuk menjelaskan tipe node RA3 baru.	3 Desember 2019
Support untuk konsol baru	Memperbarui panduan untuk menggambarkan konsol Amazon Redshift baru.	11 November 2019
Pembaruan informasi keamanan	Pembaruan dokumentasi informasi keamanan.	24 Juni 2019
Penyempurnaan snapshot	Amazon Redshift sekarang mendukung beberapa penyempurnaan untuk mengelola dan menjadwalkan snapshot.	4 April 2019
Penskalaan konkurensi	Anda dapat mengonfigurasi manajemen beban kerja (WLM) untuk mengaktifkan mode penskalaan konkurensi. Untuk informasi selengkapnya, lihat Mengonfigurasi manajemen beban kerja .	21 Maret 2019
Driver JDBC dan ODBC yang diperbarui	Amazon Redshift sekarang mendukung versi baru driver JDBC dan ODBC. Untuk informasi selengkapnya, lihat Mengkonfigurasi koneksi JDBC dan Konfigurasi dan koneksi ODBC .	4 Februari 2019

[Pemeliharaan yang ditangguhkan](#)

Jika Anda perlu menjadwalkan ulang jendela pemeliharaan cluster Anda, Anda memiliki opsi untuk menunda pemeliharaan hingga 14 hari. Jika kami perlu memperbarui perangkat keras atau melakukan pembaruan wajib lainnya selama periode penundaan Anda, kami memberi tahu Anda dan membuat perubahan yang diperlukan. Cluster Anda tidak tersedia selama pembaruan ini. Untuk informasi lebih lanjut, lihat [Menunda pemeliharaan](#).

20 November 2018

[Pemberitahuan di muka](#)

Amazon Redshift memberikan pemberitahuan sebelumnya untuk beberapa acara. Peristiwa ini memiliki kategori acara pending. Misalnya, kami mengirim pemberitahuan terlebih dahulu jika pembaruan perangkat keras diperlukan untuk salah satu node di cluster Anda. Anda dapat berlangganan acara yang tertunda sama seperti acara Amazon Redshift lainnya. Untuk informasi selengkapnya, lihat [Berlangganan notifikasi acara Amazon Redshift](#).

20 November 2018

Ubah ukuran elastis	<p>Pengubahan ukuran elastis adalah metode tercepat untuk mengubah ukuran cluster. Elastic resize menambahkan atau menghapus node pada cluster yang ada, kemudian secara otomatis mendistribusikan kembali data ke node baru. Karena tidak membuat cluster baru, operasi pengubahan ukuran elastis selesai dengan cepat, biasanya dalam beberapa menit. Untuk informasi selengkapnya, lihat Mengubah ukuran cluster.</p>	15 November 2018
Driver ODBC baru	<p>Driver Amazon Redshift ODBC telah diperbarui ke versi 1.4.3.1000. Untuk informasi selengkapnya, lihat Mengkonfigurasi koneksi ODBC.</p>	8 November 2018
Batalkan operasi pengubahan ukuran	<p>Anda sekarang dapat membatalkan operasi pengubahan ukuran saat sedang berlangsung. Untuk informasi selengkapnya, lihat Mengubah ukuran ikhtisar operasi.</p>	2 November 2018

[Ubah cluster untuk mengubah enkripsi](#)

Anda dapat memodifikasi kluster yang tidak terenkripsi untuk menggunakan enkripsi AWS Key Management Service (AWS KMS), baik menggunakan kunci AWS-managed atau kunci yang dikelola pelanggan. Saat Anda memodifikasi kluster untuk mengaktifkan enkripsi KMS, Amazon Redshift secara otomatis memigrasikan data Anda ke kluster terenkripsi baru. Anda juga dapat memigrasikan kluster yang tidak terenkripsi ke kluster terenkripsi dengan memodifikasi kluster.

16 Oktober 2018

[Spektrum Amazon Redshift mendukung peningkatan perutean VPC](#)

Anda sekarang dapat menggunakan Redshift Spectrum dengan peningkatan perutean VPC yang diaktifkan untuk cluster Anda. Anda mungkin perlu melakukan langkah-langkah konfigurasi tambahan. Untuk informasi selengkapnya, lihat [Menggunakan spektrum Amazon Redshift dengan perutean VPC](#) yang disempurnakan.

10 Oktober 2018

Editor kueri	Sekarang Anda dapat menjalankan kueri SQL dari Amazon Redshift Management Console.	4 Oktober 2018
Bagan rincian eksekusi beban kerja	Sekarang Anda bisa mendapatkan tampilan terperinci tentang kinerja beban kerja Anda dengan melihat bagan Workload Execution Breakdown di konsol. Untuk informasi selengkapnya, lihat Menganalisis kinerja beban kerja .	30 Juli 2018
Trek pemeliharaan	Anda sekarang dapat menentukan apakah cluster Anda akan selalu diperbarui ke versi terbaru Amazon Redshift atau ke versi sebelumnya dengan memilih trek pemeliharaan. Untuk informasi selengkapnya, lihat Memilih trek pemeliharaan klaster .	26 Juli 2018

Tabel berikut menjelaskan perubahan penting pada Panduan Manajemen Pergeseran Merah Amazon sebelum Juli 2018.

Perubahan	Deskripsi	Tanggal rilis
CloudWatch Metrik baru	CloudWatch Metrik baru ditambahkan untuk memantau kinerja kueri. Untuk informasi selengkapnya, lihat Memantau Amazon Redshift menggunakan metrik CloudWatch	17 Mei 2018
Enkripsi HSM	Amazon Redshift hanya mendukung manajemen kunci AWS CloudHSM modul keamanan perangkat keras	6 Maret 2018

Perubahan	Deskripsi	Tanggal rilis
	(HSM). Untuk informasi selengkapnya, lihat Enkripsi basis data Amazon Redshift .	
Rantai Peran IAM	Jika peran IAM yang dilampirkan ke kluster Anda tidak memiliki akses ke sumber daya yang diperlukan, Anda dapat merantai peran lain, mungkin milik akun lain. Cluster Anda kemudian sementara mengasumsikan peran berantai untuk mengakses data. Anda juga dapat memberikan akses lintas akun dengan merantai peran. Setiap peran dalam rantai mengasumsikan peran berikutnya dalam rantai, sampai cluster mengambil peran di akhir rantai. Anda dapat merantai maksimal 10 peran. Untuk informasi selengkapnya, lihat Merantai peran IAM di Amazon Redshift .	Februari 23, 2018
Jenis node DC2 baru	Generasi baru tipe node compact compute (DC) menawarkan kinerja yang jauh lebih baik dengan harga yang sama dengan DC1. Untuk memanfaatkan peningkatan kinerja, Anda dapat memigrasikan cluster DC1 Anda ke tipe node DC2 yang lebih baru. Untuk informasi selengkapnya, lihat Cluster dan node di Amazon Redshift .	17 Oktober 2017
Sertifikat ACM	Amazon Redshift mengganti sertifikat SSL di kluster Anda dengan sertifikat yang dikeluarkan AWS Certificate Manager (ACM). ACM adalah otoritas sertifikat publik terpercaya (CA) yang dipercaya oleh sebagian besar sistem saat ini. Anda mungkin perlu memperbarui sertifikat CA root kepercayaan Anda saat ini untuk terus terhubung ke cluster Anda menggunakan SSL. Untuk informasi selengkapnya, lihat Transisi ke sertifikat ACM untuk koneksi SSL .	18 September 2017

Perubahan	Deskripsi	Tanggal rilis
Peran terkait layanan	Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Amazon Redshift. Peran terkait layanan telah ditentukan sebelumnya oleh Amazon Redshift dan menyertakan semua izin yang diperlukan layanan untuk memanggil AWS layanan atas nama klaster Amazon Redshift Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Amazon Redshift .	18 September 2017
Autentikasi pengguna basis data IAM	Anda dapat mengonfigurasi sistem Anda untuk mengizinkan pengguna membuat kredensial pengguna dan masuk ke database berdasarkan kredensi IAM mereka. Anda juga dapat mengonfigurasi sistem Anda agar pengguna dapat masuk menggunakan sistem masuk tunggal gabungan melalui penyedia identitas yang sesuai dengan SAMP 2.0. Untuk informasi selengkapnya, lihat Menggunakan otentikasi IAM untuk menghasilkan kredensi pengguna basis data .	11 Agustus 2017
Pemulihan tingkat tabel mendukung perutean VPC yang ditingkatkan	Pemulihan tingkat tabel sekarang didukung pada cluster yang menggunakan Perutean VPC yang disempurnakan . Untuk informasi selengkapnya, lihat Memulihkan tabel dari snapshot .	19 Juli 2017
Aturan pemantauan kueri	Menggunakan aturan pemantauan kueri WLM, Anda dapat menentukan batas kinerja berbasis metrik untuk antrian WLM dan menentukan tindakan apa yang harus diambil ketika kueri melampaui batas-batas tersebut—log, hop, atau abort. Anda menentukan aturan pemantauan kueri sebagai bagian dari konfigurasi manajemen beban kerja (WLM) Anda. Untuk informasi selengkapnya, lihat Mengkonfigurasi manajemen beban kerja .	April 21, 2017

Perubahan	Deskripsi	Tanggal rilis
Perutean VPC yang disempurnakan	Saat Anda menggunakan perutean VPC Amazon Redshift yang disempurnakan, Amazon Redshift memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data Anda melalui Amazon VPC Anda. Untuk informasi selengkapnya, lihat Perutean VPC yang disempurnakan di Amazon Redshift .	15 September 2016
Bidang log koneksi baru	Log Log koneksi audit memiliki dua bidang baru untuk melacak koneksi SSL. Jika Anda secara rutin memuat log audit ke tabel Amazon Redshift, Anda perlu menambahkan kolom baru berikut ke tabel target: sslcompression dan sslexpansion.	Mei 5, 2016
Driver ODBC baru	Driver Amazon Redshift ODBC telah diperbarui ke versi 1.2.7.1007. Untuk informasi selengkapnya, lihat Mengkonfigurasi koneksi ODBC .	30 Maret 2016
Peran IAM untuk COPY dan UNLOAD	Sekarang Anda dapat menentukan satu atau beberapa peran AWS Identity and Access Management (IAM) yang dapat digunakan klaster Anda untuk otentikasi untuk mengakses layanan lain AWS . Peran IAM menyediakan alternatif yang lebih aman untuk memberikan otentikasi dengan perintah COPY, UNLOAD, atau CREATE LIBRARY. Untuk informasi selengkapnya, lihat Mengotorisasi Amazon Redshift untuk mengakses layanan AWS lain atas nama Anda dan Mengotorisasi operasi COPY, UNLOAD, CREATE EXTERNAL FUNCTION, dan CREATE EXTERNAL SCHEMA menggunakan peran IAM .	29 Maret 2016
Kembalikan dari tabel	Anda dapat memulihkan tabel dari snapshot cluster ke tabel baru di cluster aktif. Untuk informasi selengkapnya, lihat Memulihkan tabel dari snapshot .	10 Maret 2016

Perubahan	Deskripsi	Tanggal rilis
Menggunakan Kondisi IAM dalam kebijakan	Anda selanjutnya dapat membatasi akses ke sumber daya dengan menggunakan elemen Kondisi dalam kebijakan IAM. Untuk informasi selengkapnya, lihat Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci .	Desember 10, 2015
Ubah yang dapat diakses publik	Anda dapat memodifikasi klaster yang ada di VPC untuk mengubah apakah klaster tersebut dapat diakses publik. Untuk informasi selengkapnya, lihat Mengubah klaster .	November 20, 2015
Perbaikan dokumentasi	Menerbitkan berbagai perbaikan dokumentasi.	Agustus 28, 2015
Pembaruan dokumentasi	Panduan pemecahan masalah yang diperbarui tentang konfigurasi pengaturan jaringan untuk memastikan bahwa host dengan ukuran unit transmisi maksimum (MTU) yang berbeda dapat menentukan ukuran paket untuk koneksi. Untuk informasi selengkapnya, lihat Kueri tampaknya hang dan terkadang gagal mencapai cluster .	Agustus 25, 2015
Pembaruan dokumentasi	Merevisi seluruh bagian tentang kelompok parameter untuk organisasi dan kejelasan yang lebih baik. Untuk informasi selengkapnya, lihat Grup parameter Amazon Redshift .	17 Agustus 2015
Properti dinamis WLM	Parameter konfigurasi WLM sekarang mendukung penerapan beberapa properti secara dinamis. Properti lain tetap berubah statis dan mengharuskan cluster terkait di-boot ulang sehingga perubahan konfigurasi dapat diterapkan. Untuk informasi selengkapnya, lihat Sifat dinamis dan statis WLM dan Grup parameter Amazon Redshift .	3 Agustus 2015

Perubahan	Deskripsi	Tanggal rilis
Salin kluster terenkripsi KMS ke Wilayah lain AWS	Menambahkan konten tentang mengonfigurasi hibah salinan snapshot untuk mengaktifkan penyalinan cluster AWS KMS-enkripsi ke Wilayah lain. AWS Untuk informasi selengkapnya, lihat Menyalin AWS KMS—snapshot terenkripsi ke Wilayah lain AWS .	28 Juli 2015
Pembaruan dokumentasi	Memperbarui bagian enkripsi basis data untuk menjelaskan dengan lebih baik bagaimana Amazon Redshift menggunakan AWS KMS atau HSM untuk mengelola kunci, dan bagaimana proses enkripsi bekerja dengan masing-masing opsi ini. Untuk informasi selengkapnya, lihat Enkripsi basis data Amazon Redshift .	28 Juli 2015
Tipe node baru	Amazon Redshift sekarang menawarkan tipe node baru, DS2. Referensi dokumentasi yang diperbarui ke tipe node yang ada untuk menggunakan nama baru yang diperkenalkan dalam rilis ini. Juga merevisi bagian untuk menjelaskan kombinasi tipe node dengan lebih baik dan memperjelas batas kuota default. Untuk informasi selengkapnya, lihat Cluster dan node di Amazon Redshift .	Juni 9, 2015
Penawaran node cadangan	Menambahkan konten tentang penawaran node cadangan baru. Juga merevisi bagian untuk menjelaskan dan membandingkan penawaran yang tersedia dengan lebih baik, dan memberikan contoh untuk menunjukkan bagaimana harga node sesuai permintaan dan cadangan memengaruhi penagihan. Untuk informasi selengkapnya, lihat Gambaran Umum .	Juni 9, 2015

Perubahan	Deskripsi	Tanggal rilis
Driver ODBC baru	Driver Amazon Redshift ODBC telah diperbarui. Menambahkan bagian untuk versi sebelumnya dari driver ini dan tautan untuk merilis catatan untuk driver. Untuk informasi selengkapnya, lihat Mengkonfigurasi koneksi ODBC .	Juni 5, 2015
Perbaikan dokumentasi	Menerbitkan berbagai perbaikan dokumentasi.	30 April 2015
Fitur baru	Rilis Amazon Redshift ini memperkenalkan driver ODBC dan JDBC baru yang dioptimalkan untuk digunakan dengan Amazon Redshift. Untuk informasi selengkapnya, lihat Menyambung ke gudang data Amazon Redshift menggunakan alat klien SQL .	26 Februari 2015
Fitur baru	Rilis Amazon Redshift ini memperkenalkan metrik kinerja kluster yang memungkinkan Anda melihat dan menganalisis detail eksekusi kueri. Untuk informasi selengkapnya, lihat Melihat kueri dan beban .	26 Februari 2015
Pembaruan dokumentasi	Menambahkan contoh kebijakan baru yang menunjukkan pemberian izin untuk tindakan AWS layanan umum dan sumber daya yang menjadi sandaran Amazon Redshift. Untuk informasi selengkapnya, lihat Contoh kebijakan yang dikelola pelanggan .	Januari 16, 2015
Pembaruan dokumentasi	Panduan terbaru tentang pengaturan unit transmisi maksimum (MTU) untuk menonaktifkan frame jumbo TCP/IP. Untuk informasi selengkapnya, lihat Gunakan EC2-VPC saat Anda membuat cluster dan Kueri tampaknya hang dan terkadang gagal mencapai cluster .	Januari 16, 2015

Perubahan	Deskripsi	Tanggal rilis
Pembaruan dokumentasi	Merevisi konten tentang <code>wlm_json_configuration</code> parameter, dan memberikan contoh sintaks untuk mengkonfigurasi parameter ini dengan menggunakan sistem operasi Linux, Mac OS X, dan Microsoft Windows. AWS CLI Untuk informasi selengkapnya, lihat Mengkonfigurasi manajemen beban kerja .	Januari 13, 2015
Pembaruan dokumentasi	Menambahkan pemberitahuan dan deskripsi acara yang hilang. Untuk informasi selengkapnya, lihat Kategori acara Amazon Redshift dan pesan acara .	8 Januari 2015
Pembaruan dokumentasi	Panduan terbaru tentang kebijakan IAM untuk tindakan dan sumber daya Amazon Redshift. Merevisi bagian untuk meningkatkan organisasi dan kejelasan. Untuk informasi selengkapnya, lihat Keamanan di Amazon Redshift .	November 21, 2014
Fitur baru	Rilis Amazon Redshift ini memperkenalkan kemampuan untuk mengenkripsi cluster menggunakan kunci enkripsi from (). AWS Key Management Service AWS KMS AWS KMS menggabungkan perangkat keras dan perangkat lunak yang aman dan sangat tersedia untuk menyediakan sistem manajemen kunci yang diskalakan untuk cloud. Untuk informasi selengkapnya tentang AWS KMS dan opsi enkripsi untuk Amazon Redshift, lihat Enkripsi basis data Amazon Redshift dan Mengelola cluster menggunakan konsol	12 November 2014

Perubahan	Deskripsi	Tanggal rilis
Fitur baru	Rilis Amazon Redshift ini memperkenalkan kemampuan untuk menandai sumber daya, seperti cluster dan snapshot. Tag memungkinkan Anda menyediakan metadata yang ditentukan pengguna untuk mengkategorikan laporan penagihan berdasarkan alokasi biaya, dan untuk membantu Anda mengidentifikasi sumber daya dengan lebih baik dalam sekejap. Untuk informasi selengkapnya, lihat Menandai sumber daya di Amazon Redshift .	November 4, 2014
Fitur baru	Meningkatkan batas node maksimum menjadi 128 node untuk ukuran node dw1.8xlarge dan dw2.8xlarge. Untuk informasi selengkapnya, lihat Cluster dan node di Amazon Redshift .	30 Oktober 2014
Pembaruan dokumentasi	Ditambahkan link ke Microsoft Visual C ++ 2010 Redistributable Packages yang diperlukan untuk Amazon Redshift untuk menggunakan driver PostgreSQL ODBC. Untuk informasi selengkapnya, lihat Instal dan konfigurasi driver Amazon Redshift ODBC di Microsoft Windows .	30 Oktober 2014
Fitur baru	Menambahkan kemampuan untuk menghentikan kueri dan pemuatan dari konsol Amazon Redshift. Untuk informasi selengkapnya, lihat Melihat kueri dan beban dan Melihat metrik cluster selama operasi pemuatan .	28 Oktober 2014
Perbaikan dokumentasi	Menerbitkan berbagai perbaikan dokumentasi.	Oktober 17, 2014
Konten baru	Menambahkan konten tentang mematikan cluster dan menghapus cluster. Untuk informasi selengkapnya, lihat Mematikan dan menghapus cluster dan Menghapus klaster .	Agustus 14, 2014

Perubahan	Deskripsi	Tanggal rilis
Pembaruan dokumentasi	Mengklarifikasi perilaku setelah Izinkan Peningkatan Versi untuk klaster. Untuk informasi selengkapnya, lihat Ikhtisar Amazon Redshift .	Agustus 14, 2014
Pembaruan dokumentasi	Prosedur, tangkapan layar, dan pengaturan topik yang direvisi tentang bekerja dengan cluster di konsol Amazon Redshift. Untuk informasi selengkapnya, lihat Mengelola cluster menggunakan konsol .	Juli 11, 2014
Konten baru	Menambahkan tutorial baru tentang mengubah ukuran cluster Amazon Redshift, termasuk cara mengubah ukuran cluster sambil meminimalkan jumlah waktu cluster dalam mode hanya-baca. Untuk informasi selengkapnya, lihat Mengubah ukuran cluster .	27 Juni 2014
Fitur baru	Menambahkan kemampuan untuk mengganti nama cluster. Untuk informasi selengkapnya, lihat Mengganti nama cluster dan Mengubah klaster .	Juni 2, 2014
Pembaruan dokumentasi	Memperbarui contoh kode.NET untuk menggunakan penyedia data ODBC saat menghubungkan ke cluster secara terprogram dengan menggunakan.NET. Untuk informasi selengkapnya, lihat Connect ke gudang data Anda secara terprogram .	15 Mei 2014
Fitur baru	Menambahkan opsi untuk memilih grup parameter dan grup keamanan yang berbeda saat Anda memulihkan cluster dari snapshot. Untuk informasi selengkapnya, lihat Memulihkan cluster dari snapshot .	12 Mei 2014

Perubahan	Deskripsi	Tanggal rilis
Fitur baru	Menambahkan bagian baru untuk menjelaskan cara mengonfigurasi CloudWatch alarm Amazon default untuk memantau persentase ruang disk yang digunakan dalam cluster Amazon Redshift. Alarm ini adalah opsi baru dalam proses pembuatan cluster. Untuk informasi selengkapnya, lihat Alarm ruang disk default .	28 April 2014
Pembaruan dokumentasi	Informasi yang diklarifikasi tentang dukungan Elliptic curve Diffie—Hellman Exchange (ECDHE) di Amazon Redshift. Untuk informasi selengkapnya, lihat Connect menggunakan SSL .	April 22, 2014
Fitur baru	Menambahkan pernyataan tentang dukungan Amazon Redshift untuk protokol perjanjian kunci kurva Elliptic Diffie—Hellman (ECDH). Untuk informasi selengkapnya, lihat Connect menggunakan SSL .	18 April 2014
Pembaruan dokumentasi	Merevisi dan mengatur ulang topik di bagian ini Menyambung ke gudang data Amazon Redshift menggunakan alat klien SQL . Menambahkan informasi selengkapnya tentang koneksi JDBC dan ODBC, dan bagian pemecahan masalah baru untuk masalah koneksi.	15 April 2014
Pembaruan dokumentasi	Ditambahkan versi dalam contoh kebijakan IAM di seluruh panduan.	3 April 2014
Pembaruan dokumentasi	Menambahkan informasi tentang cara kerja penetapan harga saat Anda mengubah ukuran klaster. Untuk informasi selengkapnya, lihat Membeli node cadangan Amazon Redshift .	2 April 2014

Perubahan	Deskripsi	Tanggal rilis
Fitur baru	Menambahkan bagian tentang parameter baru, <code>max_cursor_result_set_size</code> , yang menetapkan ukuran set hasil maksimum, dalam megabyte, yang dapat disimpan per kursor individu. Nilai parameter ini juga mempengaruhi jumlah kursor yang aktif secara bersamaan untuk cluster. Untuk informasi selengkapnya, lihat Grup parameter Amazon Redshift .	Maret 28, 2014
Fitur baru	Menambahkan penjelasan tentang bidang Versi Cluster sekarang termasuk versi mesin cluster dan nomor revisi database. Untuk informasi selengkapnya, lihat Cluster yang disediakan Amazon Redshift .	Maret 21, 2014
Fitur baru	Memperbarui prosedur pengubahan ukuran untuk menampilkan informasi kemajuan pengubahan ukuran baru pada tab Status klaster. Untuk informasi selengkapnya, lihat Mengubah ukuran cluster .	Maret 21, 2014
Pembaruan dokumentasi	Diatur ulang dan diperbarui Apa itu Amazon Redshift? dan Ikhtisar cluster yang disediakan Amazon Redshift direvisi. Menerbitkan berbagai perbaikan dokumentasi.	21 Februari 2014
Fitur baru	Menambahkan jenis dan ukuran node baru untuk klaster Amazon Redshift, dan menulis ulang topik ikhtisar klaster terkait untuk organisasi dan kejelasan yang lebih baik berdasarkan umpan balik. Untuk informasi selengkapnya, lihat Cluster yang disediakan Amazon Redshift .	Januari 23, 2014
Fitur baru	Menambahkan informasi tentang penggunaan alamat IP elastis (EIP) untuk cluster Amazon Redshift yang dapat diakses publik di cloud pribadi virtual. Untuk informasi selengkapnya tentang EIP di Amazon Redshift, Mengelola cluster dalam VPC lihat dan Membuat cluster di VPC	Desember 20, 2013

Perubahan	Deskripsi	Tanggal rilis
Fitur baru	Menambahkan informasi tentang AWS CloudTrail log untuk Amazon Redshift. Untuk informasi selengkapnya tentang dukungan Amazon Redshift CloudTrail, lihat Logging dengan CloudTrail	13 Desember 2013
Fitur baru	Menambahkan informasi tentang log aktivitas pengguna baru dan parameter <code>enable_user_activity_logging</code> database untuk fitur pencatatan audit database di Amazon Redshift. Untuk informasi selengkapnya tentang pencatatan audit database, lihat Pencatatan audit basis data . Untuk informasi selengkapnya tentang parameter basis data, lihat Grup parameter Amazon Redshift .	Desember 6, 2013
Fitur baru	Diperbarui untuk menjelaskan konfigurasi Amazon Redshift untuk secara otomatis menyalin snapshot otomatis dan manual ke Wilayah sekunder. AWS Untuk informasi selengkapnya tentang mengonfigurasi salinan snapshot lintas wilayah, lihat Menyalin snapshot ke Wilayah lain AWS	14 November 2013
Fitur baru	Menambahkan bagian untuk menjelaskan pencatatan audit Amazon Redshift untuk koneksi dan aktivitas pengguna, dan menyimpan log ini di Amazon S3. Untuk informasi selengkapnya tentang pencatatan audit database, lihat Pencatatan audit basis data .	November 11, 2013

Perubahan	Deskripsi	Tanggal rilis
Fitur baru	Menambahkan bagian untuk menjelaskan enkripsi Amazon Redshift dengan fitur baru untuk mengelola kunci enkripsi dalam modul keamanan perangkat keras (HSM) dan memutar kunci enkripsi. Untuk informasi selengkapnya tentang enkripsi, HSM, dan rotasi kunci, lihat Enkripsi basis data Amazon Redshift Enkripsi untuk Amazon Redshift menggunakan modul keamanan perangkat keras , dan Rotasi kunci enkripsi di Amazon Redshift .	November 11, 2013
Fitur baru	Diperbarui untuk menjelaskan pemberitahuan penerbitan peristiwa Amazon Redshift dengan menggunakan Amazon SNS. Untuk informasi tentang notifikasi acara Amazon Redshift, lihat. Pemberitahuan acara Amazon Redshift	November 11, 2013
Fitur baru	Diperbarui untuk menjelaskan izin tingkat sumber daya IAM. Untuk informasi tentang izin Amazon Redshift IAM, lihat. Keamanan di Amazon Redshift	Agustus 9, 2013
Fitur baru	Diperbarui untuk menjelaskan metrik kemajuan pemulihan. Untuk informasi selengkapnya, lihat Memulihkan cluster dari snapshot .	Agustus 9, 2013
Fitur baru	Diperbarui untuk menjelaskan berbagi snapshot cluster dan membuat metrik kemajuan snapshot. Untuk informasi selengkapnya, lihat Berbagi snapshot .	Juli 17, 2013
Perbaikan dokumentasi	Menerbitkan berbagai perbaikan dokumentasi.	8 Juli 2013
Layar konsol baru	Memperbarui Panduan Manajemen Amazon Redshift untuk mencocokkan perubahan di konsol Amazon Redshift.	April 22, 2013

Perubahan	Deskripsi	Tanggal rilis
Panduan baru	Ini adalah rilis pertama dari Amazon Redshift Management Guide.	Februari 14, 2013

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.