aws

Guia de gerenciamento

# Amazon Redshift

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

# Amazon Redshift: Guia de gerenciamento

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

# Table of Contents

O que é o Amazon Redshift? ..... 1
Você é um usuário iniciante do Amazon Redshift? ..... 1
Visão geral dos recursos do Amazon Redshift Serverless ..... 2
Visão geral dos clusters provisionados do Amazon Redshift ..... 5
Gerenciamento de clusters ..... 5
Segurança e acesso a clusters ..... 6
Monitoramento de clusters ..... 8
Bancos de dados ..... 9
Comparar o Amazon Redshift Serverless a um data warehouse provisionado do Amazon Redshift Serverless ..... 9
Usar as interfaces de gerenciamento do Amazon Redshift para clusters provisionados ..... 38
Como trabalhar com AWS SDKs ..... 39
Assinatura de uma solicitação HTTP ..... 40
Configurar a CLI do Amazon Redshift ..... 45
Amazon Redshift sem servidor ..... 47
O que é o Amazon Redshift Serverless? ..... 47
Console do Amazon Redshift Serverless ..... 48
Considerações ao usar o Amazon Redshift Serverless ..... 52
Capacidade computacional do Amazon Redshift Serverless ..... 55
Noções básicas sobre a capacidade do Amazon Redshift Serverless ..... 55
Escalabilidade e otimização orientadas por IA (visualização) ..... 56
Faturamento do Amazon Redshift Serverless ..... 58
Definição de preço ..... 58
Faturamento da capacidade computacional ..... 58
Faturamento para armazenamento ..... 63
Usar o teste gratuito do Amazon Redshift sem servidor ..... 63
Observações sobre o uso de faturamento ..... 63
Conectar-se ao Amazon Redshift Serverless ..... 65
Conectar-se ao Amazon Redshift Serverless ..... 66
Conectar-se ao Amazon Redshift Serveless por meio de drivers JDBC ..... 66
Conectar-se ao Amazon Redshift Serverless com a API de dados ..... 68
Conectar-se com SSL ao Amazon Redshift Serverless ..... 68
Conexão com o Amazon Redshift Serverless por um endpoint da VPC gerenciado pelo Amazon Redshift ..... 70

Conexão ao Amazon Redshift sem servidor por um endpoint da VPC do Redshift em outra conta ou região ... 70
Definir configurações de tráfego de rede apropriadas para o Amazon Redshift sem servidor ... 75
Definir perfis de banco de dados para conceder a usuários federados no Amazon Redshift sem servidor ... 76
Recursos adicionais do ... 76
Definir perfis de banco de dados para conceder a usuários federados no Amazon Redshift sem servidor ... 76
Gerenciamento de Identidade e Acesso no Amazon Redshift Serverless ... 80
Conceder as permissões necessárias para o Amazon Redshift Serverless ... 80
Conceitos básicos das credenciais do IAM para o Amazon Redshift ... 82
Gerenciar o acesso aos objetos do banco de dados do Amazon Redshift sem servidor com permissões de perfil de banco de dados ... 83
Migrar um cluster provisionado para o Amazon Redshift Serverless ... 84
Criar um snapshot do cluster provisionado ... 85
Conexão com o Amazon Redshift sem servidor usando um driver ... 86
Usando o SDK do Amazon Redshift Serverless ... 88
Visão geral dos grupos de trabalho e namespaces do Amazon Redshift Serverless ... 89
Visão geral de grupos de trabalho e namespaces do Amazon Redshift Serverless ... 89
Gerenciar o Amazon Redshift Serverless usando o console ... 91
Configurar o Amazon Redshift Serverless pela primeira vez ... 92
Trabalhar com grupos de trabalho ... 92
Trabalhar com namespaces ... 98
Gerenciar limites de uso, limites de consulta e outras tarefas administrativas ... 101
Monitorar consultas e workloads com o Amazon Redshift Serverless ... 104
Monitorar consultas e workload com o Amazon Redshift Serverless ... 104
Registro de auditoria para o Amazon Redshift Serverless ... 108
Exportar logs ... 108
Trabalhar com snapshots e pontos de recuperação ... 119
Snapshots ... 120
Pontos de recuperação ... 123
Programação de snapshots ... 124
Cópia de backups para outra Região da AWS ... 127
Restaurar uma tabela ... 128
Uso da AWS Command Line Interface e da API do Amazon Redshift sem servidor ... 129

Compartilhar dados no Amazon Redshift Serverless ..... 132
Compartilhar dados no Amazon Redshift Serverless ..... 132
Visão geral dos recursos de marcação ..... 134
Clusters provisionados do Amazon Redshift ..... 136
Visão geral do do Amazon Redshift ..... 136
Clusters e nós ..... 137
Uso do EC2-VPC ao criar o cluster ..... 143
EC2-VPC ..... 143
EC2-Classic ..... 144
Executar um cluster ..... 144
Alarme padrão de espaço em disco ..... 145
Status do cluster ..... 146
Considerações sobre o uso de clusters provisionados do Amazon Redshift ..... 148
Considerações sobre região e zona de disponibilidade ..... 148
Manutenção do cluster ..... 149
Gerenciar limites de uso ..... 155
Atributos de rede compatíveis com os nós RA3 ..... 157
Tipos de nó ..... 158
Operações de cluster ..... 170
Redimensionar clusters ..... 170
Pausar e retomar clusters ..... 188
Renomeação de clusters ..... 190
Desativação e exclusão de clusters ..... 191
Realocar um cluster ..... 192
Snapshots e backups ..... 198
Configuração da implantação multi-AZ ..... 226
Configuração de uma implantação multi-AZ ..... 227
Gerenciar a implantação multi-AZ ..... 230
Failover da implantação multi-AZ ..... 238
Monitoramento de consultas para multi-AZ ..... 240
Gerenciamento de clusters usando o console ..... 242
Criar um cluster ..... 243
Criar cluster de visualização prévia ..... 247
Modificar um cluster ..... 248
Excluir um cluster ..... 249
Reinicialização de um cluster ..... 250

Redimensionamento de um cluster ... 251
Atualizar a versão de um cluster ... 251
Informações sobre a configuração de clusters ... 252
Obter uma visão geral do status de clusters ... 252
Criar um snapshot de um cluster ... 253
Criar ou editar um alarme de espaço em disco ... 253
Utilização dos dados de performance do cluster ... 253
Gerenciar clusters usando a AWS CLI e a API do Amazon Redshift ... 254
Gerenciamento de clusters em uma VPC ... 255
Visão geral ... 255
Criar um cluster em uma VPC ... 258
Gerenciar grupos de segurança da VPC de um cluster ... 259
Definir as configurações de comunicação do grupo de segurança para um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor ... 261
Como o Amazon Redshift funciona com o compartilhamento de VPC para recursos da AWS ... 264
Grupos de sub-rede de clusters ... 266
Histórico das versões de cluster ... 268
Trabalho com Integrações ETL zero ... 270
Considerações ... 272
Conceitos básicos das integrações ETL zero ... 274
Criar e configurar um data warehouse do Amazon Redshift de destino ... 275
Ative a diferenciação entre letras maiúsculas e minúsculas ... 277
Configurar a autorização no Amazon Redshift ... 279
Próximas etapas ... 283
Criar bancos de dados de destino ... 283
Criação de um banco de dados de destino no Amazon Redshift ... 284
Adicionar dados à origem ... 285
Consulta e criação de visões materializadas com dados replicados ... 286
Consulta de dados replicados no Amazon Redshift ... 286
Criação de visões materializadas com dados replicados ... 286
Gerenciamento de integrações ETL zero ... 288
Compartilhamento de dados no Amazon Redshift ... 290
Métricas para integrações ETL zero ... 292
Solução de problemas em integrações ETL zero ... 293
Consultar um banco de dados ... 303

Consultar um banco de dados usando o editor de consultas v2 do Amazon Redshift ..... 304
Configurar sua Conta da AWS ..... 305
Trabalhar com o editor de consultas v2 ..... 313
Interação com o SQL generativo do editor de consultas v2 (visualização) ..... 331
Carregar dados em um banco de dados ..... 339
Autorizar e executar consultas ..... 349
Autorizar e executar blocos de anotações ..... 355
Consulta ao AWS Glue Data Catalog ..... 359
Consultar um data lake ..... 363
Trabalho com unidades de compartilhamento de dados ..... 365
Programar uma consulta ..... 369
Visualizar resultados ..... 379
Compartilhar e trabalhar em equipe ..... 386
Consultar um banco de dados usando o Query Editor ..... 388
Considerações ..... 390
Habilitar o acesso ..... 390
Conectando-se com o editor de consultas ..... 392
Como usar o editor de consulta ..... 393
Programar uma consulta ..... 394
Conectar-se a um data warehouse usando ferramentas de cliente SQL ..... 399
Recomendações para conexão com ferramentas do cliente ..... 400
Configurar conexões no Amazon Redshift ..... 401
Configurar as opções de segurança para conexões ..... 578
Conexão de código e ferramentas clientes ..... 586
Conectar-se com SQL Workbench/J ..... 636
Conectar-se ao data warehouse de forma programática ..... 637
Usar um perfil de autenticação para se conectar ao Amazon Redshift ..... 637
Solução de problemas de conexão no Amazon Redshift ..... 640
Usar a API de dados ..... 649
Trabalhar com a API de dados ..... 649
Considerações ao chamar a API de dados ..... 650
Executar instruções SQL com um token de idempotência ..... 655
Autorizar acesso ..... 657
Chamar a API de dados ..... 664
Solução de problemas da API de dados ..... 689
Programar operações de API de dados com o Amazon EventBridge ..... 690

Monitorar a API de dados ... 694
Grupos de parâmetros ... 697
Visão geral ... 697
Sobre grupos de parâmetros ... 697
Valores de parâmetro padrão ... 698
Configurar valores de parâmetro usando a AWS CLI ... 700
Configurar o gerenciamento do workload ... 701
Propriedades dinâmicas e estáticas do WLM ... 702
Propriedades para o parâmetro wlm_json_configuration ... 702
Configurar o parâmetro wlm_json_configuration usando a AWS CLI ... 710
Gerenciamento de grupos de parâmetros usando o console ... 718
Criar um parameter group ... 718
Modificar um parameter group ... 719
Criação ou modificação de uma regra de monitoramento de consulta usando o console ... 722
Exclusão de um grupo de parâmetros ... 723
Associar um parameter group a um cluster ... 724
Gerenciar grupos de parâmetros usando a AWS CLI e a API do Amazon Redshift ... 724
Integração com um Parceiro da AWS ... 726
Integração de Parceiros da AWS usando o console do Amazon Redshift ... 726
Carregar dados com parceiros da AWS ... 728
Compra de nós reservados ... 729
Visão geral ... 729
Sobre as ofertas de nós reservados ... 730
Comparação das definições de preço entre as ofertas de nós reservados ... 731
Como os nós reservados funcionam ... 732
Nós reservados e faturamento consolidado ... 733
Exemplos de nós reservados ... 733
Comprar uma oferta de nó reservados com o console ... 735
Atualizar nós reservados com a AWS CLI ... 736
Comprar uma oferta de nó reservado usando a AWS CLI e a API do Amazon Redshift ... 737
Segurança ... 739
Proteção de dados ... 741
Criptografia de dados ... 742
Tokenização de dados ... 761
Privacidade do tráfego entre redes ... 761
Gerenciamento de identidade e acesso ... 762

Autenticando com identidades ... 763
Controle de acesso ... 766
Visão geral do gerenciamento de acesso ... 766
Usar políticas baseadas em identidade (políticas do IAM) ... 773
Federação de um provedor de identidades (IdP) nativo para o Amazon Redshift ... 831
Conectar o Redshift ao IAM Identity Center para proporcionar aos usuários uma experiência de logon único ... 836
Usar perfis vinculados ao serviço ... 852
Usar a autenticação do IAM para gerar credenciais do usuário do banco de dados ... 858
Autorizar o Amazon Redshift a acessar serviços da AWS ... 917
Gerenciamento das senhas de administrador do Amazon Redshift usando AWS Secrets Manager ... 953
Permissões necessárias para integração do AWS Secrets Manager ... 954
Troca do segredo da senha de administrador ... 954
Recuperação do nome do recurso da Amazon (ARN) do segredo no Amazon Redshift ... 955
Criar um segredo para credenciais de conexão de banco de dados ... 956
Considerações sobre como usar o AWS Secrets Manager com o Amazon Redshift ... 957
Registro e monitoramento ... 958
Registro em log da auditoria de banco de dados ... 958
Registrar em log com o CloudTrail ... 971
Validação de conformidade ... 983
Resiliência ... 985
Segurança da infraestrutura ... 985
Isolamento de rede ... 761
Grupos de segurança ... 987
Conectar usando um endpoint da interface da VPC ... 988
Análise de configuração e vulnerabilidade ... 994
Tarefas de rede ... 995
Usar um nome de domínio personalizado para conexões de clientes ... 995
Segurança para um nome de domínio personalizado ... 996
Configurar um nome de domínio personalizado ... 996
Trabalhando com endpoints da VPC gerenciados por Redshift ... 1006
Considerações ... 1007
Gerenciar endpoints usando o console do Redshift ... 1008
Gerenciar usando a AWS CLI ... 1010
Gerenciar usando operações de API do Amazon Redshift ... 1010

Gerenciamento usando o AWS CloudFormation ... 1011
Enhanced VPC routing ... 1011
Trabalhar com endpoints da VPC ... 1013
Enhanced VPC routing ... 1014
Redshift Spectrum e roteamento aprimorado de VPC ... 1016
Monitoramento da performance de cluster do ... 1021
Visão geral ... 1021
Dados de performance ... 1022
Métricas do Amazon Redshift ... 1023
Dimensões para métricas do Amazon Redshift ... 1034
Dados de performance de consulta e carga do Amazon Redshift ... 1036
Trabalhar com dados de performance ... 1037
Visualizar dados de performance do cluster ... 1038
Visualizar dados do histórico de consultas ... 1047
Visualizar dados de performance do banco de dados ... 1051
Visualizar dados de escalabilidade da simultaneidade e simultaneidade do workload ... 1054
Visualizar consultas e cargas ... 1056
Visualizar métricas do cluster durante as operações de carga ... 1061
Analisar a performance do workload ... 1062
Gerenciar alarmes ... 1064
Trabalhar com métricas de performance no console do CloudWatch ... 1065
Eventos ... 1067
Visão geral dos eventos de cluster ... 1067
Trabalhar com o Amazon Simple Notification Service ... 1068
Assinar notificações de eventos de cluster do Amazon Redshift ... 1069
Visualizar eventos de cluster usando o console ... 1071
Visualizar eventos de cluster usando a AWS CLI e a API do Amazon Redshift ... 1071
Gerenciar notificações de eventos de cluster ... 1071
Gerenciar notificações de eventos de cluster usando o console do Amazon Redshift ... 1072
Gerenciar notificações de eventos de cluster usando a AWS CLI e a API do Amazon Redshift ... 1072
Notificações de eventos do Amazon Redshift ... 1073
Categorias de eventos e mensagens de eventos do Amazon Redshift ... 1073
Notificações de eventos do Amazon Redshift sem servidor com o Amazon EventBridge ... 1096
Notificações de evento da integração ETL zero com o Amazon EventBridge ... 1104
Cotas e limites ... 1114

Cotas para objetos do Amazon Redshift ..... 1114
Cotas para objetos do Amazon Redshift Serverless ..... 1123
Cotas da API de dados do Amazon Redshift ..... 1125
Cotas para objetos do editor de consultas v2 ..... 1127
Cotas e limites para objetos do Amazon Redshift Spectrum ..... 1129
Restrições de nomenclatura ..... 1130
Tags ..... 1134
Visão geral da marcação ..... 1134
Requisitos de marcação ..... 1135
Gerenciamento de tags de recursos usando o console ..... 1136
Gerenciar etiquetas usando a API do Amazon Redshift ..... 1136
Versões do cluster ..... 1138
Patch 180 ..... 1138
Novos atributos ..... 1139
Patch 179 ..... 1140
Novos atributos ..... 1141
Patch 178 ..... 1142
Novos atributos ..... 1143
Patch 177 ..... 1145
Novos atributos ..... 1146
Patch 176 ..... 1147
Novos atributos ..... 1148
Patch 175 ..... 1149
Novos atributos ..... 1150
Patch 174 ..... 1150
Novos recursos para esta versão ..... 1150
Novos recursos para esta versão ..... 1150
Novos recursos para esta versão ..... 1150
Novos recursos para esta versão ..... 1150
Novos recursos para esta versão ..... 1150
Novos recursos para esta versão ..... 1150
Novos recursos para esta versão ..... 1150
Patch 173 ..... 1152
Novos recursos para esta versão ..... 1152
Novos recursos para esta versão ..... 1152
Novos recursos para esta versão ..... 1152

Novos recursos para esta versão ... 1152
Novos recursos para esta versão ... 1152
Novos recursos para esta versão ... 1152
Novos recursos para esta versão ... 1152
Novos recursos para esta versão ... 1152
Novos recursos para esta versão ... 1152
Novos recursos para esta versão ... 1152
Patch 172 ... 1153
Novos atributos ... 1154
Patch 171 ... 1154
Novos atributos ... 1155
Patch 170 ... 1155
Novos atributos ... 1155
Patch 169 ... 1155
Novos atributos ... 1156
Patch 168 ... 1156
Novos recursos ... 1156
Exemplos de código ... 1157
Ações ... 1159
Criar um cluster ... 1160
Criar uma tabela ... 1164
Excluir um cluster ... 1165
Descrever uma instrução de consulta ... 1169
Descrever clusters ... 1170
Obter o resultado da instrução ... 1176
Inserir dados em uma tabela ... 1177
Modificar um cluster ... 1179
Consultar uma tabela ... 1183
Cenários ... 1184
Conceitos básicos do Amazon Redshift ... 1184
Exemplos entre serviços ... 1198
Criar uma aplicação Web para rastrear dados do Amazon Redshift ... 1198
Histórico do documento ... 1200

# O que é o Amazon Redshift?

Boas-vindas ao Guia de gerenciamento de clusters do Amazon Redshift. O Amazon Redshift é um serviço de data warehouse totalmente gerenciado e em escala de petabytes na nuvem do . O Amazon Redshift sem servidor permite acessar e analisar dados sem todas as configurações de um data warehouse provisionado. Os recursos são provisionados automaticamente e a capacidade do data warehouse escala de maneira inteligente para oferecer performance rápida até mesmo às workloads mais exigentes e imprevisíveis. O tempo em que o data warehouse fica ocioso não é cobrado, portanto você paga apenas pelo que usa. Você pode carregar dados e começar a consultar imediatamente no editor de consultas v2 do Amazon Redshift ou na sua ferramenta de business intelligence (BI) favorita. Aproveite a melhor relação preço/performance e recursos de SQL familiares em um ambiente fácil de usar e que não exige administração.

Independentemente do tamanho do conjunto de dados, o Amazon Redshift oferece performance de consulta rápida usando as mesmas ferramentas baseadas em SQL e aplicações de business intelligence que você usa hoje.

## Você é um usuário iniciante do Amazon Redshift?

Se você for um usuário iniciante do Amazon Redshift, recomendamos que comece lendo as seguintes seções:

- Destaques do serviço e preço - Essa página de detalhes do produto mostra a proposta de valor, os destaques do serviço e o preço do Amazon Redshift.
- Conceitos básicos do Amazon Redshift sem servidor: este tópico apresenta o processo de configuração de um data warehouse com tecnologia sem servidor, criação de recursos e consulta de dados de amostra.
- Guia do desenvolvedor de banco de dados do Amazon Redshift – Se você é um desenvolvedor de banco de dados, este guia explica como projetar, construir, consultar e manter bancos de dados que compõem seu data warehouse.

Se você preferir gerenciar seus recursos do Amazon Redshift manualmente, poderá criar clusters provisionados para suas necessidades de consulta de dados. Para obter mais informações, consulte Clusters do Amazon Redshift.

Como desenvolvedor de aplicações, você pode usar a API do Amazon Redshift ou as bibliotecas do kit de desenvolvimento de software (SDK) da AWS para gerenciar clusters de maneira programática.

Se você usar a API do Amazon Redshift, deverá assinar cada solicitação HTTP ou HTTPS para a API para autenticá-la. Para obter mais informações sobre a assinatura de solicitações, acesse Assinatura de uma solicitação HTTP.

Para obter informações sobre a API, a CLI e os SDKs, acesse os seguintes links:

- Referência da API do Amazon Redshift sem servidor
- Referência da API do Amazon Redshift
- Referência da API de dados do Amazon Redshift
- Referência de comandos da AWS CLI
- Referências de SDK em Ferramentas para a Amazon Web Services.

## Visão geral dos recursos do Amazon Redshift Serverless

A maioria dos recursos compatíveis com um data warehouse provisionado do Amazon Redshift também é compatível com o Amazon Redshift Serverless. Veja a seguir alguns de seus principais recursos.

| Atributo | Descrição |
| --- | --- |
| Snapshots | É possível restaurar um snapshot do Amazon Redshift Serverless ou de um data warehouse provisionado para o Amazon Redshift Serverless. Para ter mais informações, consulte Trabalhar com snapshots e pontos de recuperação. |
| Pontos de recuperação | O Amazon Redshift Serverless cria automaticamente um ponto de recuperação a cada 30 minutos. Esses pontos de recuperação são mantidos por 24 horas. Você pode usá-los para restauração após gravações ou exclusões acidentais. Quando você restaura de um ponto de recuperação, todos os dados nos bancos de dados do Amazon Redshift Serverless são restaurados para um ponto anterior no tempo. Você também pode criar um snapshot a partir de um ponto de recuperação, caso precise manter um ponto de recuperação por um período mais longo. Para ter mais informações, consulte Trabalhar com snapshots e pontos de recuperação. |
| Capacidade base de RPU | Você pode definir uma capacidade base em unidades de processamento do Redshift (RPUs). Uma RPU fornece 16 GB de memória. Essa configuração oferece a capacidade de controlar o equilíbrio entre recursos em uso e custo |

| Atributo | Descrição |
| --- | --- |
| | para a workload. Você pode aumentar esse valor para ampliar os recursos disponíveis e melhorar a performance da consulta ou diminuir o valor para limitar seus gastos. O padrão é 128 RPUs. Você também pode definir limites de uso, como RPUs usadas por dia, para controlar os custos. Para ter mais informações, consulte Faturamento do Amazon Redshift Serverless. |
| Limites de uso do compartilhamento de dados | Você pode limitar a quantidade de dados transferidos de uma região de produtor para uma região de consumidor usando o console ou a API. Esses custos de transferência de dados diferem de acordo com a Região da AWS e são medidos em terabytes. Para obter mais informações sobre o compartilhamento de dados, consulte "Conceitos básicos sobre compartilhamento de dados usando o console" no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Funções definidas pelo usuário (UDFs) | É possível executar funções definidas pelo usuário (UDFs) no Amazon Redshift Serverless. Para obter mais informações, consulte Criar funções definidas pelo usuário no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Procedimentos armazenados | Você pode executar procedimentos armazenados no Amazon Redshift Serverless. Para obter mais informações, consulte Criar procedimentos armazenados no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Visualizações materializadas | Você pode criar visualizações materializadas no Amazon Redshift Serverless. Para obter mais informações, consulte Criar visualizações materializadas no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Funções espaciais | É possível executar funções espaciais no Amazon Redshift Serverless. Para obter informações, consulte Consultar dados espaciais no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Consultas federadas | Você pode executar consultas para unir dados com bancos de dados do Aurora e do Amazon RDS no Amazon Redshift Serverless. Para obter mais informações, consulte Consultar dados com consultas federadas no Guia do .de banco de dados do Amazon Redshift. |

| Atributo | Descrição |
| --- | --- |
| Consultas do data lake | É possível executar consultas para unir dados do data lake do Amazon S3 com o Amazon Redshift Serverless. Para obter mais informações, confira “Consultar um data lake” no Guia de gerenciamento de clusters do Amazon Redshift. |
| Log de HyperLogLog | Você pode executar funções HyperLogLog no Amazon Redshift Serverless. Para obter mais informações, consulte Usar esboços do HyperLogLog no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Consultar dados entre bancos de dados | Você pode consultar dados em bancos de dados com o Amazon Redshift Serverless. Para obter informações, consulte Consultar dados entre bancos de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Compartilhamento de dados | Você pode acessar unidades de compartilhamento de dados em data warehouses provisionados com o Amazon Redshift Serverless. Para obter informações, consulte Compartilhar dados entre clusters no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Consulta de dados semiestruturados | É possível ingerir e armazenar dados semiestruturados com o tipo de dados SUPER com o Amazon Redshift Serverless. Para obter informações, consulte Ingerir e consultar dados semiestruturados no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Marcar recursos | Você pode usar a AWS CLI ou a API do Amazon Redshift Serverless para marcar recursos com metadados relacionados ao recurso. Para obter mais informações, consulte Etiquetar recursos. |
| Machine learning | É possível usar o machine learning do Amazon Redshift com o Amazon Redshift Serverless. Para obter mais informações, consulte Usar machine learning no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Comandos e funções SQL | Com algumas exceções (como REBOOT_CLUSTER ), é possível usar comandos e funções SQL do Amazon Redshift com o Amazon Redshift Serverless. Para obter mais informações, consulte Referência de SQL no Guia do desenvolvedor de banco de dados do Amazon Redshift. |

| Atributo | Descrição |
| --- | --- |
| Recursos do CloudFormation | Usando modelos do CloudFormation, você pode implantar e atualizar recursos do Amazon Redshift Serverless. Essa integração significa que é possível gastar menos tempo gerenciando recursos para focar em seus aplicativos. Para obter mais informações sobre os recursos do CloudFormation no Amazon Redshift Serverless, consulte Referência do tipo de recurso do Amazon Redshift Serverless. |
| Recursos do CloudTrail | O Amazon Redshift sem servidor é integrado ao AWS CloudTrail para fornecer um registro das ações realizadas no Amazon Redshift sem servidor. O CloudTrail captura todas as chamadas de API para Amazon Redshift Serverless como eventos. Para obter mais informações, consulte "CloudTrail para o Amazon Redshift Serverless". |

# Visão geral dos clusters provisionados do Amazon Redshift

O serviço do Amazon Redshift gerencia todo o trabalho de configuração, operação e escalabilidade de um data warehouse. Essas tarefas incluem capacidade de provisionamento, monitoramento e backup do cluster e aplicação de patches e atualizações ao mecanismo Amazon Redshift.

O vídeo a seguir mostra como criar um cluster e consultar dados usando o editor de consultas do Amazon Redshift v2.

## Gerenciamento de clusters

Um cluster do Amazon Redshift é um conjunto de nós que consiste em um nó líder e um ou mais nós de computação. O tipo e o número de nós de computação que você precisa dependem do tamanho de seus dados, do número de consultas que você executará e da performance do runtime de consulta necessária.

### Criar e gerenciar clusters

Dependendo de suas necessidades de data warehousing, você pode começar com um cluster pequeno de nó único e facilmente escalar para um cluster maior de vários nós à medida que suas exigências mudam. Você pode adicionar ou remover nós de computação do cluster sem nenhuma interrupção no serviço. Para ter mais informações, consulte Clusters provisionados do Amazon Redshift.

### Reservar nós de computação

Se você pretende manter seu cluster em execução durante um ano ou mais, pode economizar reservando nós de computação para um período de um ano ou três anos. A reserva de nós de computação oferece economia significativa em comparação às taxas por hora que você paga quando provisiona nós de computação sob demanda. Para ter mais informações, consulte Comprar nós reservados do Amazon Redshift.

### Criar snapshots de cluster

Snapshots são backups pontuais de um cluster. Existem dois tipos de snapshots: automatizados e manuais. O Amazon Redshift armazena esses snapshots internamente no Amazon Simple Storage Service (Amazon S3) usando uma conexão Secure Sockets Layer (SSL) criptografada. Se você precisar restaurar a partir de um instantâneo, o Amazon Redshift cria um novo cluster e importa dados do snapshot que você especificar. Para obter mais informações sobre snapshots, consulte Snapshots e backups do Amazon Redshift.

## Segurança e acesso a clusters

Existem vários recursos relacionados ao acesso ao cluster e à segurança no Amazon Redshift. Esses recursos ajudam você a controlar o acesso ao seu cluster, definir regras de conectividade e criptografas dados e conexões. Esses recursos são adicionais aos recursos relacionados ao acesso ao banco de dados e à segurança no Amazon Redshift. Para obter mais informações sobre segurança de banco de dados, consulte Gerenciar segurança do banco de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift.

### Contas da AWS e credenciais do IAM

Por padrão, um cluster do Amazon Redshift é acessível apenas para a conta da AWS que cria o cluster. O cluster é bloqueado para que ninguém mais tenha acesso. Em sua conta da AWS, você usa o serviço AWS Identity and Access Management (IAM) para criar contas de usuário e gerenciar permissões para essas contas para controlar as operações de cluster. Para ter mais informações, consulte Segurança no Amazon Redshift. Para obter mais informações sobre o gerenciamento de identidades do IAM, incluindo orientação e práticas recomendadas para perfis do IAM, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift.

### Grupos de segurança

Por padrão, qualquer cluster que você criar é fechado para todos. As credenciais do IAM do controlam somente o acesso aos recursos relacionados à API do Amazon Redshift: o console do

Amazon Redshift, a interface de linha de comando (CLI), a API e o SDK. Para permitir acesso ao cluster a partir de ferramentas de cliente SQL via JDBC ou ODBC, você usa security groups:

- Se você estiver usando a plataforma EC2-VPC para seu cluster Amazon Redshift, você deve usar grupos de segurança da VPC. Recomendamos que você execute o cluster em uma plataforma EC2-VPC.

  Não será possível mover um cluster para uma VPC depois que ele for executado com a plataforma EC2-Classic. No entanto, você pode restaurar um snapshot EC2-Classic para um cluster EC2-VPC usando o console do Amazon Redshift. Para ter mais informações, consulte Restauração de um cluster usando um snapshot.
- Se você estiver usando a plataforma EC2-Classic para seu cluster Amazon Redshift, você deve usar grupos de segurança do Amazon Redshift.

Em ambos os casos, você adiciona regras ao grupo de segurança para conceder acesso de entrada explícito a um intervalo específico de endereços CIDR IP ou a um grupo de segurança do Amazon Elastic Compute Cloud (Amazon EC2) se seu cliente SQL for executado em uma instância do Amazon EC2. Para ter mais informações, consulte Grupos de segurança de clusters do Amazon Redshift.

Além das regras de acesso de entrada, você cria usuários do banco de dados para fornecer credenciais para autenticar o banco de dados no próprio cluster. Para obter mais informações, consulte Bancos de dados neste tópico.

## Criptografia

Quando você provisiona o cluster, opcionalmente, pode optar por criptografar o cluster para segurança adicional. Quando você habilitar a criptografia, o Amazon Redshift armazena todos os dados em tabelas criadas pelo usuário em um formato criptografado. Você pode usar o AWS Key Management Service (AWS KMS) para gerenciar suas chaves de criptografia do Amazon Redshift.

A criptografia é uma propriedade imutável do cluster. A única forma de mudar de um cluster criptografado para um cluster não criptografado é descarregar os dados e recarregá-los em um novo cluster. A criptografia aplica-se ao cluster e a todos os backups. Quando você restaura um cluster a partir de um snapshot criptografado, o novo cluster também é criptografado.

Para obter mais informações sobre a criptografia, chaves e módulos de segurança de hardware, consulte Criptografia de banco de dados do Amazon Redshift.

### Conexões SSL

Você pode usar criptografia de Secure Sockets Layer (SSL) para criptografar a conexão entre o cliente SQL e seu cluster. Para ter mais informações, consulte Configurar as opções de segurança para conexões.

## Monitoramento de clusters

Existem vários recursos relacionados ao monitoramento no Amazon Redshift. Você pode usar o registro em log de auditoria do banco de dados para gerar logs de atividades, configurar eventos e assinaturas de notificações para rastrear informações de seu interesse. Use as métricas no Amazon Redshift e no Amazon CloudWatch para saber sobre a integridade e a performance de seus clusters e bancos de dados.

### Registro em log da auditoria de banco de dados

Você pode usar o recurso de registro de auditoria do banco de dados para acompanhar informações sobre tentativas de autenticação, conexões, desconexões, alterar as definições de usuário do banco de dados e consultas executadas no banco de dados. Essas informações são úteis para fins de segurança e de solução de problemas no Amazon Redshift. Os logs são armazenados em buckets do Amazon S3. Para ter mais informações, consulte Registro em log da auditoria de banco de dados.

### Eventos e notificações

O Amazon Redshift rastreia eventos e retém informações sobre eles por um período de várias semanas em sua conta da AWS. Para cada evento, o Amazon Redshift registra informações como a data em que o evento ocorreu, uma descrição, a fonte do evento (por exemplo, um cluster, um grupo de parâmetros ou um snapshot) e a ID da fonte. Você pode criar assinaturas de notificação de eventos do Amazon Redshift que especificam um conjunto de filtros de eventos. Quando ocorre um evento que corresponde aos critérios do filtro, o Amazon Redshift usa o Amazon Simple Notification Service para informar que o evento ocorreu. Para obter mais informações sobre eventos e notificações, consulte Eventos do Amazon Redshift.

### Performance

O Amazon Redshift fornece dados e métricas de performance para que você possa rastrear a integridade e a performance de seus clusters e bancos de dados. O Amazon Redshift usa métricas do Amazon CloudWatch para monitorar os aspectos físicos do cluster, como utilização da CPU,

latência e taxa de transferência. O Amazon Redshift também fornece dados de performance de consulta e carga para ajudá-lo a monitorar a atividade do banco de dados em seu cluster. Para obter mais informações sobre métricas de performance e monitoramento, consulte Monitorar a performance do cluster do Amazon Redshift.

### Bancos de dados

O Amazon Redshift cria um banco de dados quando você provisiona um cluster. Este é o banco de dados que você usa para carregar dados e executar consultas em seus dados. Você pode criar bancos de dados adicionais executando um comando SQL, conforme necessário. Para obter mais informações sobre a criação de bancos de dados adicionais, vá para a Etapa 1: Criar um banco de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Ao provisionar um cluster, você especifica um usuário administrador que tem acesso a todos os bancos de dados criados no cluster. Este usuário administrados é um superusuário que é, inicialmente, o único usuário com acesso ao banco de dados, embora esse usuário possa criar outros superusuários e usuários. Para obter mais informações, acesse Superusuários e Usuários no Guia do desenvolvedor de banco de dados do Amazon Redshift.

O Amazon Redshift usa grupos de parâmetros para definir o comportamento de todos os bancos de dados em um cluster, como estilo de apresentação de data e precisão de ponto flutuante. Se você não especificar um grupo de parâmetros ao provisionar seu cluster, o Amazon Redshift associa um grupo de parâmetros padrão ao cluster. Para ter mais informações, consulte Grupos de parâmetros do Amazon Redshift.

Para obter mais informações sobre bancos de dados no Amazon Redshift, acesse o Guia do desenvolvedor de banco de dados do Amazon Redshift.

## Comparar o Amazon Redshift Serverless a um data warehouse provisionado do Amazon Redshift Serverless

Sobre o Amazon Redshift Serverless, alguns conceitos e recursos são diferentes dos recursos correspondentes de um data warehouse provisionado do Amazon Redshift. Por exemplo, uma comparação contrastante é que o Amazon Redshift Serverless não tem o conceito de cluster ou nó. A tabela a seguir descreve os recursos e o comportamento no Amazon Redshift Serverless e explica como eles diferem do recurso equivalente em um data warehouse provisionado.

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Grupo de trabalho e namespace | Para isolar workloads e gerenciar diferentes recursos no Amazon Redshift Serverless, você pode criar namespaces e grupos de trabalho para gerenciar recursos de armazenamento e computação separadamente. | Um namespace é um conjunto de objetos e usuários do banco de dados. Um grupo de trabalho é um conjunto de recursos de computação. Para obter mais informações, consulte Amazon Redshift sem servidor para entender o design do Amazon Redshift Serverless. | Um cluster provisionado é um conjunto de nós de computação e um nó líder, que você gerencia diretamente. Para ter mais informações, consulte Clusters provisionados do Amazon Redshift. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Tipos de nó | Ao trabalhar com o Amazon Redshift Serverless, você não seleciona tipos de nós nem especifica a contagem de nós como faz com um cluster provisionado do Amazon Redshift. | O Amazon Redshift Serverless provisiona e gerencia automaticamente a capacidade para você. Se preferir, você poderá especificar a capacidade inicial do data warehouse para selecionar o saldo de preço/performance correto para suas workloads. Você também pode especificar um máximo de horas | Você cria um cluster com tipos de nós que atendem às suas especificações de custo e performance. Para ter mais informações, consulte Clusters provisionados do Amazon Redshift. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | de RPU para definir controles de custos e garantir que os custos sejam previsíveis. Para ter mais informações, consulte Noções básicas sobre a capacidade do Amazon Redshift Serverless. | |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Gerenciamento da workload e escalabilidade simultânea | O Amazon Redshift pode ser escalado para períodos de carga pesada. O Amazon Redshift Serverless também pode ser escalado para atender a períodos intermitentes de alta carga. | O Amazon Redshift Serverless gerencia recursos automaticamente com eficiência e escala, com base em workloads, dentro dos limites dos controles de custo. Para ter mais informações, consulte Faturamento da capacidade computacional. | Com um data warehouse provisionado, você ativa a escalabilidade da simultaneidade em seu cluster para lidar com períodos de carga pesada. Para obter mais informações, consulte Escalabilidade da simultaneidade. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Porta | O número da porta usada para se conectar. | Com o Amazon Redshift sem servidor, você pode mudar para outra porta do intervalo de portas 5431–5455 ou 8191–8215. Para ter mais informações, consulte Conectar-se ao Amazon Redshift Serverless. | Com um data warehouse provisionado, você pode selecionar qualquer porta para conexão. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Redimensionar | Adicione ou remova recursos de computação para ter uma boa performance na workload. | O redimensionamento não é aplicável no Amazon Redshift Serverless. No entanto, você pode alterar a capacidade inicial de RPU do data warehouse, com base em seus requisitos de preço e performance. Para ter mais informações, consulte Noções básicas sobre a capacidade do Amazon | Com um cluster provisionado, você realiza o redimensionamento de um cluster para adicionar ou remover nós. Para obter mais informações, consulte "Visão geral do gerenciamento de clusters no Amazon Redshift". |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | Redshift Serverless. | |
| Pausar e reiniciar | Para economizar, será possível pausar um cluster provisionado quando não houver workloads para execução. | Com o Amazon Redshift Serverless, você só paga quando as consultas são executadas, portanto, não há necessidade de de pausar nem retomar. Para ter mais informações, consulte Faturamento da capacidade computacional. | Você pausa e retoma um cluster manualmente, com base em uma avaliação de sua workload em vários momentos. Para obter mais informações, consulte "Visão geral do gerenciamento de clusters no Amazon Redshift". |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Consultar dados externos com consultas do Spectrum | Você pode consultar dados nos buckets do Amazon S3, em vários formatos; por exemplo, JSON. | O faturamento é acumulado quando os recursos de computação processam workloads. Além disso, o faturamento é acumulado quando os dados do Redshift Spectrum são consultados, como qualquer outra transação. Para ter mais informações, consulte Faturamento da | Com um data warehouse provisionado, a capacidade do Amazon Redshift Spectrum existe em servidores separados que são consultados no cluster do Amazon Redshift. Para obter mais informações, confira “Consultar dados externos usando o Amazon Redshift Spectrum”. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | capacidade computacional. | |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Faturamento de recursos de computação | Como o faturamento é acumulado para o Amazon Redshift em comparação com o Amazon Redshift Serverless. | Com o Amazon Redshift Serverless, você paga pelas workloads executadas, em RPU-horas por segundo, com uma cobrança mínima de 60 segundos. Isso inclui consultas que acessam dados em formatos de arquivo abertos no Amazon S3. Para ter mais informações, consulte Faturamento da | Com um cluster provisionado, o faturamento ocorre por segundo quando o cluster não está pausado. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | capacidade computacional. | |
| Janela de manutenção | Como funciona a manutenção do servidor. | Não há janela de manutenção com o Amazon Redshift Serverless. As atualizações são gerenciadas com facilidade. Para obter mais informações, consulte "O que é o Amazon Redshift Serverless?". | Com um cluster provisionado, você especifica uma janela de manutenção quando ocorre aplicação de patch. (Normalmente, você escolhe um horário recorrente quando o uso é baixo.) |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Criptografia | Você pode ativar a criptografia do banco de dados. | O Amazon Redshift Serverless é sempre criptografado com o AWS KMS, com chaves gerenciadas pela AWS ou gerenciadas pelo cliente. | Os dados em um data warehouse provisionado podem ser criptografados com o AWS KMS (com chaves gerenciadas pela AWS ou gerenciadas pelo cliente) ou não criptografados. Consulte Criptografia de banco de dados do Amazon Redshift. |
| Faturamento de armazenamento | Como funciona o faturamento de armazenamento. | Para o Amazon Redshift Serverless. A taxa é calculada de acordo com a quantidade de GB por mês. Consulte Faturamento da capacidade computacional. | O armazenamento é cobrado além dos recursos de computação para um cluster provisionado com nós RA3. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Gerenciamento de usuários | Como os usuários são gerenciados. | Para um data warehouse provisionado e para o Amazon Redshift Serverless, os usuários são do IAM ou do Redshift. Para ter mais informações, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift Serverless.<br><br>Para obter mais informações sobre o gerenciamento de identidades do IAM, incluindo | |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | práticas recomendadas para perfis do IAM, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift. | |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Ferramentas e compatibilidade JDBC e ODBC | Como funcionam as conexões com os clientes. | Um data warehouse provisionando e o Amazon Redshift Serverless são compatíveis com qualquer ferramenta ou aplicação cliente compatível com JDBC ou ODBC. Para obter mais informações sobre drivers, consulte "Configurar conexões" no Guia de gerenciamento de clusters do Amazon Redshift. Para obter | |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | informações sobre como se conectar ao Amazon Redshift Serverless, consulte "Configurar conexões". | |
| Requisito de credenciais no login | Como as credenciais são processadas. | Para o Amazon Redshift Serverless, você não precisa inserir credenciais em todas as instâncias. Para ter mais informações, consulte Conectar-se ao Amazon Redshift Serverless. | O acesso ao Amazon Redshift exige credenciais de login de um usuário associado a um perfil do IAM. O perfil do IAM tem permissões específicas associadas a um data warehouse provisionado. Depois de autenticado, o usuário pode se conectar diretamente ao banco de dados, ao console do Redshift e ao editor de consultas v2. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Data API (API de dados) | Você pode acessar dados de serviços da Web e outras aplicações. | O Amazon Redshift Serverless é compatível com a API de dados do Amazon Redshift. Com o Amazon Redshift Serverless, é usado o parâmetro `workgroup-name` em vez de `cluster-identity`. Para obter mais informações sobre como chamar a API de dados, consulte Usar a API de dados | |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | Amazon Redshift. | |
| Snapshots | Oferece recuperação a um ponto anterior no tempo (PITR). | O Amazon Redshift Serverless é compatível com snapshots e pontos de recuperação. Para obter mais informações sobre snapshots e pontos de recuperação para um namespace, consulte Trabalhar com snapshots e pontos de recuperação. | Clusters provisionados são compatíveis com snapshots. Para obter mais informações, consulte “Gerenciamento de snapshots usando o console”. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Compartilhamento de dados | Oferece a possibilidade de compartilhar dados entre bancos de dados na mesma conta ou em contas diferentes. | O Amazon Redshift sem servidor é compatível com todos os recursos de compartilhamento de dados de um data warehouse provisionado. Também é compatível com o compartilhamento de dados entre o Amazon Redshift sem servidor e um data warehouse, uma ferramenta ou uma aplicação | Os clusters provisionados são compatíveis com o compartilhamento de dados entre bancos de dados, entre contas e do AWS Data Exchange. Para obter informações, consulte “Compartilhar dados entre clusters no Amazon Redshift”. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | cliente provision ada. | |
| Faixas | Fornece um cronogram a para atualizaç ões de software. | O Amazon Redshift Serverles s não tem conceito de faixa. As versões e as atualizaç ões são gerenciad as pelo serviço. Para obter mais informaçõ es sobre o design do Amazon Redshift Serverles s, consulte Trabalhar com snapshots e pontos de recuperaç ão. | Os clusters provisionados comportam a alternância entre faixas atuais e posteriores. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Tabelas e visualizações de sistema | Oferece uma forma de monitorar seus recursos e os metadados do sistema. | O Amazon Redshift sem servidor comporta novas tabelas e visualizações do sistema. Para obter mais informações sobre tabelas de sistema, consulte Visualizações de monitoramento. Para obter informações sobre como migrar consultas do uso das tabelas e visualizações do sistema provision | Um data warehouse provisionado é compatível com o conjunto existente de tabelas e visualizações do sistema para monitoramento e outras tarefas que exigem metadados do sistema. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | ado mais antigas para as novas exibições, consulte Migração para visualizações de monitoramento de SYS. | |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Grupos de parâmetros | Esse é um grupo de parâmetros que se aplica a todos os bancos de dados criados em um cluster. Esses parâmetros definem as configurações do banco de dados, como tempo limite de consulta e estilo de data. | O Amazon Redshift Serverless não tem o conceito de grupo de parâmetros. | Os data warehouses provisionados são compatíveis com grupos de parâmetros. Para obter mais informações sobre grupos de parâmetros para um cluster provisionado, consulte Grupos de parâmetros do Amazon Redshift. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Monitoramento de consultas | Oferece uma visão baseada no tempo das consultas executadas. | O monitoramento de consultas no Amazon Redshift Serverless exige que os usuários se conectem ao banco de dados para usar tabelas do sistema. Dessa forma, o monitoramento de consultas e as tabelas do sistema ficam em sincronia. As consultas de tabelas do sistema para o Amazon Redshift Serverles | O monitoramento de consultas em clusters provisionados não mostra todos os dados nas tabelas do sistema. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | s usam o usuário do banco de dados mapeado para o usuário do IAM a fim de utilizar o monitoramento de consultas. Para obter mais informações sobre monitoramento de consultas, consulte "Monitorar consultas e workloads com o Amazon Redshift Serverless". | |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Registro em log de auditoria | Fornece informações sobre conexões e atividades do usuário no banco de dados. | Com o Amazon Redshift Serverless, o CloudWatch é um destino para logs de auditoria. A entrega de logs de auditoria com base no Amazon S3 não é compatível com o Amazon Redshift Serverless. Para obter mais informações, consulte “Registro de auditoria para o Amazon Redshift | Para um cluster provisionado, a entrega de log de auditoria com base no Amazon S3 tem sido a norma. Agora, a entrega de logs de auditoria para o CloudWatch é estendida para cobrir também data warehouses provisionados. |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | Serverless”. | |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| Notificações de eventos | O Amazon EventBridge é um serviço de barramento de eventos com tecnologia sem servidor que você pode usar para conectar suas aplicações com dados de eventos de diversas origens. | O Amazon Redshift Serverless usa o Amazon EventBridge para gerenciar notificações de eventos a fim de manter você atualizado em relação às alterações no data warehouse. Para ter mais informações, consulte Notificações de eventos do Amazon Redshift sem servidor com o | Para um cluster provisionado, você gerencia notificações de eventos usando o console do Amazon Redshift para criar assinaturas de eventos. Para ter mais informações, consulte Gerenciar notificações de eventos de cluster . |

| Atributo | Descrição | Sem servidor | Provisionada |
| --- | --- | --- | --- |
| | | Amazon EventBridge. | |

# Usar as interfaces de gerenciamento do Amazon Redshift para clusters provisionados

> **Note**
>
> Este tópico aborda as interfaces de gerenciamento do Amazon Redshift para clusters provisionados. Existem interfaces de gerenciamento semelhantes para o Amazon Redshift sem servidor e a API de dados do Amazon Redshift.

O Amazon Redshift dá suporte a diversas interfaces de gerenciamento que você pode usar para criar, gerenciar e excluir clusters do Amazon Redshift: as SDKs do AWS, o AWS Command Line Interface (AWS CLI) e a API de gerenciamento do Amazon Redshift.

A API do Amazon Redshift — Você pode chamar essa API de gerenciamento do Amazon Redshift enviando uma solicitação. Elas são solicitações HTTP ou HTTPS que usam os verbos HTTP `GET` ou `POST` com um parâmetro chamado `Action`. Chamar a API do Amazon Redshift é a maneira mais direta de acessar o serviço Amazon Redshift. No entanto, isso exige que seu aplicativo manipule detalhes de baixo nível, como gerenciamento de erros e geração de um hash para assinar a solicitação.

- Para obter informações sobre como construir e assinar uma solicitação de API do Amazon Redshift, Assinatura de uma solicitação HTTP.
- Para obter informações sobre as ações da API do Amazon Redshift e os tipos de dados para o Amazon Redshift, consulte a Referência da API do Amazon Redshift.

SDKs da AWS – Você pode usar os SDKs da AWS para executar as operações relacionadas ao cluster do Amazon Redshift. Várias das bibliotecas do SDK envolvem a API do Amazon Redshift subjacente. Elas integram a funcionalidade de API na linguagem de programação específica e

processam muitos dos detalhes de nível inferior, como calcular assinaturas, processar novas tentativas de solicitação e tratamento de erros. Chamar as funções wrapper nas bibliotecas do SDK pode simplificar muito o processo de escrever uma aplicação para gerenciar um cluster do Amazon Redshift.

- O Amazon Redshift é compatível com os AWS SDKs for Java, .NET, PHP, Python, Ruby e Node.js. As funções wrapper para Amazon Redshift estão documentadas no manual de referência de cada SDK. Para obter uma lista dos SDKs da AWS e links para a documentação, consulte Ferramentas para Amazon Web Services.
- Este guia fornece exemplos de como trabalhar com o Amazon Redshift usando o Java SDK. Para obter exemplos mais gerais de código de SDK da AWS, consulte Exemplos de código para o Amazon Redshift usando SDKs da AWS.

AWS CLI – A CLI fornece um conjunto de ferramentas da linha de comando que você pode usar para gerenciar serviços da AWS em computadores com Windows, Mac e Linux. A AWS CLI inclui comandos baseados nas ações da API do Amazon Redshift.

- Para obter informações sobre como instalar e configurar a CLI do Amazon Redshift, consulte Configurar a CLI do Amazon Redshift.
- Para obter material de referência sobre os comandos da CLI do Amazon Redshift, consulte Amazon Redshift no Referência da AWS CLI.

## Usar este serviço com um AWS SDK

Os kits de desenvolvimento de software (SDKs) da AWS estão disponíveis para muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que facilitam a criação de aplicações em seu idioma preferido pelos desenvolvedores.

| Documentação do SDK | Exemplos de código |
| --- | --- |
| AWS SDK for C++ | Exemplos de código do AWS SDK for C++ |
| AWS SDK for Go | Exemplos de código do AWS SDK for Go |
| AWS SDK for Java | Exemplos de código do AWS SDK for Java |

| Documentação do SDK | Exemplos de código |
| --- | --- |
| AWS SDK for JavaScript | Exemplos de código do AWS SDK for JavaScript |
| AWS SDK para Kotlin | Exemplos de código do AWS SDK para Kotlin |
| AWS SDK for .NET | Exemplos de código do AWS SDK for .NET |
| AWS SDK for PHP | Exemplos de código do AWS SDK for PHP |
| AWS SDK for Python (Boto3) | Exemplos de código do AWS SDK for Python (Boto3) |
| AWS SDK for Ruby | Exemplos de código do AWS SDK for Ruby |
| AWS SDK para Rust | Exemplos de código do AWS SDK para Rust |
| SDK da AWS para SAP ABAP | Exemplos de código do SDK da AWS para SAP ABAP |
| AWS SDK for Swift | Exemplos de código do AWS SDK for Swift |

Exemplo de disponibilidade

Você não consegue encontrar o que precisa? Solicite um código de exemplo no link Fornecer feedback na parte inferior desta página.

## Assinatura de uma solicitação HTTP

O Amazon Redshift exige que todas as solicitações que você envia para a API de gerenciamento sejam autenticadas com uma assinatura. Este tópico explica como assinar suas solicitações.

Se você estiver usando um dos Kits de Desenvolvimento de Software (SDKs) da AWS ou a AWS Command Line Interface, a assinatura da solicitação é tratada automaticamente e você pode pular esta seção. Para obter mais informações sobre como usar os SDKs da AWS, consulte Usar as interfaces de gerenciamento do Amazon Redshift para clusters provisionados. Para obter

mais informações sobre como usar a interface da linha de comando do Amazon Redshift, acesse Referência da linha de comando do Amazon Redshift.

Para assinar uma solicitação, calcule uma assinatura digital usando a função de hash criptográfico. Um hash criptográfico é uma função que retorna um valor de hash exclusivo que é baseado na entrada. A entrada da função de hash inclui o texto da solicitação e a chave de acesso secreta que é possível obter nas credenciais temporárias. A função de hash retorna um valor de hash que você inclui na solicitação como sua assinatura. A assinatura é parte do cabeçalho `Authorization` de sua solicitação.

**Note**

Os usuários precisam de acesso programático se quiserem interagir com a AWS de fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando a AWS.
Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| Identificação da força de trabalho<br><br>(Usuários gerenciados no Centro de Identidade do IAM) | Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções da interface que deseja utilizar.<br><br>• Para a AWS CLI, consulte Configuração da AWS CLI para usar o AWS IAM Identity Center no AWS Command Line InterfaceGuia do usuário da .<br>• Para os SDKs da AWS, ferramentas e APIs da AWS, consulte Autenticação do Centro de Identidade do IAM no Guia de referência de |

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| | | ferramentas e SDKs da AWS. |
| IAM | Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções em Como usar credenciais temporárias com recursos da AWS no Guia do usuário do IAM. |
| IAM | (Não recomendado) Use credenciais de longo prazo para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções da interface que deseja utilizar.<br>• Para a AWS CLI, consulte Autenticação usando as credenciais de usuário do IAM no Guia do usuário da AWS Command Line Interface.<br>• Para as ferramentas e SDKs da AWS, consulte Autenticação usando as credenciais de longo prazo no Guia de referência de ferramentas e SDKs da AWS.<br>• Para as APIs da AWS, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM. |

Depois que o Amazon Redshift recebe a solicitação, ele recalcula a assinatura usando a mesma função de hash e a mesma entrada que você usou para assinar a solicitação. Se a assinatura

resultante corresponde à assinatura na solicitação, o Amazon Redshift processa a solicitação; caso contrário, a solicitação é rejeitada.

O Amazon Redshift oferece suporte à autenticação usando a assinatura versão 4 da AWS. O processo para cálculo de uma assinatura é composto de três tarefas. Essas tarefas são ilustradas no exemplo a seguir.

- Tarefa 1: Criar uma solicitação canônica

  Reorganize sua solicitação HTTP em um formato canônico. O uso de um formulário canônico é necessário porque o Amazon Redshift usa o mesmo formulário canônico para calcular a assinatura que compara com a que você enviou.
- Tarefa 2: Criar uma string para assinar

  Crie uma string que será usada como um dos valores de entrada para sua função hash criptográfica. A string, chamada string-to-sign, é uma concatenação do nome do algoritmo hash, da data da solicitação, de uma string do escopo da credencial e da solicitação canonizada da tarefa anterior. A string do escopo credencial em si é uma concatenação da data, da região e de informações do serviço.
- Tarefa 3: calcular uma assinatura

  Calcule uma assinatura para sua solicitação usando uma função hash criptográfica que aceite duas strings de entrada, sua string para assinar e uma chave derivada. A chave derivada é calculada começando com sua chave de acesso secreta e usando a string do escopo da credencial para criar uma série de códigos de autenticação de mensagem baseados em hash (HMAC-SHA256).

## Exemplo de cálculo de assinatura

O exemplo a seguir mostra os detalhes da criação de uma assinatura para a solicitação CreateCluster. Você pode usar este exemplo como uma referência para verificar seu próprio método de cálculo de assinatura. Outros cálculos de referência estão incluídos na seção Exemplos de assinatura de solicitação do Guia do usuário do IAM.

Você pode usar uma solicitação GET ou POST para enviar solicitações ao Amazon Redshift. A diferença entre as duas é que, para a solicitação GET, seus parâmetros são enviados como parâmetros de string de consulta. Para a solicitação POST, eles são incluídos no corpo da solicitação. O exemplo abaixo mostra uma solicitação POST.

O exemplo supõe o seguinte:

- O timestamp da solicitação é `Fri, 07 Dec 2012 00:00:00 GMT`.
- O endpoint é a região Leste dos EUA (Norte da Virgínia), `us-east-1`.

A sintaxe geral da solicitação é:

```
https://redshift.us-east-1.amazonaws.com/
   ?Action=CreateCluster
   &ClusterIdentifier=examplecluster
   &MasterUsername=masteruser
   &MasterUserPassword=12345678Aa
   &NumberOfNode=2
   &NodeType=ds2.xlarge
   &Version=2012-12-01
   &x-amz-algorithm=AWS4-HMAC-SHA256
   &x-amz-credential=AKIAIOSFODNN7EXAMPLE/20121207/us-east-1/redshift/aws4_request
   &x-amz-date=20121207T000000Z
   &x-amz-signedheaders=content-type;host;x-amz-date
```

O formato canônico da solicitação calculada para Tarefa 1: Crie uma solicitação canônica é:

```
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
```

A última linha da solicitação canônica é o hash do corpo da solicitação. A terceira linha na solicitação canônica está vazia, pois não há parâmetros de consulta para esta API.

A string-to-sign para Tarefa 2: Crie uma string-to-sign é:

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

```
06b6bef4f4f060a5558b60c627cc6c5b5b5a959b9902b5ac2187be80cbac0714
```

A primeira linha da string-to-sign é o algoritmo, a segunda linha é a time stamp, a terceira linha é o escopo da credencial e a última linha é o hash da solicitação canônica da Tarefa 1: Crie uma solicitação canônica. O nome do serviço a usar no escopo da credencial é `redshift`.

Para a Tarefa 3: calcular uma assinatura, a chave derivada pode ser representada como:

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

A chave derivada é calculada como uma série de funções de hash. Partindo de instrução interna de HMAC na fórmula acima, você concatena a frase **`AWS4`** com sua chave de acesso secreta e a utiliza como a chave para fazer hash dos dados “us-east-1”. O resultado desse hash se torna a chave para a próxima função de hash.

Após o cálculo da chave derivada, você a utiliza em uma função de hash que aceita duas strings de entrada, a sua string-to-sign e a chave derivada. Por exemplo, se você usar a chave de acesso secreta `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY` e a string-to-sign fornecida anteriormente, a assinatura calculada será como se segue:

```
9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

A etapa final é construir o cabeçalho `Authorization`. Para a chave de acesso de demonstração `AKIAIOSFODNN7EXAMPLE`, o cabeçalho (com quebras de linha adicionadas por motivo de legibilidade) é:

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

## Configurar a CLI do Amazon Redshift

Esta seção explica como configurar e executar as ferramentas da linha de comando AWS CLI para uso no gerenciamento do Amazon Redshift. As ferramentas da linha de comando do Amazon Redshift são executadas na AWS Command Line Interface (AWS CLI), que por sua vez usa Python (https://www.python.org/). A AWS CLI pode ser executada em qualquer sistema operacional compatível com Python.

## Instruções de instalação

Para começar a usar as ferramentas da linha de comando do Amazon Redshift, primeiro configure a AWS CLI e, em seguida, adicione os arquivos de configuração que definem as opções de CLI do Amazon Redshift.

Se tiver instalado e configurado a AWS CLI para outro serviço da AWS, poderá ignorar esse procedimento.

Para instalar o AWS Command Line Interface

1. Acesse Install or update to the latest version of the AWS CLI e siga as instruções para instalar a AWS CLI.

   Para acesso à CLI, você precisa de um ID de chave de acesso e de uma chave de acesso secreta. Use credenciais temporárias em vez de chaves de acesso de longo prazo quando possível. As credenciais temporárias incluem um ID de acesso, uma chave de acesso secreta e um token de segurança que indica quando as credenciais expiram. Para obter mais informações, consulte Usar credenciais temporárias com recursos da AWS no Guia do usuário do IAM.
2. Crie um arquivo contendo informações de configuração, como as chaves de acesso, a região padrão e o formato de saída do comando. Em seguida, defina a variável de ambiente `AWS_CONFIG_FILE` para referenciar esse arquivo. Para obter instruções detalhadas, vá para Configurando a interface da linha de comando da AWS no Manual do usuário da AWS Command Line Interface.
3. Execute um comando de teste para confirmar se a interface da AWS CLI está funcionando. Por exemplo, o seguinte comando deve exibir informações de ajuda da AWS CLI:

   ```
   aws help
   ```

   O seguinte comando deve exibir informações de ajuda para Amazon Redshift:

   ```
   aws redshift help
   ```

Para obter material de referência sobre os comandos da CLI do Amazon Redshift, acesse Amazon Redshift em Referência da AWS CLI.

# Amazon Redshift sem servidor

Com o Amazon Redshift Serverless, você tem a comodidade de executar e escalar análises sem precisar provisionar e gerenciar data warehouses. Com o Amazon Redshift Serverless, os analistas de dados, desenvolvedores e cientistas de dados agora podem usar o Amazon Redshift para obter insights de dados em segundos, carregando dados em registros de consulta do data warehouse. O Amazon Redshift provisiona e escala automaticamente a capacidade do data warehouse garantindo uma performance rápida para workloads exigentes e imprevisíveis. Você só paga pela capacidade utilizada. Você pode aproveitar essa simplicidade sem fazer alterações em suas aplicações de análise e business intelligence existentes.

## O que é o Amazon Redshift Serverless?

O Amazon Redshift Serverless provisiona automaticamente a capacidade do data warehouse e escala os recursos subjacentes de modo inteligente. O Amazon Redshift Serverless ajusta a capacidade em segundos para oferecer alta performance consistentemente e operações simplificadas até mesmo para as workloads mais exigentes e voláteis.

Com o Amazon Redshift Serverless, você se beneficia dos seguintes recursos:

- Acesse e analise dados sem a necessidade de configurar, ajustar e gerenciar clusters provisionados do Amazon Redshift.
- Use os recursos superiores do SQL do Amazon Redshift, a performance líder do setor e a integração de data lake para consultar perfeitamente um data warehouse, um data lake e as fontes de dados operacionais.
- Ofereça alta performance consistentemente e operações simplificadas mesmo para as workloads mais exigentes e voláteis com escalabilidade automática e inteligente.
- Use grupos de trabalho e namespaces para organizar recursos de computação e dados com controles de custo granulares.
- Pague somente enquanto o data warehouse estiver em uso.

Com o Amazon Redshift Serverless, você usa uma interface de console para acessar um data warehouse sem servidor ou APIs para criar aplicações. Pelo data warehouse, é possível acessar o armazenamento gerenciado do Amazon Redshift e seu data lake do Amazon S3.

Este vídeo mostra como o Amazon Redshift Serverless facilita a execução e escala análises sem precisar gerenciar clusters de data warehouse:

## Console do Amazon Redshift Serverless

Para começar a usar o console do Amazon Redshift sem servidor, assista ao seguinte vídeo: Conceitos básicos do Amazon Redshift.

### Painel sem servidor

No painel sem servidor, é possível ver um resumo de seus recursos e gráficos de seu uso.

- Namespace overview (Visão geral do namespace): essa seção mostra a quantidade de snapshots e unidades de compartilhamento de dados no namespace.
- Workgroups (Grupos de trabalho): essa seção mostra todos os grupos de trabalho no Amazon Redshift Serverless.
- Query metrics (Métricas de consulta): essa seção mostra a atividade de consulta da última hora.
- RPU capacity used (Capacidade de RPU utilizada) essa seção mostra a capacidade usada na última hora.
- Free trial (Teste gratuito): essa seção mostra os créditos de teste gratuito restantes em sua conta da AWS. Isso abrange todo uso de recursos e operações do Amazon Redshift Serverless, incluindo snapshots, armazenamento, grupo de trabalho e assim por diante, na mesma conta.
- Alarms (Alarmes): essa seção mostra os alarmes que você configurou no Amazon Redshift Serverless.

### Backup de dados

Na guia Data backup (Backup de dados), você pode trabalhar com o seguinte:

- Snapshots: é possível criar, excluir e gerenciar snapshots dos dados do Amazon Redshift Serverless. O período de retenção padrão é `indefinitely`, mas você pode configurá-lo como qualquer valor entre 1 e 3653 dias. Você pode autorizar Contas da AWS para restaurar namespaces de um snapshot.
- Recovery points (Pontos de recuperação): exibe os pontos de recuperação criados automaticamente para que você possa se recuperar de uma gravação ou exclusão acidental feita nas últimas 24 horas. Para recuperar dados, você pode restaurar um ponto de recuperação para qualquer namespace disponível. Você pode criar um snapshot com base em um ponto de

recuperação, caso queira manter um ponto de recuperação por um período de tempo mais longo. O período de retenção padrão é `indefinitely`, mas você pode configurá-lo como qualquer valor entre 1 e 3653 dias.

### Acesso aos dados

Na guia Data access (Acesso aos dados), você pode trabalhar com o seguinte:

- Configurações de Network and security (Rede e segurança): você pode visualizar valores relacionados à VPC, valores de criptografia do AWS KMS e valores de registro em log de auditoria. Você só pode atualizar o registro em log de auditoria. Para obter mais informações sobre como definir configurações de rede e segurança usando o console, consulte Gerenciar limites de uso, limites de consulta e outras tarefas administrativas.
- AWS KMS key: a AWS KMS key usada para criptografar recursos no Amazon Redshift Serverless.
- Permissions (Permissões): gerencie as funções do IAM que o Amazon Redshift Serverless pode assumir para usar recursos em seu nome. Para obter mais informações, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift Serverless.
- Redshift-managed VPC endpoints (Endpoints da VPC gerenciados pelo Redshift): é possível acessar a instância do Amazon Redshift Serverless por outra VPC ou sub-rede. Para ter mais informações, consulte Conectar-se ao Amazon Redshift Serverless de outros endpoints da VPC.

### Limites

Na guia Limits (Limites), você pode trabalhar com o seguinte:

- Configurações de Base capacity in Redshift processing units (RPUs) (Capacidade básica em unidades de processamento do Redshift (RPUs)): defina a capacidade básica usada para processar sua workload. Para melhorar a performance da consulta, aumente o valor da RPU.
- Usage limits (Limites de uso): o máximo de recursos computacionais que a instância do Amazon Redshift Serverless pode usar em determinado período antes que uma ação seja iniciada. Você limita a quantidade de recursos que o Amazon Redshift Serverless usa para executar a workload. O uso é medido em horas de unidades de processamento do Redshift (RPUs). Uma hora de RPU é o número de RPUs usadas em uma hora. Você determina uma ação que deverá ocorrer quando atingir um limite definido, da seguinte maneira:
  - Envie um alerta.
  - Registre uma entrada em uma tabela do sistema.

- Desative as consultas do usuário.

É possível configurar até quatro limites.

- Query limits (Limites de consulta): você pode adicionar um limite para monitorar a performance e os limites. Para obter mais informações sobre os limites de monitoramento de consultas, consulte Regras de monitoramento de consultas do WLM.

Para ter mais informações, consulte Noções básicas sobre a capacidade do Amazon Redshift Serverless.

Unidades de compartilhamento de dados

Na guia Datashares (Unidades de compartilhamento de dados), é possível trabalhar com o seguinte:

- Configurações de Datashares created in my namespace (Unidades de compartilhamento de dados criadas no meu namespace): você pode criar uma unidade de compartilhamento de dados e compartilhá-la com outros namespaces e Contas da AWS.
- Datashares from other namespaces and Contas da AWS (Unidade de compartilhamento de dados de outros namespaces e ) - é possível criar um banco de dados de uma unidade de compartilhamento de dados de outro namespace e de outras Contas da AWS.

Para obter mais informações sobre compartilhamento de dados, consulte Compartilhar dados no Amazon Redshift Serverless.

Monitoramento de consultas e bancos de dados

Na página Query and database monitoring (Monitoramento de consultas e bancos de dados), você visualiza grafos do histórico de consultas da performance do banco de dados.

Na guia Query history (Histórico de consultas) você visualiza os gráficos a seguir. É possível escolher entre Query list (Lista de consultas) e Resource metrics (Métricas de recursos):

- Query runtime (Tempo de execução da consulta): esse gráfico mostra quais consultas estão sendo executadas no mesmo período. Escolha uma barra do grafo para visualizar mais detalhes de execução de consulta.
- Queries and loads (Consultas e cargas): essa seção lista consultas e cargas por ID da consulta.
- RPU capacity used (Capacidade de RPU utilizada): esse gráfico mostra a capacidade geral em unidades de processamento do Redshift (RPUs).

- Database connections (Conexões de banco de dados): esse grafo mostra o número de conexões de banco de dados ativas.

### Performance do banco de dados

Na guia Database performance (Performance do banco de dados), você verá os seguintes gráficos:

- Queries completed per second (Consultas concluídas por segundo): esse grafo mostra o número médio de consultas concluídas por segundo.
- Queries duration (Duração das consultas): o tempo médio para concluir uma consulta.
- Database connections (Conexões de banco de dados): esse grafo mostra o número de conexões de banco de dados ativas.
- Running queries (Consultas em execução): esse grafo mostra o número total de consultas em execução em determinado momento.
- Queued queries (Consultas na fila): esse grafo mostra o número total de consultas na fila em determinado momento.
- Query run time breakdown (Detalhamento do tempo de execução da consulta): esse gráfico mostra o tempo total que as consultas gastam em execução por tipo de consulta.

### Monitoramento de recursos

Na Resource monitoring (Monitorar recursos), é possível visualizar gráficos dos recursos consumidos. É possível filtrar os dados com base em várias facetas.

- Metric filter (Filtro de métrica): você pode usar filtros de métrica a fim de selecionar filtros para um grupo de trabalho específico, bem como escolher o limite de tempo e o intervalo de tempo.
- RPU capacity used (Capacidade de RPU utilizada): esse gráfico mostra a capacidade geral em unidades de processamento do Redshift (RPUs).
- Uso de computação: este gráfico mostra o uso acumulativo de horas de RPU por período para o intervalo de tempo selecionado. Para intervalos de tempo inferiores a seis horas, as horas de RPU são mostradas na hora exata. Para intervalos de tempo de seis horas ou mais, as horas de RPU são mostradas como médias.

Na página Datashares (Unidades de compartilhamento de dados), você pode gerenciar unidades de compartilhamento de dados In my account (Em minha conta) e From other accounts (De outras

contas). Para obter mais informações sobre compartilhamento de dados, consulte Compartilhar dados no Amazon Redshift Serverless.

## Considerações ao usar o Amazon Redshift Serverless

Para obter uma lista de Regiões da AWS nas quais o Amazon Redshift sem servidor está disponível, consulte os endpoints listados para a API do Redshift sem servidor na Referência geral da Amazon Web Services.

Alguns recursos usados pelo Amazon Redshift Serverless estão sujeitos a cotas. Para obter mais informações, consulte Cotas para objetos do Amazon Redshift Serverless.

Quando você DECLARA um cursor, as especificações de tamanho do conjunto de resultados para o Amazon Redshift Serverless são especificadas em DECLARE.

Janela de manutenção: não há janela de manutenção com o Amazon Redshift Serverless. As atualizações de versão do software são aplicadas automaticamente. Não há interrupção para conexão ou execução de consulta existente quando o Amazon Redshift alterna as versões. Novas conexões sempre se conectarão e funcionarão com o Amazon Redshift Serverless instantaneamente.

IDs da zona de disponibilidade: ao configurar a instância do Amazon Redshift Serverless, abra Additional considerations (Considerações adicionais) e verifique se os IDs de sub-rede fornecidos em Subnet (Sub-rede) contêm pelo menos três dos IDs de zona de disponibilidade compatíveis. Para ver a sub-rede para mapeamento de ID da zona de disponibilidade, acesse o console da VPC e escolha Subnets (Sub-redes) para ver a lista de IDs de sub-rede com seus IDs de zona de disponibilidade. Verifique se sua sub-rede está mapeada para um ID de zona de disponibilidade compatível. Para criar uma sub-rede, consulte Criar uma sub-rede na VPC no Guia do usuário do Amazon VPC.

Três sub-redes: você deve ter pelo menos três sub-redes, e elas devem abranger três zonas de disponibilidade. Por exemplo, é possível usar três sub-redes mapeadas para as zonas de disponibilidade us-east-1a, us-east-1b e us-east-1c. Uma exceção a isso é a região Oeste dos EUA (N. da Califórnia). Ela exige três sub-redes, da mesma forma que as outras regiões, mas elas devem abranger apenas duas zonas de disponibilidade. Uma condição é que uma das zonas de disponibilidade abrangidas contenha duas sub-redes.

Requisitos de endereço IP gratuito: você deve ter endereços IP gratuitos disponíveis ao criar um grupo de trabalho do Amazon Redshift sem servidor. O número mínimo de endereços IP aumenta à medida que o número de unidades de processamento do Redshift (RPUs) para o grupo de trabalho aumenta. Especificamente, cada sub-rede na VPC do grupo de trabalho exige um número

mínimo de endereços IP. Para obter mais informações sobre como alocar endereços IP, consulte Endereçamento IP no Guia do usuário do Amazon VPC.

Os números mínimos de endereços IP gratuitos necessários ao criar um grupo de trabalho são os seguintes:

Número de endereços IP gratuitos necessários para cada sub-rede

| Unidades de processamento do Redshift (RPUs) | Endereços IP gratuitos necessários | Tamanho mínimo do CIDR |
|---|---|---|
| 8 | 9 | /27 |
| 16 | 15 | /27 |
| 32 | 13 | /27 |
| 64 | 21 | /27 |
| 128 | 37 | /26 |
| 256 | 69 | /25 |
| 512 | 133 | /24 |

Você também precisa de endereços IP gratuitos ao atualizar seu grupo de trabalho para usar mais RPUs. Os números mínimos de endereços IP gratuitos necessários ao atualizar as sub-redes para um grupo de trabalho são os seguintes:

Número de endereços IP gratuitos necessários ao atualizar uma sub-rede

| Unidades de processamento do Redshift (RPUs) | Unidades de processamento do Redshift (RPUs) atualizadas | Endereços IP gratuitos necessários |
|---|---|---|
| 8 | 16 | 10 |
| 16 | 32 | 13 |
| 32 | 64 | 16 |

| Unidades de processamento do Redshift (RPUs) | Unidades de processamento do Redshift (RPUs) atualizadas | Endereços IP gratuitos necessários |
|---|---|---|
| 64 | 128 | 28 |
| 128 | 256 | 52 |
| 256 | 512 | 100 |

Espaço de armazenamento após a migração: ao migrar pequenos clusters provisionados do Amazon Redshift para o Amazon Redshift Serverless, pode haver um aumento na alocação do espaço de armazenamento após a migração. Isso resulta da alocação otimizada de espaço de armazenamento, que, por sua vez, resulta em espaço de armazenamento pré-alocado. Esse espaço é usado durante um período à medida que os dados aumentam no Amazon Redshift Serverless.

Unidades de compartilhamento de dados entre clusters provisionados do Amazon Redshift Serverless e Amazon Redshift: quando há uma unidade de compartilhamento de dados onde o Amazon Redshift Serverless é o produtor e um cluster provisionado é o consumidor, o cluster provisionado deve ter uma versão de cluster posterior a 1.0.38214. Se você usar uma versão de cluster anterior a essa, ocorrerá um erro ao executar uma consulta. Você pode visualizar a versão do cluster no console do Amazon Redshift na guia Maintenance (Manutenção). Também é possível executar `SELECT version();`.

Tempo máximo de execução da consulta: o tempo de execução decorrido para uma consulta (em segundos). O tempo de execução não inclui o tempo gasto esperando em uma fila. Se uma consulta exceder o tempo de execução definido, o Amazon Redshift Serverless interromperá a consulta. Os valores válidos são 0–86.399.

Migrar para tabelas com chaves de classificação intercaladas : ao migrar clusters provisionados do Amazon Redshift para o Amazon Redshift Serverless, o Redshift converte tabelas com chaves de classificação intercaladas e DISTSTYLE KEY em chaves de classificação compostas. O DISTSTYLE não é alterado. Para obter mais informações sobre estilos de distribuição, consulte Trabalhar com estilos de distribuição de dados no Guia do desenvolvedor do Amazon Redshift. Para obter mais informações sobre chaves de classificação, consulte Trabalhar com chaves de classificação.

Compartilhamento de VPC: é possível criar grupos de trabalho do Amazon Redshift sem servidor em uma VPC compartilhada. Se você fizer isso, será recomendável não excluir o compartilhamento de recursos, pois isso pode resultar na indisponibilidade do grupo de trabalho.

# Capacidade computacional do Amazon Redshift Serverless

## Noções básicas sobre a capacidade do Amazon Redshift Serverless

RPUs

O Amazon Redshift Serverless mede a capacidade do data warehouse em unidades de processamento do Redshift (RPUs). As RPUs são recursos usados para lidar com workloads.

Capacidade básica

Essa configuração especifica a capacidade inicial do data warehouse que o Amazon Redshift usa para processar consultas. A capacidade inicial é especificada em RPUs. Você pode definir uma capacidade base em unidades de processamento do Redshift (RPUs). Uma RPU fornece 16 GB de memória. Definir uma capacidade inicial mais alta melhora a performance da consulta, principalmente para trabalhos de processamento de dados que consomem muitos recursos. A capacidade inicial padrão do Amazon Redshift Serverless é de 128 RPUs. Você pode ajustar a configuração Capacidade básica entre 8 RPUs e 512 RPUs, em unidades múltiplas de 8 (8, 16, 24 … 512), usando o console da AWS, a operação de API `UpdateWorkgroup` ou a operação `update-workgroup` na AWS CLI.

Com uma capacidade mínima de 8 RPUs, agora você tem mais flexibilidade para executar desde workloads mais simples a mais complexas com base nos requisitos de performance. As capacidades básicas de 8, 16 e 24 RPUs são voltadas para workloads que exigem menos de 128 TB de dados. Se seus requisitos de dados forem maiores que 128 TB, você deverá usar pelo menos 32 RPUs. Para workloads que tenham tabelas com muitas colunas e maior simultaneidade, recomendamos o uso de 32 ou mais RPUs.

## Considerações e limitações da capacidade do Amazon Redshift sem servidor

Veja a seguir considerações e limitações da capacidade do Amazon Redshift sem servidor.

- Configurações de 8 ou 16 RPUs oferecem suporte à capacidade de armazenamento gerenciado pelo Redshift de até 128 TB. Se você estiver usando mais de 128 TB de armazenamento gerenciado, não poderá fazer downgrade para menos de 32 RPUs.

- A edição da capacidade base do grupo de trabalho pode cancelar algumas das consultas em execução no grupo de trabalho.

## Escalabilidade e otimização orientadas por IA (visualização)

Esta é a documentação de pré-lançamento para escalabilidade e otimizações orientadas por IA no Amazon Redshift sem servidor, que está no lançamento de visualização. A documentação e o atributo estão sujeitos a alterações. Recomendamos o uso desse atributo somente em ambientes de teste, e não em ambientes de produção. Para conferir os termos e condições da pré-visua lização, consulte Betas e pré-visualizações nos Termos de serviços da AWS.

Essa pré-visualização está disponível nas seguintes Regiões da AWS:

- Leste dos EUA (Ohio) (us-east-2)
- Leste dos EUA (Norte da Virgínia) (us-east-1)
- Oeste dos EUA (Norte da Califórnia) (us-west-1)
- Ásia Pacific (Tóquio) (ap-northeast-1)
- Europa (Irlanda) (eu-west-1)
- UE (Estocolmo) (eu-north-1)

É possível criar um grupo de trabalho de visualização do Amazon Redshift sem servidor. Não é possível usar esses recursos em produção nem mover o grupo de trabalho para outro grupo de trabalho. Para termos e condições de visualização, consulte Beta and Previews em Termos de serviço da AWS. Para obter instruções sobre como criar um grupo de trabalho de visualização, consulte Creating a preview workgroup.

Também é possível estabelecer uma meta de desempenho do preço para o grupo de trabalho, de maneira que o Redshift possa fazer automaticamente otimizações orientadas por IA nos recursos. Assim, é possível atingir as metas de desempenho do preço e, ao mesmo tempo, otimizar os custos. Essa otimização automática de desempenho do preço será especialmente útil se você não souber qual capacidade base definir para os workloads ou se algumas partes do workload puderem se beneficiar de mais recursos alocados.

Por exemplo, se a organização normalmente executa workloads que só exigem 32 RPU, mas, de repente, introduz uma consulta mais complexa, talvez você não saiba a capacidade básica indicada.

A definição de uma capacidade básica mais alta resulta em um melhor desempenho de preço melhor, mas também gera custos mais altos, logo, o custo talvez não corresponda às expectativas. Usando escalabilidade orientada por IA e otimização de recursos, o Amazon Redshift sem servidor ajusta automaticamente as RPUs para atender às metas de desempenho de preço, mantendo os custos otimizados para a organização. Essa otimização automática é útil, independentemente do tamanho do workload. A otimização automática poderá ajudar a atingir as metas de desempenho do preço da organização, se você tiver um número qualquer de consultas complexas.

As metas de desempenho do preço são uma configuração específica do grupo de trabalho. Grupos de trabalho diferentes podem ter metas de preço de desempenho diferentes.

Para manter custos previsíveis, estabeleça uma capacidade máxima limite que o Amazon Redshift sem servidor pode alocar para os workloads.

Para configurar metas de desempenho do preço, use o console da AWS. Por padrão, a meta de desempenho do preço é habilitada quando você cria um novo grupo de trabalho e é definida como Equilibrada. Para estabelecer uma meta de desempenho do preço diferente ou especificar uma capacidade base para o grupo de trabalho, use configurações personalizadas ao criar um grupo de trabalho. Para obter mais informações sobre como criar um grupo de trabalho, consulte Creating a workgroup with a namespace.

Para editar a meta de desempenho do preço para o grupo de trabalho:

1. No console do Amazon Redshift sem servidor, escolha Configuração do grupo de trabalho.
2. Escolha o grupo de trabalho para o qual você deseja editar a meta de desempenho do preço. Escolha a guia Permissões e Editar.
3. Escolha Meta de desempenho do preço e ajuste o controle deslizante de acordo com a meta na qual você deseja definir o grupo de trabalho.
4. Escolha Save changes (Salvar alterações).

Para atualizar o máximo de RPUs que o Amazon Redshift sem servidor pode alocar para a workload, vá até a guia Limites da configuração do grupo de trabalho.

Para saber mais sobre otimizações orientadas por IA e escalabilidade de recursos, assista ao vídeo a seguir.

# Faturamento do Amazon Redshift Serverless

## Definição de preço

Para obter informações sobre preço, consulte Preço do Amazon Redshift.

## Faturamento da capacidade computacional

Capacidade básica e seu efeito no faturamento

Quando as consultas são executadas, você é cobrado de acordo com a capacidade usada em determinada duração, em horas de RPU por segundo. Quando nenhuma consulta estiver em execução, você não será cobrado pela capacidade computacional. Você também receberá uma cobrança pelo Redshift Managed Storage (RMS), com base na quantidade de dados armazenados.

Ao criar o grupo de trabalho, você tem a opção de definir a Capacidade básica de computação. Para atender aos requisitos de preço/performance da workload em um nível do grupo de trabalho, ajuste a capacidade básica acima ou abaixo para um grupo de trabalho existente. Selecione o grupo de trabalho em Configuração do grupo de trabalho e escolha a guia Limites para alterar a capacidade básica usando o console.

Conforme o número de consultas aumenta, o Amazon Redshift sem servidor escala automaticamente para fornecer performance consistente.

Limite máximo de horas de uso de RPU

Para manter os custos previsíveis para o Amazon Redshift Serverless, você pode definir as Maximum RPU hours (Horas máximas de RPU) usadas por dia, por semana ou por mês. É possível defini-lo usando o console ou com a API. Quando um limite é atingido, é possível especificar que uma entrada de log é gravada em uma tabela do sistema, ou você recebe um alerta, ou as consultas do usuário estão desativadas. Definir o máximo de horas de RPU ajuda a manter os custos sob controle. As configurações do máximo de horas de RPU se aplicam ao grupo de trabalho para consultas que acessam dados no data warehouse e consultas que acessam dados externos, como em uma tabela externa no Amazon S3.

Veja um exemplo a seguir:

Suponhamos que você defina um limite de 100 horas para cada semana. Para fazer isso no console, faça o seguinte:

1. Escolha o grupo de trabalho e Gerenciar limites de uso na guia Limites.
2. Adicione um limite de uso, escolhendo a frequência Semanal, uma duração de 100 horas e definindo a ação como Desativar consultas de usuário.

Neste exemplo, se você atingir o limite de 100 horas de RPU para uma semana, as consultas serão desativadas.

A definição do máximo de horas de RPU para o grupo de trabalho não limita desempenho ou os recursos computacionais do grupo de trabalho. É possível ajustar as configurações a qualquer momento sem afetar o processamento de consultas. A meta de definir o máximo de horas de RPU é ajudar você a atender aos requisitos de preço e desempenho. Para obter mais informações sobre faturamento sem servidor, consulte Preços do Amazon Redshift.

Outra maneira de manter o custo do Amazon Redshift sem servidor previsível é usar Detecção de anomalias de custo da AWS para reduzir as chances de surpresas no faturamento e possibilitar mais controle.

> **Note**
>
> A Calculadora de preços do Amazon Redshift é útil para fazer estimativas de preços. Você insere os recursos de computação de que precisa e ela fornece uma pré-visualização do custo.

## Definição da capacidade máxima para controlar custos de recursos computacionais

A configuração de capacidade máxima funciona como o máximo de RPU que o Amazon Redshift sem servidor pode escalar. Ela ajuda a controlar o custo de recursos computacionais. De maneira semelhante à forma como a capacidade base define uma quantidade mínima de recursos computacionais disponíveis, a capacidade máxima define um máximo para o uso de RPU. Assim, isso ajuda os gastos a cumprirem os planos. A capacidade máxima se aplica especificamente a cada grupo de trabalho e limita o uso da computação sempre.

Como a capacidade máxima difere dos limites de uso de horas de RPU

A finalidade dos limites máximos de horas de RPU e da configuração de capacidade máxima é controlar os custos. Porém, eles conseguem isso por meios diferentes. Os seguintes pontos explicam a diferença:

- Capacidade máxima: esta configuração estabelece a contagem máxima de RPUs que o Amazon Redshift sem servidor usa para fins de escalabilidade. Quando a escalabilidade de computação automática é necessária, ter um valor maior para a capacidade máxima pode aumentar throughput de consultas. Quando o limite de capacidade máxima é atingido, o grupo de trabalho não aumenta a escala verticalmente ainda mais.
- Limite máximo de horas de uso de RPU: diferentemente da capacidade máxima, essa configuração não define um limite máximo de capacidade. Porém, ele realiza outras ações para ajudar você a limitar custos. Entre elas estão a adição de uma entrada a um log, a notificação ou a interrupção da execução de consultas, se você quiser.

É possível usar exclusivamente a capacidade máxima ou complementá-la com ações dos limites máximos de uso de horas de RPU.

Um caso de uso de capacidade máxima

Cada grupo de trabalho pode ter uma configuração de capacidade máxima diferente. Isso ajuda você a impor exgências orçamentárias. Para ilustrar como isso funciona, vamos pressupor o seguinte:

- Você tem um grupo de trabalho com a capacidade base definida como 256 RPUs. Você tem workloads estáveis com pouco mais de 256 RPUs durante a maior parte do mês.
- A capacidade máxima está ajustada em 512 RPUs.

Suponhamos que você tenha um alto uso inesperado em um período de três dias para gerar relatórios estatísticos ad-hoc. Nesse caso, você tem a capacidade máxima definida para evitar custos de computação além de 512 RPUs. Ao fazer isso, você pode ter certeza de que a capacidade computacional não excederá esse limite máximo.

Observações sobre uso de capacidade máxima

Essas observações podem ajudar você a definir a capacidade máxima da maneira indicada:

- Cada grupo de trabalho do Amazon Redshift sem servidor pode ter uma configuração de capacidade máxima diferente.
- Se você tiver um período de uso muito intensivo de recursos e a capacidade máxima estiver definida em um nível baixo de RPU, isso poderá atrasar o processamento da workload e resultar em uma experiência de usuário que não é a ideal.
- A configuração da capacidade máxima não interfere na execução de consultas, mesmo em períodos de uso intensivo da RPU. Isso não funciona como um limite de uso, o que pode impedir

a execução de consultas. Ele só limita recursos computacionais disponíveis para o grupo de trabalho. É possível exibir a capacidade usada durante um período no painel do Amazon Redshift sem servidor. Para obter mais informações sobre como exibir dados de resumo, consulte Checking Amazon Redshift Serverless summary data using the dashboard.

- A configuração da capacidade máxima está ajustada em 5.632 RPUs.

Como definir capacidade máxima

Você pode definir a capacidade máxima no console. Para um grupo de trabalho existente, é possível alterar a configuração em Configuração do grupo de trabalho. Você também pode usar a CLI para defini-lo usando um comando como o seguinte exemplo:

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

Isso define a configuração de capacidade máxima para o grupo de trabalho com o nome indicado. Depois de defini-la, você poderá verificar o valor no console para verificá-lo. Você também pode verificar o valor usando a CLI executando o comando `get-workgroup`.

Você pode desativar a configuração de capacidade máxima definindo-a como `-1` da seguinte forma:

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

## Monitoramento do uso e do custo do Amazon Redshift sem servidor

Há várias maneiras de fazer uma estimativa do uso e do faturamento do Amazon Redshift Serverless. As visualizações do sistema podem ser úteis porque os metadados do sistema, incluindo dados de consulta e uso, são oportunos e você não precisa definir nenhuma configuração para consultá-los. O CloudWatch também pode ser útil para monitorar o uso da instância do Amazon Redshift Serverless e tem outros recursos para fornecer insights e definir ações.

Visualizar o uso consultando uma visualização do sistema

Consulte a tabela do sistema SYS_SERVERLESS_USAGE para monitorar o uso e conhecer as cobranças pelas consultas:

```
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
```

Essa consulta fornece o custo por dia incorrido para o Amazon Redshift Serverless, com base no uso.

Notas de uso para determinar o uso e o custo

- Você paga pelas workloads executadas, em RPU-horas por segundo, com uma cobrança mínima de 60 segundos.
- Os registros da tabela do sistema sys_serverless_usage mostram o custo incorrido em intervalos de de 1 minuto. É importante compreender as seguintes colunas:

  A coluna charged_seconds:

  - Fornece os segundos de unidade de computação (RPU) cobrados durante o intervalo de tempo. Os resultados incluem todas as cobranças mínimas no Amazon Redshift Serverless.
  - Tem informações sobre o uso de recursos de computação após a conclusão das transações. Portanto, o valor dessa coluna poderá ser 0 se as transações não tiverem sido concluídas.

  A coluna compute_seconds:

  - Fornece informações de uso de computação em tempo real. Isso não inclui as cobranças mínimas no Amazon Redshift Serverless. Portanto, pode diferir dos segundos cobrados cobrados durante o intervalo.
  - Mostra informações de uso durante cada transação (mesmo que a transação não tenha terminado), portanto, os dados fornecidos são em tempo real.
- Há situações em que compute_seconds é 0, mas charged_seconds é maior que 0 ou vice-versa. Esse é um comportamento normal resultante da forma como os dados são registrados na visualização do sistema. Para uma representação mais precisa dos detalhes do uso da tecnologia sem servidor, recomendamos agregar os dados em SYS_SERVERLESS_USAGE.

Para obter mais informações sobre monitoramento de tabelas e visualizações, consulte Monitorar consultas e workloads com o Amazon Redshift Serverless.

Visualizar o uso com o CloudWatch

É possível usar as métricas disponíveis no CloudWatch para monitorar o uso. As métricas geradas para o CloudWatch são `ComputeSeconds`, indicando o total de segundos de RPU usados no minuto

atual, e `ComputeCapacity`, indicando a capacidade computacional total para esse minuto. Também é possível encontrar métricas de uso no console do Redshift, no Redshift Serverless dashboard (Painel do Redshift Serverless). Para obter mais informações sobre o CloudWatch, consulte O que é o Amazon CloudWatch?

## Faturamento para armazenamento

A capacidade de armazenamento principal é cobrada como Redshift Managed Storage (RMS). O armazenamento é cobrado por GB/mês. O faturamento de armazenamento é separado do faturamento de capacidade de computação. O armazenamento usado para snapshots do usuário é faturado com base nas taxas de faturamento de backup padrão, dependendo do nível de uso.

Os custos de transferência de dados e os custos de machine learning (ML) aplicam-se separadamente, da mesma forma que os clusters provisionados. A replicação de snapshots e o compartilhamento de dados entre as regiões da AWS são cobrados de acordo com as taxas de transferência descritas na página de preços. Para obter mais informações, consulte Preços do Amazon Redshift.

### Visualizar o uso de faturamento com o CloudWatch

A métrica `SnapshotStorage`, que rastreia o uso do armazenamento de snapshots, é gerada e enviada para o CloudWatch. Para obter mais informações sobre o CloudWatch, consulte O que é o Amazon CloudWatch?

## Usar o teste gratuito do Amazon Redshift sem servidor

O Amazon Redshift Serverless oferece um teste gratuito. Se participar do teste gratuito, você poderá visualizar o saldo de créditos do teste gratuito no console do Redshift e verificar o uso do teste gratuito na visualização do sistema SYS_SERVERLESS_USAGE. Observe que os detalhes de faturamento do uso do teste gratuito não aparecem no console de faturamento. Você só poderá visualizar o uso no console de faturamento após o término do teste gratuito. Para obter mais informações sobre o teste gratuito do Amazon Redshift, consulte Teste gratuito do Amazon Redshift sem servidor.

## Observações sobre o uso de faturamento

- Uso de gravação: uma consulta ou uma transação só é medida e registrada depois de concluída, revertida ou interrompida. Por exemplo, se uma transação for executada por dois dias, o uso

da RPU será registrado após a conclusão. Você pode monitorar o uso contínuo em tempo real consultando `sys_serverless_usage`. O registro de transações pode ser refletido como variação de uso da RPU e efetivar custos para horas específicas e uso diário.

- Gravar transações explícitas: como prática recomendada, é importante encerrar as transações. Se você não finalizar ou reverter uma transação em aberto, o Amazon Redshift Serverless continuará a usar RPUs. Por exemplo, se você gravar um `BEGIN TRAN` explícito, é importante ter as instruções `COMMIT` e `ROLLBACK` correspondentes.
- Consultas canceladas: se você executar uma consulta e cancelá-la antes da conclusão, ainda assim será cobrado pelo tempo em que a consulta foi executada.
- Escalabilidade: a instância do Amazon Redshift Serverless pode iniciar a escalabilidade para períodos de processamento de carga mais alta, a fim de manter uma performance consistente. O faturamento do Amazon Redshift Serverless inclui computação inicial e capacidade escalada de acordo com a mesma taxa de RPU.
- Redução da escala verticalmente: o Amazon Redshift Serverless aumenta a escala verticalmente de acordo com a capacidade inicial de RPU para lidar com períodos de carga maior. Em alguns casos, a capacidade de RPU pode permanecer em uma configuração mais alta por um período após a queda da carga da consulta. Recomendamos que você defina o máximo de horas de RPU no console para se proteger contra custos inesperados.
- Tabelas do sistema: quando você consulta uma tabela do sistema, o tempo de consulta é cobrado.
- Redshift Spectrum: quando você tem o Amazon Redshift Serverless e executa consultas, não há uma cobrança separada para consultas de data lake. Para consultas sobre dados armazenados no Amazon S3, a cobrança é igual (por tempo de transação) à das consultas em dados locais.
- Consultas federadas: as consultas federadas são cobradas em termos de RPUs usadas em um intervalo de tempo específico, da mesma maneira que as consultas no data warehouse ou data lake.
- Armazenamento: o armazenamento é cobrado separadamente, por GB/mês.
- Cobrança mínima: a cobrança mínima é de 60 segundos de uso de recursos, que é medido por segundo.
- Faturamento de snapshots: o faturamento de snapshots não é alterado. Ele é cobrado de acordo com o armazenamento, a uma taxa de GB/mês. É possível restaurar gratuitamente seu data warehouse para pontos específicos nas últimas 24 horas com detalhamento de 30 minutos. Para obter mais informações, consulte Preços do Amazon Redshift.

### Práticas recomendadas para manter o faturamento previsível no Amazon Redshift Serverless

Veja a seguir as práticas recomendadas e as configurações integradas que ajudam a manter o faturamento consistente.

- Encerre cada transação. Quando você usa `BEGIN` para iniciar uma transação, é importante usar `END` também.
- Use o tratamento de erros de práticas recomendadas para responder tranquilamente aos erros e encerrar cada transação. Minimizar transações abertas ajuda a evitar o uso desnecessário de RPU.
- Use o `SESSION TIMEOUT` para ajudar transações abertas e sessões ociosas. Isso faz com que qualquer sessão mantida ociosa ou inativa por mais de 3.600 segundos (1 hora) atinja o tempo limite. Isso faz com que qualquer transação mantida aberta e inativa por mais de 21.600 segundos (6 horas) atinja o tempo limite. Essa configuração de tempo limite pode ser alterada explicitamente para um usuário específico, como quando você deseja manter uma sessão aberta para uma consulta de longa execução. O tópico CREATE USER (CRIAR USUÁRIO) mostra como ajustar `SESSION TIMEOUT` para um usuário.
  - Na maioria dos casos, recomendamos que você não estenda o valor `SESSION TIMEOUT`, a menos que você tenha um caso de uso que o exija especificamente. Se a sessão permanecer ociosa com uma transação aberta, isso pode resultar em um caso em que as RPUs são usadas até que a sessão seja fechada. Isso resultará em custos desnecessários.
  - O Amazon Redshift Serverless tem um tempo máximo de 86.399 segundos (24 horas) para uma consulta em execução. O período máximo de inatividade para uma transação aberta é de 6 horas antes que o Amazon Redshift Serverless encerre a sessão associada à transação. Para obter mais informações, consulte Cotas para objetos do Amazon Redshift Serverless.

## Conectar-se ao Amazon Redshift Serverless

Depois de configurar a instância do Amazon Redshift Serverless, você pode se conectar a ela por vários métodos, descritos a seguir. Caso tenha várias equipes ou projetos e queira gerenciar custos separadamente, você pode usar Contas da AWS separadas.

Para obter uma lista de Regiões da AWS nas quais o Amazon Redshift sem servidor está disponível, consulte os endpoints listados para a API do Redshift sem servidor na Referência geral da Amazon Web Services.

O Amazon Redshift Serverless se conecta ao ambiente sem servidor em sua Conta da AWS na Região da AWS atual. O Amazon Redshift sem servidor é executado em uma VPC dentro dos intervalos de porta de 5431 a 5455 e de 8191 a 8215. O padrão é 5439. No momento, só é possível alterar as portas com a operação de API `UpdateWorkgroup` e a operação `update-workgroup` da AWS CLI.

## Conectar-se ao Amazon Redshift Serverless

Você pode se conectar a um banco de dados (chamado `dev`) no Amazon Redshift sem servidor com a sintaxe a seguir.

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

Por exemplo, a string de conexão a seguir especifica a região us-east-1.

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

## Conectar-se ao Amazon Redshift Serveless por meio de drivers JDBC

Você pode usar um dos métodos a seguir para se conectar ao Amazon Redshift Serverless com o cliente SQL de sua preferência usando o driver JDBC versão 2 fornecido pelo Amazon Redshift.

Para se conectar com credenciais de login para autenticação do banco de dados usando o driver JDBC versão 2.1.x ou posterior, use a sintaxe a seguir. O número da porta é opcional; se não estiver incluído, o Amazon Redshift Serverless usará como padrão a porta número 5439. Você pode mudar para outra porta do intervalo de portas 5431–5455 ou 8191–8215. Para alterar a porta padrão de um endpoint de tecnologia sem servidor, use a AWS CLI e a API do Amazon Redshift.

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

Por exemplo, a string de conexão a seguir especifica o padrão do grupo de trabalho, o ID da conta 123456789012 e a região us-east-2.

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

Para se conectar ao IAM usando o driver JDBC versão 2.1.x ou posterior, use a sintaxe a seguir. O número da porta é opcional; se não estiver incluído, o Amazon Redshift Serverless usará como

padrão a porta número 5439. Você pode mudar para outra porta do intervalo de portas 5431–5455 ou 8191–8215. Para alterar a porta padrão de um endpoint de tecnologia sem servidor, use a AWS CLI e a API do Amazon Redshift.

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

Por exemplo, a string de conexão a seguir especifica o padrão do grupo de trabalho, o ID da conta 123456789012 e a região us-east-2.

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

Para ODBC, use a sintaxe a seguir.

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

Se você estiver usando uma versão do driver JDBC anterior à 2.1.0.9 e se conectar ao IAM, será necessário usar a sintaxe a seguir.

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

Por exemplo, a string de conexão a seguir especifica o padrão do grupo de trabalho e a Região da AWS us-east-1.

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

Para obter mais informações sobre drivers, consulte Configurar conexões no Amazon Redshift.

## Como encontrar uma string de conexão JDBC e ODBC

Para conectar-se ao grupo de trabalho com a ferramenta do cliente SQL, você precisa ter a string de conexão JDBC ou ODBC. Você pode encontrar a string de conexão no console do Amazon Redshift sem servidor, na página de detalhes de um grupo de trabalho.

Como encontrar a string de conexão de um grupo de trabalho

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

2. No menu de navegação, escolha Redshift sem servidor.
3. No menu de navegação, escolha Configuração do grupo de trabalho e selecione o nome do grupo de trabalho na lista para abrir seus detalhes.
4. O URL do JDBC e URL do ODBC estão disponíveis, juntamente com detalhes adicionais, na seção Informações gerais. Cada string é baseada na região da AWS em que o grupo de trabalho é executado. Escolha o ícone ao lado da string de conexão apropriada para copiá-la.

## Conectar-se ao Amazon Redshift Serverless com a API de dados

Também é possível usar a API de dados do Amazon Redshift para se conectar ao Amazon Redshift Serverless. Use o parâmetro `workgroup-name` em vez do `cluster-identifier` nas chamadas da AWS CLI.

Para obter mais informações sobre a API de dados, consulte Usar a API de dados Amazon Redshift. Por exemplo, para chamar o código da API de dados em Python e outros exemplos, consulte Conceitos básicos da API de dados do Redshift e veja as pastas `quick-start` e `use-cases` no GitHub.

## Conectar-se com SSL ao Amazon Redshift Serverless

### Configurar uma conexão segura com o Amazon Redshift Serverless

Para oferecer compatibilidade com conexões SSL, o Redshift sem servidor cria e instala um certificado SSL emitido pelo AWS Certificate Manager (ACM) para cada grupo de trabalho. Os certificados ACM são publicamente confiáveis pela maioria dos sistemas operacionais, navegadores da Web e clientes. Poderá ser necessário baixar um pacote de certificados, caso seus clientes ou aplicações SQL se conectem ao Redshift sem servidor usando SSL com a opção de conexão `sslmode` definida como `require`, `verify-ca` ou `verify-full`. Se o cliente precisar de um certificado, o Redshift sem servidor fornecerá um certificado em pacote da seguinte forma:

- Baixe o pacote em https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt.
  - O número de soma de verificação MD5 esperado é 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - O número da soma de verificação sha256 é 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  Não use o pacote de certificados anterior localizado em `https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt`.

- Na Região da AWS da China, baixe o pacote de https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt.
  - O número de soma de verificação MD5 esperado é 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - O número da soma de verificação sha256 é 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  Não use os pacotes de certificados anteriores localizados em `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` e `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem`

> **Important**
>
> O Redshift sem servidor mudou a maneira como os certificados SSL são gerenciados. Talvez seja necessário atualizar os certificados CA raiz confiáveis atuais para continuar se conectando aos grupos de trabalho usando SSL. Para ter mais informações sobre certificados do ACM para conexões SSL, consulte Transição para certificados ACM das conexões SSL.

Por padrão, os bancos de dados do grupo de trabalho aceitam as conexões que usam ou não SSL.

Para criar um grupo de trabalho que só aceite conexões SSL, use o comando `create-workgroup` e defina o parâmetro `require_ssl` como `true`. Para usar o exemplo a seguir, substitua *`yourNamespaceName`* pelo nome do namespace e substitua *`yourWorkgroupName`* pelo nome do grupo de trabalho.

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

Para atualizar um grupo de trabalho existente que só aceite conexões SSL, use o comando `update-workgroup` e defina o parâmetro `require_ssl` como `true`. Observe que o Redshift sem servidor reiniciará o grupo de trabalho ao atualizar o parâmetro `require_ssl`. Para usar o exemplo a seguir, substitua *`yourWorkgroupName`* pelo nome do grupo de trabalho.

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

```
--workgroup-name yourWorkgroupName \
--config-parameters parameterKey=require_ssl,parameterValue=true
```

O Amazon Redshift oferece suporte ao protocolo de acordo de chave Elliptic Curve Diffie—Hellman Ephemeral (ECDHE). Com o ECDHE, o cliente e o servidor têm, cada um, um par de chaves públicas/privadas de curva elíptica que é usado para estabelecer um segredo compartilhado através de um canal inseguro. Não é necessário configurar nada no Amazon Redshift para habilitar o ECDHE. Se você se conectar a partir de uma ferramenta de cliente SQL que usa ECDHE para criptografar a comunicação entre o cliente e o servidor, o Amazon Redshift usa a lista de cifras fornecida para fazer a conexão apropriada. Para obter mais informações, consulte Elliptic curve diffie—hellman na Wikipedia e Cifras no site do OpenSSL.

# Conexão com o Amazon Redshift Serverless por um endpoint da VPC gerenciado pelo Amazon Redshift

## Conectar-se ao Amazon Redshift Serverless de outros endpoints da VPC

Para obter informações sobre como instalar ou configurar um endpoint da VPC gerenciado para um grupo de trabalho do Amazon Redshift sem servidor, consulte Trabalhando com endpoints da VPC gerenciados por Redshift no Amazon Redshift.

# Conexão ao Amazon Redshift sem servidor por um endpoint da VPC do Redshift em outra conta ou região

## Conexão ao Amazon Redshift sem servidor por um endpoint da VPC cruzado

O Amazon Redshift Serverless é provisionado em uma VPC. Você pode conceder acesso a uma VPC em outra conta para acessar o Amazon Redshift sem servidor na conta. Isso é semelhante a uma conexão por um endpoint da VPC gerenciado, mas, nesse caso, a conexão se origina, por exemplo, em um cliente do banco de dados em outra conta. Existem algumas operações que é possível realizar:

- O proprietário de um banco de dados pode conceder acesso a uma VPC contendo o Amazon Redshift sem servidor para outra conta na mesma região.
- Um proprietário do banco de dados pode revogar o acesso ao Amazon Redshift sem servidor.

O principal benefício do acesso entre contas é permitir uma colaboração mais fácil no banco de dados. Os usuários não precisam ser provisionados na conta que contém o banco de dados para acessá-lo, o que reduz etapas de configuração e economiza tempo.

Permissões necessárias para conceder acesso a uma VPC em outra conta

Para conceder acesso ou alterar o acesso permitido, o concessor exige uma política de permissões atribuída com as seguintes permissões:

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

Talvez você precise de outras permissões especificadas na política AWS gerenciada AmazonRedShiftFullAccess. Para obter mais informações, consulte Granting permissions to Amazon Redshift Serverless.

O beneficiário exige uma política de permissões atribuída com as seguintes permissões:

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

Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.

Esta é uma política de recursos de exemplo usada para configurar o acesso entre VPCs:

```
{
    "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"
                        ]
                    }
                }
            }
        }
    ]
}
```

Os procedimentos a seguir nesta seção pressupõem que o usuário que os executa tenha as permissões atribuídas indicadas, por exemplo, por meio de um perfil do IAM atribuído que tenha as permissões listadas. Os procedimentos também pressupõem que o grupo de trabalho tenha um perfil do IAM associado às permissões de recurso indicadas.

Concessão de acesso à VPC para outras contas, usando o console

Este procedimento mostra as etapas para configurar o acesso ao banco de dados quando você é o proprietário do banco de dados e deseja conceder acesso a ele.

Concessão de acesso pela conta do proprietário

1. Nas propriedades do grupo de trabalho do Amazon Redshift sem servidor, na guia Acesso a dados, há uma lista chamada Contas concedidas. Ela mostra contas e VPCs com acesso

concedido ao grupo de trabalho. Encontre a lista e escolha Conceder acesso para adicionar uma conta à lista.

2. Uma janela é exibida na qual é possível adicionar as informações do beneficiário. Digite o ID da conta da AWS, que é o ID de 12 dígitos da conta para a qual você deseja conceder acesso.
3. Conceda acesso a todas as VPCs para o beneficiário ou a VPCs específicas. Se só conceder acesso a VPCs específicas, você poderá adicionar os IDs delas inserindo cada uma e escolhendo Adicionar VPC.
4. Salve as alterações quando você tiver terminado.

Quando você salva as alterações, a conta é exibida na lista Contas concedidas. A entrada mostra o ID da conta e a lista de VPCs com acesso concedido.

O proprietário do banco de dados também pode revogar o acesso a uma conta. O proprietário pode revogar o acesso a qualquer momento.

Revogação do acesso a uma conta

1. É possível começar pela lista de contas concedidas. Primeiro, selecione uma ou mais contas.
2. Escolha Revogar acesso.

Depois que o acesso for concedido, um administrador do banco de dados do beneficiário poderá verificar o console para determinar se ele tem acesso.

Uso do console para confirmar se o acesso foi concedido para você acessar outra conta

1. Nas propriedades do grupo de trabalho do Amazon Redshift sem servidor, na guia Acesso a dados, há uma lista chamada Contas autorizadas. Ela mostra contas que podem ser acessadas nesse grupo de trabalho. O beneficiário não pode usar o URL do endpoint do grupo de trabalho para acessar diretamente o grupo de trabalho. Para acessar o grupo de trabalho, você, como beneficiário, vá até a seção Endpoint e escolhe Criar um endpoint.
2. Em seguida, como beneficiário, você fornece um nome de endpoint e uma VPC para acessar o grupo de trabalho.
3. Depois de ser criado com êxito, o endpoint será exibido na seção Endpoint e haverá um URL do endpoint para ele. É possível usar o URL desse endpoint para acessar o grupo de trabalho.

Concessão de acesso a outras contas, usando os comandos de CLI

A conta que concede acesso deve primeiro conceder acesso a outra conta para se conectar usando `put-resource-policy`. O proprietário do banco de dados pode chamar `put-resource-policy` a fim de autorizar outra conta para criar conexões com o grupo de trabalho. A conta do beneficiário pode acabar usando `create-endpoint-authorization` para criar conexões com o grupo de trabalho por meio das VPCs permitidas.

Ela mostra as propriedades de `put-resource-policy`, que você pode chamar para permitir acesso a uma conta e VPC específicas.

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

Depois de chamar o comando, você poderá chamar `get-resource-policy`, especificando `resource-arn` para saber quais contas e VPCs têm permissão para acessar o recurso.

A chamada a seguir pode ser feita pelo beneficiário. Ela mostra informações sobre o acesso concedido. Mais especificamente, ela retorna uma lista contendo as VPCs que receberam acesso.

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

A finalidade disso é para o beneficiário obter informações da conta concessora sobre autorizações de endpoint. `owner-account` é a conta de compartilhamento. Quando você executa isso, ele retorna `CrossAccountVpcs` para cada grupo de trabalho, que é uma lista de VPCs permitidas. Para referência, ele mostra todas as propriedades disponíveis para um grupo de trabalho:

```
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**
>
> Como lembrete, a realocação do cluster não é um pré-requisito para configurar recursos de rede do Redshift adicionais, como os usados na recuperação de desastres ou para outros fins. Também não é necessário ativá-lo para habilitar o seguinte:
>
> - Conexão de uma VPC entre contas ou regiões ao Redshift: você pode se conectar a partir de uma nuvem privada virtual (VPC) da AWS a outra que contenha um banco de dados do Redshift, conforme descrito nesta seção.
> - Configuração de um nome de domínio personalizado: você pode criar um nome de domínio personalizado, também conhecido como URL personalizado, para o cluster do Amazon Redshift ou para o grupo de trabalho do Amazon Redshift Serverless, para deixar o nome do endpoint mais fácil de lembrar e simples. Para obter mais informações, consulte Usar nome de domínio personalizado para conexões de clientes.

# Definir configurações de tráfego de rede apropriadas para o Amazon Redshift sem servidor

## Conectar-se ao Amazon Redshift sem servidor quando ele está acessível ao público geral

As instruções para definir suas configurações de tráfego de rede estão disponíveis em Acessibilidade pública com configuração de grupo de segurança padrão ou personalizada. Isso inclui um caso de uso em que o cluster está acessível ao público geral.

## Conectar-se ao Amazon Redshift sem servidor quando ele não está acessível ao público geral

As instruções para definir suas configurações de tráfego de rede estão disponíveis em Acessibilidade privada com configuração de grupo de segurança padrão ou personalizado. Isso inclui um caso de uso em que o cluster não está disponível na internet.

## Definir perfis de banco de dados para conceder a usuários federados no Amazon Redshift sem servidor

Você pode definir perfis em sua organização que determinam quais perfis de banco de dados conceder no Amazon Redshift sem servidor. Para ter mais informações, consulte Definir perfis de banco de dados para conceder a usuários federados no Amazon Redshift sem servidor.

## Recursos adicionais do

Para obter mais informações sobre conexões seguras com o Amazon Redshift sem servidor, incluindo concessão de permissões, autorização de acesso a serviços adicionais e criação de perfis do IAM, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift Serverless.

## Definir perfis de banco de dados para conceder a usuários federados no Amazon Redshift sem servidor

Ao fazer parte de uma organização, você tem um conjunto de perfis associados. Por exemplo, você tem perfis para seu cargo, como programador e gerente. Seus perfis determinam a quais aplicações e dados você tem acesso. A maioria das organizações usa um provedor de identidades, como o Microsoft Active Directory, para atribuir perfis a usuários e grupos. O uso de perfis para controlar o acesso a recursos cresceu, pois reduz o gerenciamento de usuários individuais por parte das organizações.

Recentemente, o controle de acesso baseado em perfil foi introduzido no Amazon Redshift sem servidor. Usando perfis de banco de dados, você pode proteger o acesso a dados e objetos, como esquemas ou tabelas, por exemplo. Ou você pode usar perfis para definir um conjunto de permissões elevadas, como para um monitor de sistema ou administrador de banco de dados. Mas depois de conceder permissões de recursos aos perfis de banco de dados, há uma etapa adicional, que é conectar os perfis de um usuário da organização aos perfis do banco de dados. Você pode atribuir cada usuário aos seus perfis de banco de dados no login inicial executando instruções SQL, mas esse método é muito trabalhoso. Uma maneira mais fácil é definir os perfis de banco de dados a serem concedidos e enviá-los para o Amazon Redshift sem servidor. Isso tem a vantagem de simplificar o processo inicial de login.

Você pode enviar perfis para o Amazon Redshift sem servidor usando `GetCredentials`. Quando um usuário faz login pela primeira vez em um banco de dados do Amazon Redshift sem servidor, um usuário de banco de dados associado é criado e mapeado para os perfis de banco de dados

correspondentes. Este tópico detalha o mecanismo para enviar perfis para o Amazon Redshift sem servidor.

O envio de perfis de banco de dados tem alguns casos de uso principais:

- Quando um usuário faz login por meio de um provedor de identidades de terceiros, normalmente com a federação configurada, e envia os perfis por meio de uma etiqueta de sessão.
- Quando um usuário faz login por meio das credenciais de login do IAM e seus perfis são enviados por meio de uma chave e um valor de etiqueta.

Para obter mais informações sobre o controle de acesso baseado em perfil, consulte Controle de acesso baseado em perfil (RBAC).

## Configurar perfis de banco de dados

Antes de enviar perfis para o Amazon Redshift sem servidor, você deve configurar perfis em seu banco de dados e conceder a eles as permissões apropriadas nos recursos do banco de dados. Por exemplo, em um cenário simples, você pode criar um perfil de banco de dados chamado sales e conceder a ele acesso para consultar tabelas com dados de vendas. Para obter mais informações sobre como criar perfis de banco de dados e conceder permissões, consulte CREATE ROLE e GRANT.

## Casos de uso para definir perfis de banco de dados que serão concedidos a usuários federados

Essas seções descrevem alguns casos de uso em que o envio de perfis de banco de dados para o Amazon Redshift sem servidor pode simplificar o acesso aos recursos do banco de dados.

### Fazer login usando um provedor de identidades

O primeiro caso de uso pressupõe que sua organização tenha identidades de usuário em um serviço de gerenciamento de identidade e acesso. Esse serviço pode ser baseado na nuvem, como JumpCloud ou Okta, ou on-premises, como o Microsoft Active Directory. O objetivo é mapear automaticamente os perfis de um usuário do provedor de identidades para seus perfis de banco de dados quando esse usuário faz login em um cliente, como o editor de consultas V2, ou com um cliente JDBC. Para configurar isso, é necessário concluir algumas tarefas de configuração. Incluindo o seguinte:

1. Configure a integração federada com o provedor de identidades (IdP) usando uma relação de confiança. Isso é um pré-requisito. Depois dessa configuração, o provedor de identidades será responsável por autenticar o usuário via declaração SAML e por fornecer credenciais de login. Para obter mais informações, consulte Integrar provedores de soluções SAML de terceiros com a AWS. Você também pode encontrar mais informações em Federação de acesso ao editor de consultas v2 do Amazon Redshift com os Serviços de Federação do Active Directory (AD FS) ou Federação de acesso de logon único ao editor de consultas v2 do Amazon Redshift com Okta.
2. O usuário deve ter as seguintes permissões:
   - `GetCredentials`: fornece credenciais para autorização temporária de login no Amazon Redshift sem servidor.
   - `sts:AssumeRoleWithSAML`: fornece um mecanismo para vincular um armazenamento ou diretório de identidades corporativas ao acesso baseado em perfis da AWS.
   - `sts:TagSession`: permissão para a ação de sessão de etiquetas, na entidade principal do provedor de identidades.

   Nesse caso, `AssumeRoleWithSAML` retorna um conjunto de credenciais de segurança para usuários que foram autenticados via resposta autenticada por SAML. Essa operação fornece um mecanismo para vincular um armazenamento ou diretório de identidades ao acesso baseado em perfis da AWS sem credenciais específicas do usuário. Para usuários com permissão para `AssumeRoleWithSAML`, o provedor de identidades é responsável por gerenciar a declaração SAML usada para enviar as informações do perfil.

   Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.
3. Você configura a etiqueta `RedshiftDbRoles` com os valores de perfil separados por dois pontos, no formato role1:role2. Por exemplo, `.manager:engineer` Eles podem ser recuperados de uma implementação de etiqueta de sessão configurada em seu provedor de identidades. A solicitação de autenticação SAML envia os perfis de forma programática. Para obter mais informações sobre o envio de etiquetas de sessão, consulte Enviar etiquetas de sessão no AWS STS.

   Nos casos em que você envio um nome de perfil que não existe no banco de dados, ele é ignorado.

Nesse caso de uso, quando um usuário faz login usando uma identidade federada, seus perfis são enviados na solicitação de autorização por meio da chave e do valor da etiqueta de sessão. Depois

da autorização, `GetCredentials` envia os perfis para o banco de dados. Após uma conexão bem-sucedida, os perfis de banco de dados são mapeadas e o usuário pode executar tarefas de banco de dados correspondentes ao perfil. A parte essencial da operação é que a etiqueta de sessão `RedshiftDbRoles` receba os perfis na solicitação de autorização inicial. Para obter mais informações sobre o envio de etiquetas de sessão, consulte Enviar etiquetas de sessão usando AssumeRoleWithSAML.

Fazer login usando credenciais do IAM

No segundo caso de uso, os perfis podem ser enviados para um usuário e ele pode acessar uma aplicação cliente de banco de dados por meio de credenciais do IAM.

1. Nesse caso, o usuário que faz login deve receber permissões de política para as seguintes ações:
   - `tag:GetResources`: retorna os recursos marcados associados a etiquetas especificadas.
   - `tag:GetTagKeys`: retorna as chaves de etiqueta atualmente em uso.

     Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.
2. Permissões também são necessárias para acessar o serviço de banco de dados, como o Amazon Redshift sem servidor.
3. Para esse caso de uso, configure os valores das etiquetas para os perfis no AWS Identity and Access Management. Você pode optar por editar etiquetas e criar uma chave de etiqueta chamada redshiftDBRoles com uma string de valor de etiqueta que contém os perfis. Por exemplo, manager:engineer.

Quando um usuário faz login, seu perfil é adicionado à solicitação de autorização e enviado para o banco de dados. Ele é mapeado para um perfil de banco de dados existente.

## Recursos adicionais do

Conforme mencionado nos casos de uso, você pode configurar a relação de confiança entre seu IdP e a AWS. Para obter mais informações, consulte Configurar o IdP do SAML 2.0 com confiança da parte dependente e incluir declarações.

# Gerenciamento de Identidade e Acesso no Amazon Redshift Serverless

O acesso ao Amazon Redshift requer credenciais que a AWS pode usar para autenticar suas solicitações. Essas credenciais devem ter permissões para acessar os recursos da AWS, como o Amazon Redshift Serverless.

As seções a seguir fornecem detalhes sobre como você pode usar o AWS Identity and Access Management (IAM) e o Amazon Redshift para ajudar a proteger seus recursos, controlando quem pode acessá-los. Para obter mais informações, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift.

## Conceder as permissões necessárias para o Amazon Redshift Serverless

Para acessar outros produtos da AWS, o Amazon Redshift Serverless necessita de permissões.

### Autorizar o Amazon Redshift Serverless a acessar outros produtos da AWS para você

Alguns recursos do Amazon Redshift exigem que o Amazon Redshift acesse outros serviços da AWS em seu nome. Para que a instância do Amazon Redshift Serverless atue por você, forneça credenciais de segurança para ela. O método preferido para fornecer credenciais de segurança é especificar uma função do AWS Identity and Access Management (IAM). Também é possível criar uma função do IAM por meio do console do Amazon Redshift e defini-la como padrão. Para obter mais informações, consulte Criar uma função do IAM como padrão para o Amazon Redshift.

Para acessar outros produtos da AWS, crie uma função do IAM com as devidas permissões. Também é necessário associar a função ao Amazon Redshift Serverless. Além disso, especifique o nome do recurso da Amazon (ARN) da função ao executar o comando do Amazon Redshift ou especifique a palavra-chave `default`.

Ao alterar a relação de confiança do perfil do IAM em https://console.aws.amazon.com/iam/, verifique se ele contém `redshift-serverless.amazonaws.com` e `redshift.amazonaws.com` como nomes de serviço da entidade principal. Para obter informações sobre como gerenciar funções do IAM ´para acessar outros produtos da AWS em seu nome, consulte Autorizar o Amazon Redshift a acessar outros serviços da AWS em seu nome.

## Criar uma função do IAM como padrão para o Amazon Redshift

Quando você cria funções do IAM pelo console do Redshift, o Amazon Redshift cria as funções de maneira programática em sua Conta da AWS. O Amazon Redshift também anexa automaticamente políticas gerenciadas pela AWS a elas. Essa metodologia significa que você pode permanecer no console do Amazon Redshift e não precisa alternar para o console do IAM para criar a função.

A função do IAM que você cria pelo console do cluster tem a política gerenciada `AmazonRedshiftAllCommandsFullAccess` anexada automaticamente. Essa função do IAM permite que o Amazon Redshift copie, carregue, consulte e analise dados de recursos da AWS em sua conta do IAM. Os comandos relacinados incluem: COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL e CREATE LIBRARY. Para obter mais informações, sobre como criar uma função do IAM como padrão para o Amazon Redshift, consulte Criar uma função do IAM como padrão para o Amazon Redshift.

Para começar a criar um perfil do IAM como padrão para o Amazon Redshift, abra o AWS Management Console, escolha o console do Amazon Redshift e selecione Redshift sem servidor no menu. No painel Sem servidor, você pode criar um grupo de trabalho. As etapas de criação mostram como você seleciona um perfil do IAM ou configura um novo.

Quando você já tiver um grupo de trabalho do Amazon Redshift sem servidor e quiser configurar perfis do IAM para ele, abra o AWS Management Console. Escolha o console do Amazon Redshift e selecione Redshift sem servidor. No console do Amazon Redshift Serverless, escolha Configuração do namespace. Em Segurança e criptografia, você pode editar as permissões.

### Atribuir perfis do IAM a um namespace

Cada perfil do IAM é uma identidade da AWS com políticas de permissões que determinam quais ações cada função pode executar na AWS. A função pode ser assumida por qualquer pessoa que precise dela. Além disso, cada namespace é uma coleção de objetos, como tabelas e esquemas, e usuários. Ao usar o Amazon Redshift Serverless, você pode associar vários perfis do IAM ao namespace. Isso facilita a estruturação de suas permissões de forma adequada para uma coleção de objetos de banco de dados, para que as funções possam executar ações em dados internos e externos. Por exemplo, para que você possa executar um comando `COPY` em um banco de dados do Amazon Redshift para recuperar dados do Amazon S3 e preencher uma tabela do Redshift.

Você pode associar várias funções a um namespace usando o console, conforme descrito anteriormente nesta seção. Também é possível usar o comando `CreateNamespace` da API ou o comando `create-namespace` da CLI. Com o comando da API ou da CLI, você pode atribuir

perfis do IAM ao namespace preenchendo `IAMRoles` com um ou mais perfis. Especificamente, você adiciona ARNs para funções específicas à coleção.

Gerenciamento de perfis do IAM associados ao namespace

No AWS Management Console, você pode gerenciar políticas de permissões para perfis no AWS Identity and Access Management. É possível gerenciar os perfis do IAM para o namespace usando as configurações disponíveis em Namespace configuration (Configuração do namespace). Para obter mais informações sobre namespaces e seu uso no Amazon Redshift Serverless, consulte Visão geral dos grupos de trabalho e namespaces do Amazon Redshift Serverless.

## Conceitos básicos das credenciais do IAM para o Amazon Redshift

Ao fazer login no console do Amazon Redshift e experimentar o Amazon Redshift sem servidor pela primeira vez, recomendamos que você se conecte como usuário com um perfil do IAM anexado que tenha as políticas necessárias. Depois de começar a criar uma instância do Amazon Redshift sem servidor, o Amazon Redshift registra o nome do perfil do IAM que você usou ao fazer login. É possível usar as mesmas credenciais para fazer login no console do Amazon Redshift e no console do Amazon Redshift sem servidor.

Ao criar a instância do Amazon Redshift Serverless, você pode criar um banco de dados. Use o editor de consultas v2 para se conectar ao banco de dados com a opção de credenciais temporárias.

Para adicionar um novo nome e senha de usuário administrador que persistem para o banco de dados, escolha Customize admin user credentials (Personalizar credenciais de usuário administrador) e insira um novo nome de usuário administrador e senha de usuário administrador.

Para começar a usar o Amazon Redshift sem servidor e criar um grupo de trabalho e um namespace no console pela primeira vez, use um perfil do IAM com uma política de permissões anexada. Verifique se esse usuário ou perfil tem a permissão de administrador `arn:aws:iam::aws:policy/AdministratorAccess` ou a permissão completa do Amazon Redshift `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess` anexada à política do IAM.

Os cenários a seguir descrevem como suas credenciais do IAM são usadas pelo Amazon Redshift sem servidor ao iniciar o console do Amazon Redshift sem servidor:

- Se escolher Use default settings (Usar configurações padrão), o Amazon Redshift Serverless converterá sua identidade atual do IAM em um superusuário de banco de dados. É possível usar a mesma identidade do IAM com o console do Amazon Redshift Serverless para executar ações de superusuário no banco de dados do Amazon Redshift Serverless.

- Se escolher Customize settings (Personalizar configurações) sem especificar o Admin user name (Nome de usuário administrador) e a senha no Amazon Redshift Serverless, as credenciais atuais do IAM serão usadas como suas credenciais de usuário administrador padrão.
- Se escolher Customize settings (Personalizar configurações sem especificar Admin user name (Nome de usuário administrador) e senha no Amazon Redshift Serverless, o Amazon Redshift Serverless converterá sua identidade do IAM atual em superusuário de banco de dados. O Amazon Redshift Serverless criará outro par de nome de usuário e senha de login de longo prazo também como superusuário. É possível usar sua identidade do IAM atual ou o par de nome de usuário e senha criado para fazer login no banco de dados como superusuário.

## Gerenciar o acesso aos objetos do banco de dados do Amazon Redshift sem servidor com permissões de perfil de banco de dados

Esse procedimento mostra como conceder permissão para consultar uma tabela por meio de um perfil de banco de dados do Amazon Redshift. O perfil é atribuído por meio de uma tag anexada a um usuário no IAM e passada para o Amazon Redshift durante o login. É uma explicação com exemplo dos conceitos em Definir perfis de banco de dados para conceder a usuários federados no Amazon Redshift sem servidor. A vantagem de concluir essas etapas é que você pode associar um usuário a um perfil de banco de dados e evitar definir as respectivas permissões para cada objeto de banco de dados. Ele simplifica o gerenciamento da capacidade do usuário de consultar, modificar ou adicionar dados às tabelas e realizar outras ações.

O procedimento pressupõe que você já tenha configurado um banco de dados do Amazon Redshift sem servidor e possa conceder permissões no banco de dados. Ele também pressupõe que você tenha permissões para criar um usuário do IAM no console da AWS, criar um perfil do IAM e atribuir permissões de política.

1. Crie um usuário do IAM usando o console do IAM. Posteriormente, você se conectará ao banco de dados com esse usuário.
2. Crie um perfil de banco de dados do Redshift usando o editor de consultas v2 ou outro cliente SQL. Para obter mais informações sobre como criar perfis de banco de dados, consulte CREATE ROLE.

   ```
   CREATE ROLE urban_planning;
   ```

Consulte a visualização do sistema SVV_ROLES para verificar se o perfil foi criado. Ela também retorna perfis do sistema.

```
SELECT * from SVV_ROLES;
```

3. Conceda permissão ao perfil de banco de dados que você criou para selecionar em uma tabela. (O usuário do IAM que você criou acabará se conectando e selecionando registros da tabela por meio do perfil do banco de dados.) O nome do perfil e o nome da tabela na amostra de código a seguir são exemplos. Aqui, é concedida permissão para selecionar em uma tabela chamada `cities`.

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

4. Use o console do AWS Identity and Access Management para criar um perfil do IAM. Esse perfil concede permissão para usar o editor de consultas v2. Crie um perfil do IAM e, para o tipo de entidade confiável, escolha Conta da AWS. Depois, selecione Esta conta. Conceda ao perfil as seguintes permissões de política:

   - `AmazonRedshiftReadOnlyAccess`
   - `tag:GetResources`
   - `tag:GetTagKeys`
   - Todas as ações para sqlworkbench, incluindo `sqlworkbench:ListDatabases` e `sqlworkbench:UpdateConnection`.

5. No console do IAM, adicione uma tag com a chave `RedshiftDbRoles` para o usuário do IAM que você criou anteriormente. O valor da tag deve corresponder ao perfil do banco de dados que você criou na primeira etapa. É `urban_planning` na amostra.

Depois de concluir essas etapas, atribua o perfil do IAM ao usuário que você criou no console do IAM. Quando o usuário faz login no banco de dados com o editor de consultas v2, o nome do perfil de banco de dados na tag é passado para o Amazon Redshift e associado a ele. Assim, eles podem consultar as tabelas apropriadas por meio do perfil de banco de dados. Para ilustrar, o usuário neste exemplo pode consultar a tabela `cities` por meio do perfil de banco de dados `urban_planning`.

# Migrar um cluster provisionado para o Amazon Redshift Serverless

Para migrar um cluster provisionado para o Amazon Redshift Serverless, siga as etapas a seguir.

# Criar um snapshot do cluster provisionado

Para transferir dados do cluster provisionado para o Amazon Redshift Serverless, crie um snapshot do cluster provisionado e restaure o snapshot no Amazon Redshift Serverless. O Amazon Redshift converte automaticamente chaves intercaladas em chaves compostas quando você restaura um snapshot de cluster provisionado para um namespace de tecnologia sem servidor.

> **Note**
>
> Antes de migrar seus dados para um grupo de trabalho com tecnologia sem servidor, garanta que suas necessidades de cluster provisionado sejam compatíveis com a quantidade de RPU que você escolher no Amazon Redshift Serverless.

Para criar um snapshot do cluster provisionado

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, Snapshots e Create snapshot (Criar snapshot).
3. Insira as propriedades da definição do snapshot e escolha Create snapshot (Criar snapshot). Pode levar algum tempo para o snapshot estar disponível.

Para restaurar um snapshot de cluster provisionado para um namespace de tecnologia sem servidor:

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. Comece no console do cluster provisionado do Amazon Redshift e navegue até a página Clusters, Snapshots.
3. Escolha um snapshot para usar.
4. Selecione Restore from snapshot (Restaurar a partir do snapshot), Restore to serverless namespace (Restaurar para namespace com tecnologia sem servidor).
5. Escolha um namespace para o qual deseja restaurar o snapshot.
6. Confirme que você deseja restaurar a partir do snapshot. Essa ação substitui todos os bancos de dados de seu endpoint sem servidor pelos dados do cluster provisionado. Escolha Restore.

Para obter mais informações sobre snapshots de cluster provisionado, consulte Snapshots do Amazon Redshift.

## Conexão com o Amazon Redshift sem servidor usando um driver

Para conectar ao Amazon Redshift Serverless com o cliente SQL de sua preferência, é possível usar o driver JDBC versão 2 fornecido pelo Amazon Redshift. Recomendamos conectar usando o driver JDBC versão 2.1.x ou posterior. O número da porta é opcional. Se você não o incluir, o Amazon Redshift Serverless usará como padrão a porta número 5439. Você pode mudar para outra porta do intervalo de portas 5431–5455 ou 8191–8215. Para alterar a porta padrão de um endpoint de tecnologia sem servidor, use a AWS CLI e a API do Amazon Redshift.

Para encontrar o endpoint exato a ser usado para o driver JDBC, ODBC ou Python, consulte Configuração do grupo de trabalho no Amazon Redshift sem servidor. Também é possível usar a operação `GetWorkgroup` da API do Amazon Redshift sem servidor ou a operação `get-workgroups` da AWS CLI para retornar informações sobre seu grupo de trabalho, depois conectar-se.

### Conectar-se usando autenticação baseada em senha

Para se conectar usando a autenticação baseada em senha, use a sintaxe a seguir.

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

Para conectar usando o driver Python do Amazon Redshift, use a sintaxe a seguir.

```
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
```

## Conectar-se usando IAM

Se você preferir fazer login com o IAM, use o endpoint de driver a seguir. Esse endpoint de driver permite que você se conecte a um banco de dados específico e use a operação da API `GetCredentials` do Amazon Redshift Serverless.

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

Esse endpoint de driver não é compatível com personalização de `dbUser`, `dbGroup` e `auto-create`. Por padrão, o driver cria automaticamente usuários do banco de dados no login e os atribui aos grupos de acordo com os grupos que você definiu no IAM. Observação: os nomes de grupo que você especifica no IAM devem conter somente letras minúsculas, números, sublinhado (_), sinal de adição (+), ponto (.), arroba (@) ou hífen (-). Caso contrário, o driver pode não se conectar ao `dbGroup`.

Certifique-se de que sua identidade da AWS tenha a política do IAM correta para a ação `RedshiftServerlessGetCredentials`. Veja a seguir um exemplo de política do IAM que concede as permissões corretas para uma identidade da AWS se conectar ao Amazon Redshift Serverless. Para obter mais informações sobre as permissões do IAM, consulte Adicionar permissões de identidade do IAM.

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

## Conectar-se usando o IAM com dbUser e dbGroups

Se você quiser usar as opções de conexão dbUser e dbGroup personalizadas, use o endpoint de driver a seguir. Como o outro endpoint de driver do Amazon Redshift Serverless, essa sintaxe cria automaticamente usuários de banco de dados no login. Esse endpoint de driver usa a operação de

API GetCredentials do Amazon Redshift sem servidor. O dbUser deve começar com uma letra, deve conter somente caracteres alfanuméricos, sublinhado (_), sinal de adição (+), ponto (.), arroba (@) ou hífen (-), e deve conter no máximo 128 caracteres. O dbGroups deve conter somente letras minúsculas, números, sublinhado (_), sinal de adição (+), ponto (.), arroba (@) ou hífen (-).

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

Para conectar usando o driver Python do Amazon Redshift, use a sintaxe a seguir.

```
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
```

### Conexão usando ODBC

Para conectar usando ODBC, use a sintaxe a seguir.

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

## Usando o SDK do Amazon Redshift Serverless

Se você escreveu scripts de gerenciamento usando o SDK do Amazon Redshift, deverá usar o novo SDK do Amazon Redshift sem servidor para gerenciar o Amazon Redshift sem servidor e os recursos associados. Para obter mais informações sobre as operações da API disponíveis, consulte o Guia de referência da API do Amazon Redshift Serverless.

# Visão geral dos grupos de trabalho e namespaces do Amazon Redshift Serverless

Para isolar workloads e gerenciar diferentes recursos no Amazon Redshift Serverless, você pode criar namespaces e grupos de trabalho e gerenciar recursos de armazenamento e computação separadamente.

## Visão geral de grupos de trabalho e namespaces do Amazon Redshift Serverless

O namespace é uma coleção de objetos e usuários do banco de dados. O namespace relacionado ao armazenamento agrupa esquemas, tabelas, usuários ou chaves do AWS Key Management Service para criptografar dados. As propriedades de armazenamento incluem o nome do banco de dados e a senha do usuário administrador, permissões, criptografia e segurança. Outros recursos agrupados em namespaces incluem unidades de compartilhamento de dados, pontos de recuperação e limites de uso. É possível configurar essas propriedades de armazenamento usando o console do Amazon Redshift Serverless, a AWS Command Line Interface ou as APIs do Amazon Redshift Serverless para o recurso específico.

O grupo de trabalho é uma coleção de recursos de computação. Os grupos de trabalho relacionados à computação agrupam recursos de computação, como RPUs, grupos de sub-redes da VPC e grupos de segurança. As propriedades do grupo de trabalho incluem configurações de rede e segurança. Outros recursos agrupados em grupos de trabalho incluem limites de acesso e uso. É possível configurar essas propriedades de computação usando o console do Amazon Redshift Serverless, a AWS Command Line Interface ou as APIs do Amazon Redshift Serverless.

Você pode criar um ou mais namespaces e grupos de trabalho. Cada namespace só pode ter um grupo de trabalho associado a ele. Por sua vez, cada grupo de trabalho só pode ser associado a um namespace.

### Conceitos básicos do Amazon Redshift Serverless usando o console

Configurar o Amazon Redshift Serverless envolve percorrer várias etapas de configuração. Ao seguir as etapas para configurar o Amazon Redshift Serverless, você cria um namespace e um grupo de trabalho e associa um ao outro. Para começar a definir a configuração do Amazon Redshift Serverless usando o console do Amazon Redshift Serverless, você pode escolher Get started with Amazon Redshift Serverless (Conceitos básicos do Amazon Redshift Serverless) para configurar

o Amazon Redshift Serverless e começar a interagir com ele. Você pode escolher um ambiente com configurações padrão, o que torna a configuração mais rápida, ou definir explicitamente as configurações de acordo com os requisitos da sua organização. Durante esse processo, você especifica as configurações para seu grupo de trabalho e namespace.

Depois de configurar o ambiente, Propriedades de grupo de trabalho e Propriedades de namespace ajudam você a se familiarizar com as configurações.

## Gerenciamento dos grupos de trabalho e namespaces usando a AWS Command Line Interface e a API do Amazon Redshift sem servidor

Além de usar o console da AWS, também é possível usar a AWS CLI ou a API do Amazon Redshift sem servidor para interagir com grupos de trabalho e namespaces. A tabela abaixo lista as operações de API e CLI que é possível usar para gerenciar snapshots e pontos de recuperação.

| Operação de API | Comando da CLI | Descrição |
|---|---|---|
| CreateNamespace | create-namespace | Cria um namespace. Por padrão, o Amazon Redshift sem servidor cria namespaces com uma chave AWS Key Management Service padrão, mas é possível especificar outra chave para criptografar os dados. Você também pode criar um namespace restaurando um snapshot. Consulte Working with snapshots and recovery points para obter mais informações. |
| UpdateNamespace | update-namespace | Atualiza um namespace. |
| GetNamespace | get-namespace | Recupera informações sobre um namespace. |
| ListNamepaces | list-namespaces | Recupera informações sobre uma lista de namespaces. |

| Operação de API | Comando da CLI | Descrição |
| --- | --- | --- |
| DeleteNamespace | delete-namespace | Exclui um namespace. |
| CreateWorkgroup | create-workgroup | Cria um grupo de trabalho. Ao criar um grupo de trabalho, verifique se você tem um namespace existente que é possível associar ao grupo de trabalho. Ao criar o grupo de trabalho, você pode especific ar recursos computacionais, como sub-redes, grupos de segurança ou RPUs. |
| UpdateWorkgroup | update-workgroup | Atualiza um grupo de trabalho. |
| GetWorkgroup | get-workgroup | Recupera informações sobre um grupo de trabalho. |
| ListWorkgroups | list-workgroups | Recupera informações sobre uma lista de grupos de trabalho. |
| DeleteWorkgroup | delete-workgroup | Exclui um grupo de trabalho. |

# Gerenciar o Amazon Redshift Serverless usando o console

Para criar, editar e excluir seu data warehouse do Amazon Redshift Serverless, use o Serverless dashboard (Painel do Serverless) no console do Amazon Redshift. O acesso a configurações específicas do console depende do perfil do IAM e das permissões que você tem.

Para obter mais informações sobre como configurar o Amazon Redshift Serverless, consulte Configurar o Amazon Redshift Serverless pela primeira vez. Para obter informações sobre como criar e configurar grupos de trabalho, consulte Trabalhar com grupos de trabalho. Para obter informações sobre como configurar namespaces, consulte Trabalhar com namespaces.

# Configurar o Amazon Redshift Serverless pela primeira vez

A primeira vez que seleciona o Serverless dashboard (Painel do Serverless), ele apresenta as etapas para configurar o Amazon Redshift Serverless. Em Get started with the serverless experience (Conceitos básicos da experiência com a tecnologia sem servidor), você pode configurar um data warehouse do Amazon Redshift Serverless usando um conjunto de dados de exemplo. O Amazon Redshift Serverless carrega automaticamente o conjunto de dados de dados de exemplo durante o processo de criação. Depois que o data warehouse é criado, você pode consultar dados imediatamente. Para obter mais informações sobre como configurar o Amazon Redshift Serverless pela primeira vez, consulte "Set up Amazon Redshift Serverless for the first time" (Configurar o Amazon Redshift Serverless pela primeira vez).

# Trabalhar com grupos de trabalho

Para isolar workloads e gerenciar recursos no Amazon Redshift Serverless, você pode criar grupos de trabalho e namespaces. Os grupos de trabalho relacionados à computação agrupam recursos de computação, como RPUs e grupos de sub-redes da VPC. Se você não criou um grupo de trabalho e um namespace e está procurando instruções que mostrem como começar a usar o Amazon Redshift Serverless, consulte Configurar o Amazon Redshift Serverless pela primeira vez.

## Criar um grupo de trabalho com um namespace

Estas etapas pressupõem que você concluiu a configuração inicial do Amazon Redshift Serverless. Se você não criou um grupo de trabalho e um namespace e está procurando instruções que mostrem como começar a usar o Amazon Redshift Serverless, consulte Configurar o Amazon Redshift Serverless pela primeira vez.

Para criar um grupo de trabalho, conclua as seguintes etapas:

1. Escolha o Serverless dashboard (Painel do Serverless). Escolha Create workgroup (Criar grupo de trabalho).
2. Insira o nome do grupo de trabalho.
3. Escolha uma Virtual private cloud (VPC) (Nuvem privada virtual (VPC)) para o Amazon Redshift Serverless. Isso atribui o grupo de trabalho a uma rede virtual específica em seu ambiente da AWS. Para obter mais informações sobre VPCs, consulte Visão geral de VPCs e sub-redes.
4. Escolha um ou mais VPC security groups (Grupos de segurança da VPC). Para obter mais informações, consulte Controlar o tráfego para recursos usando grupos de segurança.

5. Em Subnet (Sub-rede), especifique uma ou mais sub-redes para associar ao seu banco de dados. Essas sub-redes estão contidas na VPC que você escolheu anteriormente e devem estar em três zonas de disponibilidade distintas. Para obter informações, consulte Considerações ao usar o Amazon Redshift Serverless.
6. Selecione a capacidade de base da RPU em conformidade com seus requisitos.

Escolher um namespace

1. Escolha Create a new namespace (Criar um namespace) e insira o nome do namespace, ou Add to an existing namespace (Adicionar a um namespace existente) e selecione o namespace na lista suspensa.
2. Em Database name and password (Nome e senha do banco de dados), especifique o nome do primeiro banco de dados. Você também pode especificar um administrador diferente do administrador do console padrão, editando as Admin user credentials (Credenciais do usuário administrador).
3. Em Permissions (Permissões), você escolhe Associate IAM role (Associar perfil do IAM) para associar perfis do IAM ao namespace e ao grupo de trabalho. Para obter mais informações sobre como associar perfis do IAM ao Amazon Redshift, consulte Gerenciamento de identidade e acesso no Amazon Redshift.
4. Você pode personalizar as configurações de criptografia criando uma chave ou escolhendo uma chave diferente da padrão. Em Audit logging (Registro em log de auditoria), escolha os logs a serem exportados. Cada tipo de log especifica metadados diferentes. Selecione Continue (Continuar) para revisar suas escolhas.

Revisar as escolhas do grupo de trabalho

1. Revise as configurações em Review and create (Revisar e criar). Essa seção mostra as configurações que você escolheu nas etapas anteriores.
2. Escolha Salvar.

Depois de criar o grupo de trabalho, ele é adicionado à lista de Workgroups (Grupos de trabalho).

## Criar visualização prévia de grupo de trabalho

Para testar novos recursos do Amazon Redshift sem servidor, crie um grupo de trabalho do Amazon Redshift sem servidor em Visualização prévia. Você não pode usar esses recursos em

produção nem mover seu grupo de trabalho de Preview (Pré-visualização) para um grupo de trabalho de produção. Para conferir os termos e condições da pré-visualização, consulte Betas e pré-visualizações nos Termos de serviços da AWS.

Os seguintes recursos estão disponíveis em grupos de trabalho em pré-visualização no momento:

- Trabalho com Integrações ETL zero

Como criar um grupo de trabalho em Preview (Pré-visualização)

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Painel do Serverless e escolha Configuração do grupo de trabalho. Os grupos de trabalho de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada grupo de trabalho é exibido nas colunas na lista.
3. Um banner na página Configuração do grupo de trabalho apresenta grupos de trabalho em pré-visualização. Escolha o botão Create preview workgroup (Criar grupo de trabalho de pré-visualização) para abrir a página de criação de grupo de trabalho.
4. Insira as propriedades para o grupo de trabalho. Recomendamos inserir um nome que indique que o grupo de trabalho está em versão de pré-visualização. Escolha opções para o grupo de trabalho, incluindo opções rotuladas como -preview (-pré-visualização), para os recursos que deseja testar. Continue pelas páginas para inserir opções para o grupo de trabalho e namespace. Para obter informações gerais sobre como criar grupos de trabalho, consulte the section called “Criar um grupo de trabalho com um namespace”.
5. Escolha Criar para criar um grupo de trabalho em pré-visualização.
6. Quando seu grupo de trabalho de pré-visualização estiver disponível, use seu cliente SQL para carregar e consultar dados.

Para obter informações sobre a pré-visualização em clusters provisionados, consulte Criar cluster de visualização prévia.

## Exibir as propriedades de um grupo de trabalho

No Amazon Redshift Serverless, um grupo de trabalho é uma coleção de recursos disponíveis para uso. Ao escolher o Amazon Redshift Serverless, no Console da AWS, você pode escolher Workgroup configuration (Configuração do grupo de trabalho) no menu de navegação para

visualizar uma lista. Você pode usar a caixa Search (Pesquisar) para encontrar grupos de trabalho que atendam aos seus critérios de pesquisa. Cada entrada do grupo de trabalho tem algumas propriedades exibidas:

- Workgroup (Grupo de trabalho): o nome do grupo de trabalho. Você pode selecioná-lo para exibir e editar as propriedades do grupo de trabalho.
- Status: mostra se o grupo de trabalho está disponível.
- Namespace: o namespace associado ao grupo de trabalho. Cada grupo de trabalho é associado a um namespace.
- Creation date (Data de criação): a data em que o grupo de trabalho foi criado.
- Etiquetas: etiquetas associadas ao grupo de trabalho.

### Propriedades de grupo de trabalho

Você pode listar grupos de trabalho escolhendo Workgroup configuration (Configuração do grupo de trabalho) no menu à esquerda. Depois, você pode escolher um grupo de trabalho na lista. Vários painéis mostram propriedades para o grupo de trabalho. Você também pode executar ações. General information (Informações gerais) exibe o seguinte:

- Workgroup (Grupo de trabalho): o nome do grupo de trabalho.
- Namespace: o namespace associado ao grupo de trabalho. Você pode optar por visualizar suas propriedades. Um grupo de trabalho é associado a um único namespace.
- Date created (Data de criação): quando o grupo de trabalho foi criado.
- Status: indica se os recursos do grupo de trabalho estão disponíveis. Se estiver disponível, você poderá se conectar com um cliente à instância do Amazon Redshift Serverless, para consultar dados ou criar recursos de banco de dados, ou poderá se conectar com o editor de consultas v2.
- Endpoint: o URL.
- JDBC URL (URL do JDBC): o URL para estabelecer conexões de cliente JDBC. É possível usar esse URL a fim de se conectar a um driver JDBC para o Amazon Redshift. Para obter mais informações, consulte Configurar uma conexão para um driver JDBC versão 2.1 para o Amazon Redshift.
- ODBC URL (URL do ODBC): o URL para estabelecer conexões de cliente ODBC. Ele contém propriedades, como o banco de dados e o ID do usuário, e seus valores.
- Versão do grupo de trabalho e versão do patch: o Amazon Redshift sem servidor lança regularmente versões e patches novos. Você pode usar a versão do grupo de trabalho e os

números da versão do patch para rastrear atualizações de software até o grupo de trabalho do Amazon Redshift sem servidor. Para obter mais informações sobre alterações e recursos em patches específicos, consulte Cluster versions for Amazon Redshift.

A guia Data access (Acesso aos dados) contém vários painéis:

- Network and security (Rede e segurança): você pode ver as propriedades da rede, como o identificador da Virtual private cloud (VPC) (Nuvem privada virtual (VPC)), a lista VPC security group (Grupo de segurança da VPC), o Enhanced VPC routing (Roteamento de VPC aprimorado) e a configuração Publicly accessible (Acessível publicamente). Se escolher Edit (Editar), você poderá alterar essas configurações. Além disso, você pode selecionar Turn on enhanced VPC routing (Ativar o roteamento aprimorado de VPC), que roteia o tráfego de rede entre o banco de dados sem servidor e repositórios de dados por meio de uma VPC, para maior privacidade e segurança. Você também pode selecionar Turn on Public Accessible (Tornar acessível ao público), o que torna o banco de dados acessível publicamente de fora da VPC, permitindo que instâncias e dispositivos se conectem.
- Redshift managed VPC endpoints (Endpoints da VPC gerenciados pelo Redshift): você pode criar endpoints da VPC gerenciados para acessar o Amazon Redshift Serverless de outra VPC.

A guia Limits (Limites) tem configurações para controlar os limites de uso e capacidade do Amazon Redshift Serverless. Ela contém os seguintes painéis:

- Base capacity in Redshift processing units (RPUs) (Capacidade inicial em unidades de processamento do Redshift (RPUs)): é possível definir a capacidade inicial dos recursos de computação usados para processar a workload. Para ter mais informações, consulte Noções básicas sobre a capacidade do Amazon Redshift Serverless.
- Limites de uso: é possível configurar até quatro limites para o máximo de recursos computacionais que a instância do Amazon Redshift sem servidor pode usar em um período e selecionar ações para o Amazon Redshift sem servidor realizar ao atingir esses limites. Por exemplo, é possível definir o grupo de trabalho para ter dois limites, um de 500 horas de RPU e outro de 900 horas de RPU. É possível fazer o Amazon Redshift sem servidor enviar um alerta quando atingir o primeiro limite de 500 horas de RPU e, em seguida, desativar as consultas do usuário quando atingir o segundo limite de 900 horas. Esses limites ajudam a controlar os custos e deixá-los mais previsíveis.
- Query limits (Limites de consulta): você pode definir limites para consultas, como a configuração de tempo limite. Esses limites ajudam você a otimizar o custo e a performance.

A guia Guias tem o painel Etiquetas, que mostra todas as etiquetas criadas por você criou para o grupo de trabalho. Para obter mais informações sobre como marcar recursos, consulte Visão geral dos recursos de marcação.

## Excluir um grupo de trabalho

É possível excluir um grupo de trabalho usando o console. Antes de fazer isso, faça backup dos dados e crie snapshots. Recursos excluídos como parte do grupo de trabalho em muitos casos não podem ser recuperados.

Execute as etapas a seguir:

1. Selecione Amazon Redshift Serverless, escolha Workgroup configuration (Configuração do grupo de trabalho) e Delete Amazon Redshift Serverless instance (Excluir instância do Amazon Redshift Serverless).

2. Uma caixa de diálogo é aberta. Quando você opta por excluir o grupo de trabalho, todos os limites de uso são removidos, todos os endpoints da VPC são removidos e o acesso aos endpoints da VPC é removido.

   Digite delete (excluir) e selecione Delete (Excluir) para confirmar.

Depois de concluir as etapas, o status do grupo de trabalho será Deleting (Excluindo) e um banner indicará que o grupo de trabalho está sendo excluído. Enquanto o processo de exclusão estiver em andamento, alguns recursos do Serverless dashboard (Painel do Serverless) ficarão desabilitados. Mas você pode configurar clusters provisionados no Provisioned clusters dashboard (Painel de clusters provisionados).

Depois de excluir o grupo de trabalho, ele não aparecerá com o namespace. Você pode selecionar o botão Create workgroup (Criar grupo de trabalho) para criar um.

Você pode excluir um grupo de trabalho existente e associar um novo grupo de trabalho com uma configuração diferente ao mesmo namespace. Ao criar outro grupo de trabalho, escolha a capacidade inicial que funciona com o tamanho dos dados associados ao namespace.

É possível associar um grupo de trabalho a um namespace criado com uma chave gerenciada pelo cliente (CMK). Para obter mais informações sobre o AWS KMS, consulte Conceitos do AWS KMS.

# Trabalhar com namespaces

No Amazon Redshift Serverless, um namespace define um contêiner lógico para objetos de banco de dados. Ele pode conter tabelas, grupos de trabalho e outros recursos do banco de dados. Se você não criou um grupo de trabalho e um namespace e está procurando instruções sobre como começar a usar o Amazon Redshift Serverless, consulte Configurar o Amazon Redshift Serverless pela primeira vez.

## Pesquisar um namespace

No menu do Amazon Redshift, você pode escolher pela lista de Namespaces para visualizar ou editar as propriedades de um namespace. As informações no console incluem o nome do namespace, o nome do administrador e outras propriedades.

As configurações e propriedades de um namespace estão em várias guias. Incluindo o seguinte:

- Workgroup (Grupo de trabalho): mostra os grupos de trabalho associados ao namespace.
- Data back up (Backup de dados): você pode configurar e criar snapshots e configurar pontos de recuperação.
- Security and encryption (Segurança e criptografia): você pode gerenciar permissões de perfil do IAM e visualizar ou editar suas configurações de segurança e criptografia. Isso inclui o status da chave de criptografia e as configurações de registro de auditoria.
- Datashares (Unidade de compartilhamento de dados): mostra as unidades de compartilhamento de dados.

## Propriedades de namespace

No Amazon Redshift Serverless, um namespace define um contêiner para objetos de banco de dados. É possível selecionar Namespace configuration (Configuração do namespace) na lista de navegação, escolher um namespace na lista e editar suas configurações.

As informações gerais do namespace incluem o seguinte:

- Namespace: o nome.
- Namespace ID (ID do namespace): o identificador exclusivo.
- ARN: um identificador exclusivo usado para especificar o recurso na AWS. Ele contém propriedades como a região e o serviço.

- Status: o status, como Available (Disponível).
- Date created (Data de criação): a data em que o namespace foi criado.
- Storage used (Armazenamento usado): o espaço de armazenamento usado pelo namespace e todos os seus objetos.
- Admin user name (Nome de usuário do administrador): a conta de administrador. Normalmente, essa é a conta usada para criar o namespace.
- Database name (Nome do banco de dados): o nome do banco de dados contido pelo namespace.
- Total table count (Contagem total de tabelas): a contagem de tabelas em todos os esquemas.

Configurações e propriedades adicionais para o namespace estão em várias guias. Incluindo o seguinte:

- Workgroup (Grupo de trabalho): mostra o grupo de trabalho associado ao namespace.
- Data back up (Backup de dados): nesse painel, você pode configurar e criar snapshots e configurar pontos de recuperação.
- Security and encryption (Segurança e criptografia): você pode gerenciar permissões de perfil do IAM e visualizar ou editar suas configurações de segurança e criptografia. Isso inclui o status da chave de criptografia e as configurações para ativar um registro de auditoria. Para obter mais informações sobre o registro de auditoria do Amazon Redshift Serverless, consulte Registro de auditoria do Amazon Redshift Serverless.
- Datashares (Unidade de compartilhamento de dados): mostra as unidades de compartilhamento de dados. Com o compartilhamento de dados, você pode fornecer acesso aos dados sem a necessidade de copiá-los ou movê-los. Para obter mais informações sobre o compartilhamento de dados, consulte Compartilhar dados no Amazon Redshift Serverless.

## Editar a segurança e a criptografia

O Amazon Redshift Serverless é protegido por meio de criptografia do KMS. Você pode atualizar as configurações de criptografia usando o console:

1. Selecione Namespace configuration (Configuração do namespace) no menu principal do console, escolha o namespace a ser editado e selecione Edit (Editar) na guia Security and encryption (Segurança e criptografia). Uma caixa de diálogo é exibida.
2. Você pode selecionar Personalizar configurações de criptografia e  Selecionar uma chave gerenciada pelo cliente da AWS a fim de alterar a chave usada para criptografar os recursos.

3. Em Audit logging (Registro em log de auditoria), escolha os logs a serem exportados. Cada tipo de log especifica metadados diferentes.
4. Para concluir a atualização de configuração, escolha Save changes (Salvar alterações).

## Alterar a chave do AWS KMS de um namespace

No Amazon Redshift, os dados em repouso são protegidos por criptografia. O Amazon Redshift Serverless usa a criptografia da chave do AWS KMS automaticamente para criptografar os recursos e snapshots do Amazon Redshift Serverless. Como uma prática recomendada, a maioria das organizações analisa o tipo de dados que armazenam e tem um plano para alternar as chaves de criptografia em uma programação. A frequência de alternância das chaves pode variar dependendo das políticas de segurança dos dados. O Amazon Redshift Serverless permite a alteração da chave do AWS KMS do namespace para que você possa aderir às políticas de segurança da sua organização.

Quando você altera a chave do AWS KMS, os dados permanecem inalterados.

Alterar uma chave do AWS KMS usando o console

No Amazon Redshift, os dados em repouso são protegidos por criptografia. O Amazon Redshift Serverless usa a criptografia da chave do AWS KMS automaticamente para criptografar snapshots do Amazon Redshift Serverless. Como uma prática recomendada, a maioria das organizações analisa o tipo de dados que armazenam e tem um plano para alternar as chaves de criptografia em uma programação. A frequência de alternância das chaves pode variar dependendo das políticas de segurança dos dados. O Amazon Redshift Serverless permite a alteração da chave do AWS KMS do namespace para que você possa aderir às políticas de segurança da sua organização.

Quando você altera a chave do AWS KMS, os dados permanecem inalterados.

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Namespace configurations (Configurações do namespace). Escolha o namespace na lista.
3. Na guia Security and encryption (Segurança e criptografia), selecione Edit (Editar).
4. Selecione Customize encryption settings (Personalizar configurações de criptografia) e escolha uma chave para o namespace. Se preferir, crie uma chave.

Alterar as chaves de criptografia do AWS KMS usando a AWS CLI

Use `update-namespace` para alterar a chave do AWS KMS do namespace. Veja a seguir a sintaxe do comando:

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

Você deve ter um namespace criado ou o comando da CLI resultará em um erro.

O tempo necessário para alterar a chave depende da quantidade de dados no Amazon Redshift Serverless. Isso geralmente leva quinze minutos para cada 8 TB de dados armazenados.

Limitações

Não é possível mudar de uma chave do KMS gerenciada pelo cliente para uma chave do AWS KMS. Nesse caso, é preciso criar um namespace.

Você não pode executar outras ações enquanto a chave está sendo alterada.

### Excluir um namespace

Se você quiser excluir um namespace com um grupo de trabalho associado, primeiro será necessário excluir o grupo de trabalho.

No console do Amazon Redshift Serverless, conclua as seguintes etapas:

1. Selecione Namespace configuration (Configuração do namespace) no menu à esquerda e escolha o namespace que deseja excluir da lista.
2. Selecione Actions (Ações) e escolha Delete namespace (Excluir namespace).
3. Uma caixa de diálogo é aberta. Você pode manter seus dados criando um snapshot manual antes de concluir a operação de exclusão.

   Digite delete (excluir) e selecione Delete (Excluir) para confirmar.

## Gerenciar limites de uso, limites de consulta e outras tarefas administrativas

Você pode definir as configurações no console para controlar o uso e limitar o custo.

## Gerenciar limites de uso, incluindo a definição de limites de RPU

Na guia Limits (Limites) de um grupo de trabalho, você pode adicionar um ou mais limites de uso para controlar o máximo de RPUs que você usa em determinado período ou para definir um limite de uso de compartilhamento de dados.

1. Selecione Manage usage limits (Gerenciar limites de uso). A seção de limites é exibida na parte inferior do painel Uso de computação por período.
2. Estabeleça um limite de uso, em número de horas de RPU.
3. Escolha uma Frequência, que é Diária, Semanal ou Mensal. Isso define o período para o limite de uso. A opção Daily (Diária) oferece um controle mais detalhado.
4. Defina um limite de uso, em número de horas.
5. Defina a ação. Elas podem ser as seguintes:

   - Log to system table (Registrar na tabela do sistema): adiciona um registro a uma tabela do sistema, que você pode consultar para determinar se o limite é excedido.
   - Alert (Alerta): usa o Amazon SNS para configurar assinaturas de notificação e enviar notificações se um limite for violado. Você pode escolher um tópico existente do Amazon SNS ou criar um.
   - Turn off user queries (Desativar as consultas do usuário): desativa consultas para interromper o uso do Amazon Redshift Serverless. Também é enviada uma notificação.

   As duas primeiras ações são informativas, mas a última desativa o processamento de consultas.
6. Se preferir, defina um Cross-Region data sharing usage limit (Limite de uso do compartilhamento de dados entre regiões), o que limita a quantidade de dados transferidos da região de produtor para a região de consumidor que os consumidores podem consultar. Para fazer isso, escolha Add limit (Adicionar limite) e siga as etapas.
7. Escolha Salvar alterações na parte inferior da página para salvar o limite.
8. Configure até mais três limites conforme necessário.

Para obter mais informações conceituais sobre RPUs e cobranças, consulte Faturamento do Amazon Redshift Serverless.

## Gerenciar limites de consulta

Na guia Limits (Limites) de um grupo de trabalho, você pode adicionar um limite para monitorar o desempenho e os limites. Para obter mais informações sobre os limites de monitoramento de consultas, consulte Regras de monitoramento de consultas do WLM.

1. Selecione Manage query limits (Gerenciar limites de consulta). Selecione Add new limit (Adicionar novo limite) na caixa de diálogo Manage query limits (Gerenciar limites de consulta).
2. Escolha o tipo de limite que deseja definir e insira um valor para o limite correspondente.
3. Escolha Save changes (Salvar alterações) para salvar o limite.

Quando você altera o limite de consulta e os parâmetros de configuração, o banco de dados é reiniciado.

## Filtrar consultas

Você pode usar os filtros disponíveis no painel sem servidor. Para adicionar consultas, execute as etapas a seguir.

1. À esquerda do painel Query summary (Resumo de consultas), selecione a lista suspensa para filtrar por consultas concluídas, consultas com falha ou ambas.
2. À direita do painel Query summary (Resumo de consultas), selecione a lista suspensa para filtrar por consultas em execução, consultas em fila ou ambas.

## Alterar a senha de administrador

1. Escolha Namespace configuration (Configuração de namespace). Selecione Change admin password (Alterar senha do administrador). Uma caixa de diálogo é exibida.
2. Você pode especificar um New admin username (Novo nome de usuário administrador) e uma New admin user password (Nova senha de usuário administrador).
3. Escolha Salvar.

## Verificar os dados de resumo do Amazon Redshift Serverless usando o painel

O painel do Amazon Redshift Serverless contém uma coleção de painéis que mostram rapidamente métricas e informações sobre o grupo de trabalho e o namespace. Esses painéis incluem o seguinte:

- Resources summary (Resumo dos recursos): exibe informações gerais sobre o Amazon Redshift Serverless, como o armazenamento usado e outras métricas.
- Query summary (Resumo de consultas): exibe informações sobre consultas, incluindo consultas concluídas e consultas em execução. Escolha View details (Visualizar detalhes) para ir para uma tela que tenha outros filtros.
- RPU capacity used (Capacidade de RPU utilizada): exibe a capacidade geral usada em determinado período; por exemplo, nas últimas dez horas.
- Datashares (Unidades de compartilhamento de dados): mostra a contagem de unidades de compartilhamento de dados, que são usadas para compartilhar dados entre contas da AWS, por exemplo. As métricas mostram quais unidades de compartilhamento de dados exigem autorização e outras informações.
- Uso total de computação: mostra o total de horas de RPU consumidas para o grupo de trabalho selecionado em um intervalo de tempo selecionado, até os últimos sete dias.

No painel, você pode analisar rapidamente essas métricas disponíveis para verificar detalhes sobre o Amazon Redshift Serverless, revisar consultas ou monitorar itens de trabalho.

# Monitorar consultas e workloads com o Amazon Redshift Serverless

## Monitorar consultas e workload com o Amazon Redshift Serverless

É possível monitorar consultas e workloads do Amazon Redshift Serverless com as visualizações fornecidas pelo sistema.

### Conceder acesso para monitoramento de consultas

Um superusuário pode fornecer acesso a usuários que não são superusuários para que possam monitorar as consultas para todos os usuários. Primeiro, você adiciona uma política para um usuário ou uma função para fornecer acesso para monitoramento de consulta. Em seguida, você concede permissão de monitoramento de consultas ao usuário ou à função.

Para adicionar a política de monitoramento de consultas

1. Escolha https://console.aws.amazon.com/iam/.
2. Em Access management (Gerenciamento de acesso), escolha Policies (Políticas).

3. Escolha Create Policy (Criar política).
4. Escolha JSON e cole a definição de política a seguir.

```
{
"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. Escolha Revisar política.
6. Em Name (Nome), insira um nome para a política, como `query-monitoring`.
7. Escolha Criar política.

Depois de criar a política, você pode conceder as permissões apropriadas.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.

- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Para conceder permissão de monitoramento de consultas a um usuário

Usuários com a permissão `sys:monitor` podem visualizar todas as consultas. Além disso, usuários com permissão `sys:operator` podem cancelar consultas, analisar o histórico de consultas e executar operações de vácuo.

1. Insira o seguinte comando para fornecer acesso de monitor do sistema, onde user-name é o nome do usuário ao qual você deseja fornecer acesso.

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

2. (Opcional) Insira o seguinte comando para fornecer acesso de operador do sistema, onde user-name é o nome do usuário a quem você deseja fornecer acesso.

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

Para conceder permissão de monitoramento de consultas a uma função

Os usuários com a uma função que tenha a permissão `sys:monitor` podem visualizar todas as consultas. Além disso, usuários com uma função que tenha a permissão `sys:operator` podem cancelar consultas, analisar o histórico de consultas e executar operações de vácuo.

1. Insira o seguinte comando para fornecer acesso de monitor do sistema, onde user-name é o nome da função à qual você deseja fornecer acesso.

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

2. (Opcional) Insira o seguinte comando para fornecer acesso de operador do sistema, onde user-name é o nome da função à qual você deseja fornecer acesso.

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

## Visualizações de monitoramento

As visualizações de monitoramento são exibições do sistema no Amazon Redshift Serverless usadas para monitorar o uso de consultas e workload. Essas visualizações estão localizadas no esquema `pg_catalog`. As visualizações do sistema disponíveis foram projetadas visando fornecer as informações necessárias para monitorar o Amazon Redshift Serverless, que é muito mais simples do que as necessárias para clusters provisionados. As visualizações do sistema SYS foram criadas para funcionar com o Amazon Redshift Serverless. Para exibir as informações fornecidas por essas exibições, execute instruções SQL SELECT.

As visualizações do sistema são definidas para serem compatíveis com os seguintes objetivos de monitoramento.

Monitorar workloads

É possível monitorar suas atividades de consulta ao longo do tempo para:

- Compreender os padrões de workload, para que você saiba qual é a normal (linha de base) e o que está dentro dos contratos de nível de serviço (SLAs) comerciais.
- Identificar rapidamente o desvio da normal, que pode ser um problema transitório ou algo que justifique novas ações.

Monitoramento de carga e descarga de dados

A entrada e saída de dados do Amazon Redshift Serverless é uma função essencial. Use COPY e UNLOAD para carregar ou descarregar dados. Além disso, é necessário monitorar o andamento minuciosamente em termos de bytes/linhas transferidos e arquivos concluídos para monitorar a adesão aos Acordos de Nível de Serviço empresariais. Isso normalmente é feito executando consultas de tabela do sistema com frequência (ou seja, a cada minuto) para rastrear o progresso e gerar alertas para investigação/ação corretiva, caso sejam detectados desvios consideráveis.

Diagnóstico de falhas e problemas

Há casos em que você deve tomar providências para falhas de consulta ou tempo de execução. Os desenvolvedores contam com tabelas do sistema para autodiagnosticar problemas e determinar as devidas correções.

Ajuste de performance

Talvez seja necessário ajustar consultas que não atendam aos requisitos do SLA desde o início ou que tenham se degradado ao longo do tempo. Para ajustar, você precisa ter detalhes de tempo de execução, inclusive plano de execução, estatísticas, duração e consumo de recursos. São necessários dados de linha de base para consultas ofensivas a fim de determinar a causa do desvio e orientar você a como melhorar a performance.

Monitorar eventos de objetos do usuário

É necessário monitorar ações e atividades em objetos do usuário, como atualizar visualizações materializadas, limpar e analisar. Isso inclui eventos gerenciados pelo sistema, como atualização automática para visualizações materializadas. Convém monitorar quando um evento termina se ele for iniciado pelo usuário ou a última execução bem-sucedida, se o sistema for iniciado.

Rastreamento de uso para cobrança

É possível monitorar suas tendências de uso ao longo do tempo para:

- Informar as estimativas de planejamento orçamentário e expansão dos negócios.
- Identificar possíveis oportunidades de economia de custos, como remover dados de baixa atividade.

Use as exibições do sistema SYS para monitorar o Amazon Redshift sem servidor. Para obter mais informações sobre as exibições de monitoramento SYS, consulte SYS monitoring views.

# Registro de auditoria para o Amazon Redshift Serverless

## Exportar logs

É possível configurar o Amazon Redshift Serverless para exportar dados de log de conexão, usuário e atividade do usuário para um grupo no Amazon CloudWatch Logs. Com o Amazon CloudWatch Logs, você pode executar análise em tempo real de dados de log e usar o CloudWatch para criar alarmes e visualizar métricas. É possível usar o CloudWatch Logs para armazenar seus registros de log em armazenamento persistente.

Você pode criar alarmes do CloudWatch para monitorar suas métricas usando o console do Amazon Redshift. Para obter mais informações sobre a criação de alarmes, consulte Gerenciar alarmes.

Para exportar os dados de log gerados para o Amazon CloudWatch Logs, os respectivos logs deverão ser selecionados para exportação nas configurações do Amazon Redshift Serverless,

no console. Você pode fazer isso escolhendo as definições da Configuração do namespace em Segurança e criptografia.

## Monitorar eventos de log no CloudWatch

Depois de selecionar quais logs do Redshift exportar, você pode monitorar eventos no Amazon CloudWatch Logs. Um novo grupo de logs é criado automaticamente para o Amazon Redshift sem servidor, em que `log_type` representa o tipo de log.

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

Quando você cria seu primeiro grupo de trabalho e namespace, default é o nome do namespace. O nome do grupo de logs varia de acordo com o que você chama de namespace.

Por exemplo, se você exportar o log de conexão, os dados de log serão armazenados no grupo de logs a seguir.

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

Os eventos de log são exportados para um grupo de logs usando o fluxo de log sem servidor. O comportamento depende de qual das seguintes condições é true:

- Um grupo de logs com o nome especificado já existe. O Redshift exporta dados de log usando o grupo de logs existente. Para criar grupos de log com períodos de retenção de log, filtros de métricas e acesso de clientes predefinidos, você pode usar a configuração automatizada como a fornecida pelo AWS CloudFormation.
- Um grupo de logs com o nome especificado não existe. Quando uma entrada de log correspondente é detectada no log da instância, o Amazon Redshift Serverless cria um novo grupo de logs no Amazon CloudWatch Logs automaticamente. O grupo de logs usa o período de retenção de logs padrão de Never Expire (Nunca expira). Para alterar o período de retenção de logs, use o console do Amazon CloudWatch Logs, a AWS CLI ou a API do CloudWatch Logs. Para obter mais informações sobre alteração de períodos de retenção de logs no CloudWatch Logs, consulte Alterar a retenção de logs de dados em Trabalhar com grupos de logs e fluxos de log.

Para pesquisar informações nos eventos de logs, use o console do Amazon CloudWatch Logs, a AWS CLI ou a API do Amazon CloudWatch Logs. Para obter mais informações sobre como procurar e filtrar dados de log, consulte Procurar e filtrar dados de log.

## Métricas do Amazon Redshift Serverless

As métricas do Amazon Redshift Serverless são divididas em métricas de computação e métricas de dados e armazenamento, abrangendo os conjuntos de dimensões de grupo de trabalho e namespace, respectivamente. Para obter mais informações sobre grupos de trabalho e namespaces, consulte Visão geral de grupos de trabalho e namespaces do Amazon Redshift Serverless.

As métricas de computação do CloudWatch são as seguintes:

Métricas de computação do CloudWatch

| Nome da métrica | Unidades | Descrição | Conjuntos de dimensões |
|---|---|---|---|
| `QueriesCompletedPerSecond` | Número de consultas | O número de consultas realizadas por segundo. | {Database, LatencyRange, Workgroup}, {LatencyRange, Workgroup} |
| `QueryDuration` | Microssegundos | O tempo médio para concluir uma consulta. | {Database, LatencyRange, Workgroup}, {LatencyRange, Workgroup} |
| `QueriesRunning` | Número de consultas | O número de consultas em execução em um determinado momento. | {Database, QueryType, Workgroup}, {QueryType, Workgroup} |
| `QueriesQueued` | Número de consultas | O número de consultas na fila em um determinado momento. | {Database, QueryType, Workgroup}, {QueryType, Workgroup} |

| Nome da métrica | Unidades | Descrição | Conjuntos de dimensões |
| --- | --- | --- | --- |
| DatabaseConnections | Número de conexões | O número de conexões com um banco de dados em um determinado momento. | {Database, Workgroup}, {Workgroup} |
| QueryRuntimeBreakdown | Milissegundos | O tempo total de execução de consultas, por estágio de consulta. | {Database, Stage, Workgroup}, {Stage, Workgroup} |
| ComputeCapacity | RPU | Número médio de unidades de computaçã o alocadas nos últimos 30 minutos, arredondadas para o inteiro mais próximo. | {Workgroup} |
| ComputeSeconds | Segundos de RPU | Segundos de unidade de computação acumulados usados nos últimos 30 minutos. | {Workgroup} |

| Nome da métrica | Unidades | Descrição | Conjuntos de dimensões |
| --- | --- | --- | --- |
| QueriesSucceeded | Número de consultas | O número de consultas que tiveram êxito nos últimos 5 minutos. | {Database, QueryType, Workgroup}, {QueryType, Workgroup} |
| QueriesFailed | Número de consultas | O número de consultas que falharam nos últimos 5 minutos. | {Database, QueryType, Workgroup}, {QueryType, Workgroup} |

| Nome da métrica | Unidades | Descrição | Conjuntos de dimensões |
| --- | --- | --- | --- |
| `UsageLimitAvailable` | RPU-horas ou TBs | Dependendo do UsageType, o UsageLimitAvailable retorna o seguinte:<br>• Se o UsageType for SERVERLESS_COMPUTE, o UsageLimitAvailable retornará o número restante de RPU-horas que o grupo de trabalho pode consultar no limite fornecido.<br>• Se o UsageType for CROSS_REGION_DATASHARING, o UsageLimitAvailable retornará o número | {UsageLimitId, UsageType, Workgroup} |

| Nome da métrica | Unidades | Descrição | Conjuntos de dimensões |
| --- | --- | --- | --- |
| | | restante de TBs que o cliente pode verificar no limite determinado. | |

| Nome da métrica | Unidades | Descrição | Conjuntos de dimensões |
| --- | --- | --- | --- |
| `UsageLimitConsumed` | RPU-horas ou TBs | Dependendo do UsageType, o UsageLimitConsumed retorna o seguinte:<br>• Se o UsageType for SERVERLESS_COMPUTE, o UsageLimitConsumed retornará o número de RPU-horas que o grupo de trabalho já consultou no limite fornecido.<br>• Se o UsageType for CROSS_REGION_DATASHARING, o UsageLimitConsumed retornará o número de TBs que o cliente já | {UsageLimitId, UsageType, Workgroup} |

| Nome da métrica | Unidades | Descrição | Conjuntos de dimensões |
| --- | --- | --- | --- |
| | | usou para verificar no limite determinado. | |

As métricas de dados e armazenamento do CloudWatch são as seguintes:

Métricas de dados e armazenamento do CloudWatch

| Nome da métrica | Unidades | Descrição | Conjuntos de dimensões |
| --- | --- | --- | --- |
| `TotalTableCount` | Número de tabelas | O número de tabelas de usuário existentes em um momento específico. Esse total não inclui tabelas do Amazon Redshift Spectrum. | {Database, Namespace} |
| `DataStorage` | Megabytes | O número de megabytes usados, em disco ou espaço de armazenamento, para dados do Redshift. | {Namespace} |

A métrica `SnapshotStorage` é independente do namespace e do grupo de trabalho. A métrica `SnapshotStorage` do CloudWatch é a seguinte:

Métrica SnapshotStorage do CloudWatch

| Nome da métrica | Unidades | Descrição | Conjuntos de dimensões |
|---|---|---|---|
| `SnapshotStorage` | Megabytes | O número de megabytes usados, em disco ou espaço de armazenamento, para snapshots. | {} |

Conjuntos de dimensões são as dimensões de agrupamento aplicadas às métricas. Você pode usar esses grupos de dimensões para especificar como suas estatísticas são recuperadas.

A tabela a seguir detalha dimensões e valores de dimensão para métricas específicas:

Dimensões e valores de dimensão do CloudWatch

| Dimensão | Descrição e valores |
|---|---|
| `DatabaseName` | O nome do banco de dados. Um valor personalizado. |
| `Latency` | Os valores possíveis são:<br>• Short (Curta): abaixo de 10 segundos<br>• Medium (Média): entre 10 segundos e 10 minutos<br>• Long (Longa): acima de 10 minutos |
| `QueryType` | Os valores possíveis são `INSERT`, `DELETE`, `UPDATE`, `UNLOAD`, `LOAD`, `SELECT`, `CTAS` e `OTHER`. |

| Dimensão | Descrição e valores |
| --- | --- |
| `stage` | Os estágios de execução de uma consulta. Os valores possíveis são:<br>• QueryPlanning: tempo gasto analisando e otimizando comandos de SQL.<br>• QueryWaiting: tempo gasto esperando na fila de WLM.<br>• QueryExecutingRead: Tempo gasto executando leitura de consultas.<br>• QueryExecutingInsert: Tempo gasto executando inserção de consultas.<br>• QueryExecutingDelete: Tempo gasto executando exclusão de consultas.<br>• QueryExecutingUpdate: Tempo gasto executando atualização de consultas.<br>• QueryExecutingCtas: Tempo gasto executando consultas de "criar tabela como".<br>• QueryExecutingUnload: Tempo gasto executando descarregamento de consultas.<br>• QueryExecutingCopy: Tempo gasto executando cópia de consultas.<br>• QueryCommit: Confirmar tempo gasto. |
| `Namespace` | O nome do namespace. Um valor personali zado. |
| `Workgroup` | O nome do grupo de trabalho. Um valor personalizado. |
| `UsageLimitId` | O identificador do limite de uso. |

| Dimensão | Descrição e valores |
| --- | --- |
| UsageType | O recurso do Amazon Redshift Serverless que está sendo limitado. Os valores possíveis são:<br>• SERVERLESS_COMPUTE<br>• CROSS_REGION_DATASHARING |

# Trabalhar com snapshots e pontos de recuperação

Um backup no Amazon Redshift sem servidor é uma representação pontual dos objetos e dos dados no namespace. Existem dois tipos de backups: snapshots criados manualmente e pontos de recuperação criados automaticamente pelo Amazon Redshift sem servidor para você. Os pontos de recuperação são criados a cada 30 minutos e mantidos por 24 horas.

Se achar que deseja recuperar os dados em um snapshot ou em um ponto de recuperação, você poderá restaurar um snapshot para um namespace de tecnologia sem servidor ou para um cluster provisionado. Há três cenários nos quais você pode restaurar snapshots:

- Restaure um snapshot sem servidor para um namespace sem servidor.
- Restaure um snapshot sem servidor para um cluster provisionado.
- Restaure um snapshot de cluster provisionado para um namespace sem servidor.

Ao restaurar um snapshot de tecnologia sem servidor para um cluster provisionado, você deve escolher o tipo de nó a ser usado, como RA3, e o número de nós, permitindo controlar configurações no nível do cluster ou do nó.

Para restaurar um snapshot de cluster provisionado para um namespace sem servidor, inicie pelo console provisionado do Redshift, escolha o snapshot a ser restaurado, depois selecione Restore from snapshot (Restaurar com base no snapshot) e Restore to serverless namespace (Restaurar para namespace sem servidor). O Amazon Redshift converte tabelas com chaves intercaladas em chaves de classificação compostas quando você restaura um snapshot de cluster provisionado para um namespace de tecnologia sem servidor. Para obter mais informações sobre chaves de classificação, consulte Trabalhar com chaves de classificação.

Se quiser incluir contexto adicional, você pode marcar snapshots e pontos de recuperação com pares de chave-valor que fornecem metadados e informações para snapshots e pontos de

recuperação. Para obter mais informações sobre como marcar recursos, consulte Visão geral da marcação de recursos.

Por fim, você também pode compartilhar snapshots com outras contas da AWS, o que as permite acessar dados dentro do snapshot e executar consultas.

## Snapshots

É possível restaurar um snapshot criado no console do Amazon Redshift Serverless para um namespace disponível associado a um grupo de trabalho. Um namespace estará disponível quando estiver pronto para consulta e/ou modificação. Você pode restaurar um snapshot criptografado com uma chave do KMS gerenciada pela AWS em um namespace sem servidor.

Para ver uma lista de todos os seus snapshots, no console Amazon Redshift Serverless, escolha Data backup (Backup de dados).

Para criar um snapshot

1. No console do Amazon Redshift Serverless, escolha Data backup (Backup de dados).
2. Escolha Criar snapshot.
3. Escolha um namespace para o qual deseja criar um snapshot.
4. Insira um identificador de snapshot.
5. (Opcional) Escolha um período de retenção. Se escolher Custom value (Valor personalizado), escolha o número de dias. O valor escolhido deve ser de 1 a 3653 dias. O padrão é reter indefinidamente.
6. Escolha Create (Criar).

Como criar um snapshot com base na configuração do namespace

1. No console do Amazon Redshift Serverless, escolha Namespace configuration (Configuração do namespace).
2. Escolha o namespace que servirá de base para a criação do snapshot. Você só pode criar snapshots de namespaces associados a um grupo de trabalho e cujo status é Available (Disponível).
3. Selecione a guia Data backup (Backup de dados).
4. Escolha Criar snapshot.

5. Insira um identificador de snapshot.
6. (Opcional) Escolha um período de retenção. Se escolher Custom value (Valor personalizado), escolha o número de dias. O valor escolhido deve ser de 1 a 3653 dias.
7. Escolha Create (Criar).

Como atualizar o período de retenção de um snapshot

1. No console do Amazon Redshift Serverless, escolha Data backup (Backup de dados).
2. Escolha um snapshot para atualizar.
3. Selecione Actions (Ações) e Set manual snapshot settings (Definir configurações de snapshot manual).
4. Escolha um período de retenção. Se escolher Custom value (Valor personalizado), escolha o número de dias.
5. Escolha Save changes (Salvar alterações).

Para excluir um snapshot

> **Note**
>
> Não é possível excluir um snapshot que foi compartilhado com outra conta. Antes de excluí-lo, você deve primeiro remover o acesso dessa conta ao snapshot.

1. No console do Amazon Redshift Serverless, escolha Data backup (Backup de dados).
2. Escolha um snapshot para excluir.
3. Escolha Ações, Excluir.
4. Escolha Delete (Excluir).

Como criar um snapshot final de todos os dados em um namespace antes de excluir o namespace.

1. No console do Amazon Redshift Serverless, escolha Namespace configuration (Configuração do namespace).
2. Escolha o namespace a ser excluído.
3. Escolha Ações, Excluir.

4. Selecione Create final snapshot (Criar snapshot final).
5. Insira um nome para o snapshot.
6. Insira “delete” (excluir).
7. Escolha Delete (Excluir).

Como compartilhar um snapshot com outro conta da AWS ou remover o acesso de uma conta a um snapshot

1. No console do Amazon Redshift Serverless, escolha Data backup (Backup de dados).
2. Escolha um snapshot para compartilhar.
3. Selecione Actions (Ações) e Manage access (Gerenciar acesso).
4. Para compartilhar um snapshot com outra conta, insira um ID de Conta da AWS. Para remover o acesso de uma conta, escolha Remover.
5. Escolha Save changes (Salvar alterações).

## Restauração de um snapshot

A restauração de um snapshot para um namespace de tecnologia sem servidor substitui o banco de dados atual pelo banco de dados no snapshot.

A restauração de um snapshot para um namespace sem servidor é concluída em duas fases. A primeira fase é concluída em alguns minutos, restaura os dados para o namespace e os disponibiliza para consultas. A segunda fase de restauração é onde o banco de dados é ajustado, o que pode causar pequenos problemas de performance. Essa segunda fase pode durar de algumas horas a vários dias e, em alguns casos, algumas semanas. O tempo depende do tamanho dos dados, mas a performance melhora progressivamente à medida que o banco de dados é ajustado. No final dessa fase, o namespace sem servidor está totalmente ajustado e é possível enviar consultas sem problemas de performance.

Como restaurar um snapshot para um namespace sem servidor

1. No console do Amazon Redshift Serverless, escolha Data backup (Backup de dados).
2. Escolha o snapshot a ser restaurado. Você só pode restaurar um snapshot por vez.
3. Selecione Actions (Ações) e Restore to serverless namespace (Restaurar para namespace sem servidor).

4. Escolha um namespace disponível para fazer a restauração. Você só pode restaurar para namespaces cujo status é Available (Disponível).
5. Escolha Restore.

Como restaurar um snapshot para um cluster provisionado

1. No console do Amazon Redshift Serverless, escolha Data backup (Backup de dados).
2. Escolha um snapshot para restaurar.
3. Selecione Action (Ação) e Restore to provisioned cluster (Restaurar para cluster provisionado).
4. Insira o identificador de um cluster.
5. Escolha um Node type (Tipo de nó). O número de nós depende do tipo de nó.
6. Siga as instruções na página do console para inserir as propriedades de Cluster configuration (Configuração do cluster). Para obter mais informações, consulte Creating a cluster (Criar um cluster).

Para obter mais informações sobre snapshots em clusters provisionados, consulte Amazon Redshift snapshots and backups.

## Pontos de recuperação

Os pontos de recuperação no Amazon Redshift sem servidor são criados aproximadamente a cada 30 minutos e salvos por 24 horas.

No console do Amazon Redshift Serverless, escolha Data backup (Backup de dados) para gerenciar pontos de recuperação. Você também pode executar as seguintes operações:

- Restaurar um ponto de recuperação para um namespace sem servidor.
- Converter um ponto de recuperação em snapshot.

Como restaurar um ponto de recuperação para um namespace sem servidor

1. No console do Amazon Redshift Serverless, escolha Data backup (Backup de dados).
2. Em Recovery points (Pontos de recuperação), escolha a Creation time (Hora de criação) do ponto de recuperação que você deseja restaurar.
3. Escolha Restore. Você só pode restaurar para namespaces cujo status é Available (Disponível).
4. Digite restore no campo de entrada de texto e escolha Restore (Restaurar).

Como converter um ponto de recuperação em snapshot

1. No console do Amazon Redshift Serverless, escolha Data backup (Backup de dados).
2. Em Recovery points (Pontos de recuperação), escolha a Creation time (Hora de criação) do ponto de recuperação que você deseja converter em um snapshot.
3. Escolha Create snapshot from recovery point (Criar snapshot usando o ponto de recuperação).
4. Insira um Snapshot identifier (identificador de snapshot).
5. Escolha Create (Criar).

## Programação de snapshots

Para controlar com precisão quando fazer um snapshot, é possível criar uma programação de snapshot para namepaces específicos. Ao programar a criação de snapshot, você pode criar um evento único ou usar expressões cron do Unix para criar uma programação recorrente. As expressões Cron dão suporte a três campos e são separadas por um espaço em branco.

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

| Campos | Valores | Curingas |
|---|---|---|
| Minutos | 0–59 | , - * / |
| Horas | 0–23 | , - * / |
| Dia do mês | 1–31 | , - * ? / L W |
| Mês | 1-12 ou JAN-DEZ | , - * / |
| Dia da semana | 1-7 ou SUN-SAT | , - * ? L # |
| Ano | 1970–2199 | , - * / |

Curingas

- A , (vírgula) curinga inclui valores adicionais. No campo `Day-of-week`, `MON,WED,FRI` incluirá segunda-feira, quarta-feira e sexta-feira. Os valores totais são limitados a 24 por campo.

- O - (traço) curinga especifica intervalos. No campo `Hour`, 1–15 incluiria as horas 1 a 15 do dia especificado.
- O * (asterisco) curinga inclui todos os valores no campo. No campo `Hours`, * incluirá cada hora.
- A / (barra) curinga especifica incrementos. No campo `Hours`, você pode inserir **`1/10`** para especificar a cada décima hora, a partir da primeira hora do dia (por exemplo, 01:00, 11:00 e 21:00).
- O curinga ? (interrogação) especifica um ou outro. No campo `Day-of-month`, você pode inserir 7 e, se não se importar com qual dia da semana era o sétimo, pode inserir ? no campo Dia da semana.
- O curinga L nos campos `Day-of-month` ou `Day-of-week` especifica o último dia do mês ou da semana.
- O curinga W no campo `Day-of-month` especifica um dia da semana. No campo `Day-of-month`, `3W` especifica o dia mais próximo do terceiro dia da semana do mês.
- O curinga # no campo Dia da semana especifica uma determinada instância do dia da semana definido dentro de um mês. Por exemplo, 3#2 seria a segunda terça-feira do mês: o 3 refere-se a terça-feira, porque é o terceiro dia de cada semana, e o 2 refere-se ao segundo dia desse tipo dentro do mês.

> **Note**
>
> Se você usar um caractere “#”, poderá definir apenas uma expressão no campo do dia da semana. Por exemplo, "3#1,6#3" não é válido porque é interpretado como duas expressões.

Limites

- Não é possível especificar os campos `Day-of-month` e `Day-of-week` na mesma expressão cron. Se você especificar um valor em um dos campos, deverá usar um ? (ponto de interrogação) no outro.
- Os cronogramas de snapshot não são compatíveis com as seguintes frequências:
  - Snapshots programados com frequência superior a 1 por hora.
  - Snapshots programados com frequência inferior a 1 por dia (24 horas).

  Se você tem programações sobrepostas que resultam na programação de snapshots em uma janela de 1 hora, o resultado é um erro de validação.

A tabela a seguir tem algumas strings cron de exemplo.

| Minutos | Horas | Dia da semana | Significado |
|---|---|---|---|
| 0 | 14-20/1 | TER | A cada hora entre 14h e 20h na terça-feira. |
| 0 | 21 | SEG-SEX | Todas as noites, às 21h, de segunda a sexta-feira. |
| 30 | 0/6 | SÁB-DOM | Incremento a cada 6 horas no sábado e domingo, a partir de 30 minutos após meia-noite (00:30) daquele dia. Isso resulta em um snapshot às [00:30, 06:30, 12:30 e 18:30] de cada dia. |
| 30 | 12/4 | * | Incremento a cada 4 horas, a partir de 12:30 de cada dia. O resultado é [12:30, 16:30, 20:30]. |

O exemplo a seguir demonstra como criar uma programação executada em incrementos de duas horas a partir das 15h15 de cada dia.

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

Atualmente, só é possível usar a API do Amazon Redshift sem servidor ou criar uma programação de snapshot. Para obter mais informações sobre essas operações, consulte Using the AWS CLI and Amazon Redshift Serverless API.

# Cópia de backups para outra Região da AWS

É possível configurar o Amazon Redshift sem servidor para copiar automaticamente snapshots e pontos de recuperação para outra Região da AWS. Quando você cria um snapshot na origem Região da AWS, ele é copiado para uma região de destino. É possível configurar o namespace para que ele só copie snapshots e pontos de recuperação para uma Região da AWS de destino por vez. Para obter uma lista de Regiões da AWS nas quais o Amazon Redshift sem servidor esteja disponível, consulte os endpoints listados para a API do Redshift sem servidor na Referência geral da Amazon Web Services.

Ao configurar a cópia de backups, você também pode especificar um período de retenção do tempo pelo qual o Amazon Redshift sem servidor deve manter o snapshot copiado. Não é possível alterar os períodos de retenção dos pontos de recuperação, que devem ser de um dia. Os períodos de retenção de snapshots na região de destino é separado do período de retenção do snapshot na região de origem. Por padrão, o período de retenção deve manter indefinidamente o snapshot. Se você escolher Valor personalizado, escolha o número de dias. O valor escolhido deve estar entre 1 e 3.653 dias.

Para alterar a região de destino para a qual copiar snapshots, desative primeiro a cópia de backups e, em seguida, especifique a nova região de destino ao reabilitar a cópia.

Depois que um snapshot ou um ponto de recuperação for copiado para uma região de destino, você poderá usá-lo a fim de restaurar dados para a região.

Por padrão, os dados são criptografados com uma chave gerenciada pela AWS por você. Para usar uma chave diferente, escolha a chave que você deseja usar ao configurar a cópia de backup na Região da AWS de origem, e o Amazon Redshift sem servidor cria automaticamente uma concessão, o que permite a criptografia de snapshots na Região da AWS de destino.

Para copiar backups para outra região, verifique se você tem as seguintes permissões do IAM:

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

Se estiver usando a própria chave KMS para criptografar os backups, você também precisará das seguintes permissões:

```
kms:CreateGrant
```

```
kms:DescribeKey
```

Para configurar a cópia dos snapshots ou dos pontos de recuperação para outra Região da AWS

1. No console do Amazon Redshift sem servidor, escolha o namespace para o qual você deseja configurar a cópia de snapshots ou pontos de recuperação.
2. Escolha as Ações, Configurar o backup entre regiões.
3. Escolha o destino Região da AWS para o qual o snapshot deve ser copiado.
4. (Opcional) Escolha por quanto tempo o snapshot deve ser retido. Se você escolher Valor personalizado, escolha o número de dias. O valor escolhido deve estar entre 1 a 3.653 dias , inclusive. O padrão é reter indefinidamente.
5. (Opcional) Escolha uma chave AWS KMS diferente a ser usada na criptografia na região de destino.
6. Escolha Save configuration.

## Restaurar uma tabela

Também é possível restaurar uma tabela específica de um snapshot ou ponto de recuperação. Ao fazer isso, você especifica o snapshot de origem ou o ponto de recuperação, o banco de dados, o esquema, a tabela, o banco de dados de destino, o esquema e o nome da nova tabela. Essa nova tabela não pode ter o mesmo nome de uma tabela existente. Se quiser substituir uma tabela existente restaurando uma tabela, você deverá primeiro renomear ou descartar a tabela antes de restaurá-la.

A tabela de destino é criada usando-se as definições de coluna da tabela de origem, os atributos da tabela e os atributos da coluna, exceto as chaves externas. Para evitar conflitos por causa de dependências, a tabela de destino não herda chaves externas da tabela de origem. Todas as dependências, como visualizações ou permissões concedidas na tabela de origem, não são aplicadas à tabela de destino.

Se o proprietário da tabela de origem existir, esse usuário será o proprietário da tabela restaurada, desde que o usuário tenha permissões suficientes para se tornar o proprietário de uma relação no banco de dados e no esquema especificados. Do contrário, a tabela restaurada será de propriedade do usuário administrador que foi criado quando o cluster foi iniciado.

A tabela restaurada retorna ao estado em que estava no momento em que o backup foi feito. Isso inclui regras de visibilidade de transação definidas pela adesão do Amazon Redshift ao

isolamento serializável, o que significa que os dados serão imediatamente visíveis para transações em andamento iniciadas após o backup.

Você pode usar o console do Amazon Redshift Serverless para restaurar as tabelas de um snapshot.

A restauração de uma tabela do backup de dados tem as seguintes limitações:

- Você só pode restaurar uma tabela por vez.
- Todas as dependências, como visualizações ou permissões concedidas na tabela de origem, não são aplicadas à tabela de destino.
- Se a segurança por linha estiver ativada para uma tabela que está sendo restaurada, o Amazon Redshift Serverless restaurará a tabela com a segurança por linha ativada.

Para restaurar uma tabela usando o console do Amazon Redshift sem servidor

1. No console do Amazon Redshift Serverless, escolha Data backup (Backup de dados).
2. Escolha o instantâneo ou o ponto de recuperação que tem a tabela a ser restaurada.
3. Escolha Ações, Restaurar tabela do snapshot ou Restaurar tabela do ponto de recuperação.
4. Insira informações sobre o snapshot de origem ou o ponto de recuperação e a tabela de destino e, em seguida, escolha Restaurar tabela.

## Uso da AWS Command Line Interface e da API do Amazon Redshift sem servidor

Além de usar o Console da AWS, também é possível usar a AWS CLI ou a API do Amazon Redshift Serverless para interagir com snapshots e pontos de recuperação. A tabela abaixo lista as operações de API e CLI que é possível usar para gerenciar snapshots e pontos de recuperação.

| Operação de API | Comando da CLI | Descrição |
| --- | --- | --- |
| CreateSnapshot | create-snapshot | Cria um snapshot. Os snapshots devem estar associados a um namespace , portanto, você deve incluir o nome de um namespace na solicitação. Por padrão, |

| Operação de API | Comando da CLI | Descrição |
| --- | --- | --- |
| | | o Amazon Redshift sem servidor mantém snapshots por um período indefinido, mas é possível especificar um período de retenção. |
| RestoreFromSnapshot | restore-from-snapshot | Restaura os bancos de dados em um snapshot para o namespace. Se você estiver restaurando um snapshot do Amazon Redshift Serverless para um cluster provisionado, será necessário especificar o `snapshotArn` do snapshot que você está restaurando. Do contrário, se você estiver restaurando de tecnologia sem servidor para tecnologia sem servidor, poderá especificar `snapshotArn` ou `snapshotName`, mas não ambos. |
| RestoreTableFromSnapshot | restore-table-from-snapshot | Restaura uma tabela de um snapshot para o namespace do Amazon Redshift sem servidor. Não é possível usar essa operação para restaurar tabelas com chaves de classificação intercaladas. |
| GetSnapshot | get-snapshot | Recupera informações sobre um snapshot. |
| ListSnapshots | list-snapshots | Recupera informações sobre vários snapshots. |

| Operação de API | Comando da CLI | Descrição |
| --- | --- | --- |
| DeleteSnapshot | delete-snapshot | Exclui um snapshot. |
| RestoreFromRecoveryPoint | restore-from-recovery-point | Restaura os dados dentro de um ponto de recuperação para o namespace. |
| RestoreTableFromRecoveryPoint | restore-table-from-recovery-point | Restaura uma tabela de um ponto de recuperação para o namespace do Amazon Redshift sem servidor. Não é possível usar essa operação para restaurar tabelas com chaves de classificação intercaladas. |
| ConvertRecoveryPointToSnapshot | convert-recovery-point-to-snapshot | Converte um ponto de recuperação em um snapshot. |
| GetRecoveryPoint | get-recovery-point | Recupera informações sobre um ponto de recuperação. |
| ListRecoveryPoints | list-recovery-points | Recupera informações sobre vários pontos de recuperação. |

Para programar a criação de snapshot, use as operações de API a seguir.

| Operação de API | Comando da CLI | Descrição |
| --- | --- | --- |
| CreateScheduledAction | create-scheduled-action | Cria uma ação programada, que contém uma programação e uma ação do Amazon Redshift sem servidor. Por exemplo, é possível criar uma programação de quando |

| Operação de API | Comando da CLI | Descrição |
| --- | --- | --- |
| | | executar a operação da API `CreateSnapshot` . |
| DeleteScheduledAction | delete-scheduled-action | Exclui uma ação programada. |
| GetScheduledAction | get-scheduled-action | Recupera informações sobre uma ação programada. |
| ListScheduledActions | list-scheduled-actions | Recupera informações sobre uma lista de ações programadas. |
| UpdateScheduledAction | update-scheduled-action | Atualiza uma ação programada. |

# Compartilhar dados no Amazon Redshift Serverless

Use o compartilhamento de dados para compartilhar as informações mais atualizadas e consistentes à medida que são atualizadas no Amazon Redshift Serverless.

## Compartilhar dados no Amazon Redshift Serverless

Com o compartilhamento de dados, você tem acesso ao vivo aos dados para que os usuários possam ver as informações mais atualizadas e consistentes conforme elas são atualizadas no Amazon Redshift Serverless.

### Conceitos básicos do compartilhamento de dados do Amazon Redshift Serverless

É possível compartilhar dados para fins de leitura em diferentes instâncias do Amazon Redshift Serverless dentro ou entre Contas da AWS.

Você pode começar a compartilhar dados usando a interface SQL ou o console do Amazon Redshift. Para obter mais informações, consulte Conceitos básicos de compartilhamento de dados usando a interface SQL ou Conceitos básicos do compartilhamento de dados usando o console no Guia do desenvolvedor de banco de dados do Amazon Redshift no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Com o compartilhamento de dados, os namespaces e os clusters provisionados do Amazon Redshift Serverless podem compartilhar dados ao vivo entre si, estejam eles na mesma Conta da AWS, em Contas da AWS diferentes ou em Regiões da AWS diferentes. Para obter informações, consulte Regiões em que o compartilhamento de dados está disponível.

Para começar a compartilhar dados em uma Conta da AWS, abra o AWS Management Console e escolha o console do Amazon Redshift. Selecione Namespace configuration (Configuração do namespace) e Datashares (Unidades de compartilhamento de dados). Siga os procedimentos em Conceitos básicos do compartilhamento de dados usando o console no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Para começar a compartilhar dados entre Contas da AWS, abra o AWS Management Console e escolha o console do Amazon Redshift. Selecione Datashares. Siga os procedimentos em Conceitos básicos do compartilhamento de dados usando o console no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Para começar a consultar dados em uma unidade de compartilhamento de dados, crie um banco de dados em um namespace que tenha um grupo de trabalho associado a ele. Com base em uma unidade de compartilhamento de dados, escolha um namespace que tenha um grupo de trabalho associado a ele e crie um banco de dados para consultar dados. Siga os procedimentos em Criar bancos de dados com base em unidades de compartilhamento de dados.

## Conceder acesso para visualizar unidades de compartilhamento de dados usando o console

Um superusuário pode fornecer acesso a usuários que não são superusuários para que possam visualizar as unidade de compartilhamento de dados criadas por todos os usuários.

Para fornecer acesso a uma unidade de compartilhamento de dados para um usuário, use o comando a seguir, onde datashare_name é o nome da unidade de compartilhamento de dados e user-name é o nome do usuário para o qual deseja fornecer acesso.

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

Para conceder acesso a uma unidade de compartilhamento de dados para um grupo de usuários, primeiro crie um grupo de usuários com usuários. Para obter informações sobre como criar grupos de usuários, consulte CREATE GROUP. Depois, conceda acesso à unidade de compartilhamento de dados para um usuário usando o comando a seguir, em que datashare_name é o nome da unidade

de compartilhamento de dados e user-group é o nome do grupo de usuários ao qual você deseja conceder acesso.

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

Para obter informações sobre como usar a instrução GRANT, consulte GRANT.

### Considerações sobre o compartilhamento de dados no Amazon Redshift Serverless

Veja as seguintes considerações para trabalhar com o compartilhamento de dados do Amazon Redshift Serverless:

- O Amazon Redshift só oferece suporte a clusters provisionados dos tipos de instância ra3.16xlarge, ra3.4xlarge e ra3.xlplus, e endpoint de tecnologia sem servidor como produtores ou consumidores de compartilhamento de dados.
- Por padrão, o Amazon Redshift Serverless é criptografado.

Para obter uma lista de limitações das unidades de compartilhamento de dados, incluindo objetos de banco de dados compatíveis, requisitos de criptografia e requisitos de chaves de classificação, consulte Considerações ao usar o compartilhamento de dados no Amazon Redshift no Guia do desenvolvedor de banco de dados do Amazon Redshift.

## Visão geral dos recursos de marcação

Na AWS, as etiquetas são rótulos definidos pelo usuário que consistem em pares de chave-valor. O Amazon Redshift Serverless é compatível com a marcação para fornecer metadados sobre recursos rapidamente.

As etiquetas não são necessárias para recursos, mas elas ajudam a fornecer o contexto. Talvez você queira marcar recursos com metadados com informações relacionadas ao recurso. Por exemplo, suponha que você queira rastrear quais recursos pertencem a um ambiente de teste e a um ambiente de produção. Você poderia criar uma chave chamada “environment” e fornecer o valor “test” ou “production” para identificar os recursos usados em cada ambiente. Se você usa marcação em outros serviços da AWS ou tem categorias padrão para seus negócios, recomendamos que você crie os mesmos pares de chave-valor para recursos a fim de manter a consistência.

Se você excluir um recurso, todas as tags associadas serão excluídas. É possível usar tanto a AWS CLI como o console do e o Amazon Redshift Serverless para marcar recursos sem servidor. As operações de API disponíveis são `TagResource`, `UntagResource` e `ListTagsForResource`.

Cada recurso tem um conjunto de tags, que é uma coleção de uma ou mais tags atribuídas ao recurso. Cada recurso pode ter até 50 tags por conjunto de tags. Você pode adicionar tags ao criar um recurso e após a criação de um recurso. Você pode adicionar etiquetas aos seguintes tipos de recurso sem servidor:

- Grupos de trabalho
- Namespaces
- Snapshots do
- Pontos de recuperação

As tags têm os seguintes requisitos:

- As chaves não podem ser prefixadas com `aws:`.
- As chaves devem ser exclusivas por conjunto de tags.
- Uma chave deve ter entre 1 e 128 caracteres permitidos.
- Um valor deve ter entre 0 e 256 caracteres permitidos.
- Os valores não precisam ser exclusivos por conjunto de tags.
- Os caracteres permitidos para chaves e valores são letras Unicode, dígitos, espaço em branco e qualquer um dos seguintes símbolos: _ . : / = + - @.
- As chaves e os valores diferenciam letras maiúsculas de minúsculas.

Como gerenciar tags de seus recursos do Amazon Redshift Serverless

1. No console do Amazon Redshift Serverless, selecione Manage Tags (Gerenciar tags).
2. Insira o tipo de recurso a ser pesquisado e selecione Search resources (Pesquisar recursos). Escolha o recurso para o qual você deseja gerenciar etiquetas e selecione Gerenciar etiquetas.
3. Especifique as chaves e os valores opcionais que deseja adicionar ao recurso. Ao modificar uma tag, você pode alterar o valor dela, mas não a chave.
4. Depois de terminar de adicionar, remover ou modificar tags, selecione Save changes (Salvar alterações) e Apply (Aplicar) para salvar as alterações.

# Clusters provisionados do Amazon Redshift

Nas seções a seguir, você pode aprender os fundamentos da criação de um data warehouse, iniciando um conjunto de nós de computação, chamado de cluster do Amazon Redshift.

Tópicos


- Visão geral do do Amazon Redshift
- Uso do EC2-VPC ao criar o cluster
- Alarme padrão de espaço em disco
- Status do cluster
- Considerações sobre o uso de clusters provisionados do Amazon Redshift
- Operações de cluster
- Configuração da implantação multi-AZ
- Gerenciamento de clusters usando o console
- Gerenciar clusters usando a AWS CLI e a API do Amazon Redshift
- Gerenciamento de clusters em uma VPC
- Histórico das versões de cluster


## Visão geral do do Amazon Redshift

Um data warehouse do Amazon Redshift é um conjunto de recursos de computação chamados nós, que são organizados em um grupo chamado cluster. Cada cluster executa um mecanismo do Amazon Redshift e contém um ou mais bancos de dados.

> **Note**
>
> No momento, o mecanismo Amazon Redshift versão 1.0 está disponível. No entanto, conforme o mecanismo é atualizado, várias versões do mecanismo Amazon Redshift podem estar disponíveis para seleção.

# Clusters e nós no Amazon Redshift

Um cluster do Amazon Redshift consiste em nós. Cada cluster tem um nó de liderança e um ou mais nós de computação. O nó líder recebe consultas de aplicativos cliente, analisa as consultas e desenvolve planos de execução de consulta. Em seguida, o nó principal coordena a execução paralela desses planos com os nós de computação e agrega os resultados intermediários desses nós. Então, ele retorna os resultados de volta para os aplicativos cliente.

Os nós de computação executam planos de execução de consultas e transmitem dados entre si para atender a essas consultas. Os resultados intermediários são enviados ao nó de liderança para agregação antes de serem enviados novamente para os aplicativos clientes. Para obter mais informações sobre nós líderes e nós de computação, consulte Arquitetura do sistema de data warehouse no Guia do desenvolvedor de banco de dados do Amazon Redshift.

> **Note**
>
> Quando você cria um cluster no console do Amazon Redshift (https://console.aws.amazon.com/redshiftv2/), você pode obter uma recomendação de configuração de cluster com base no tamanho dos dados e das características de consulta. Para usar esta calculadora de dimensionamento, procure Ajude-me a escolher no console nas regiões da AWS que oferecem suporte a tipos de nó RA3. Para obter mais informações, consulte Criar um cluster.

Quando você inicia um cluster, uma opção que você especifica é o tipo de nó. O tipo de nó determina a CPU, RAM, capacidade de armazenamento e o tipo de unidade de armazenamento de cada nó.

O Amazon Redshift oferece diferentes tipos de nós para acomodar seus workloads e recomendamos a escolha de RA3 ou DC2 dependendo da performance necessária, tamanho dos dados e crescimento de dados esperado.

Os nós RA3 com armazenamento gerenciado permitem que otimizar o data warehouse com escalabilidade e pagando separadamente por computação e armazenamento gerenciado. Com o RA3, você escolhe o número de nós com base nos requisitos de performance e paga apenas pelo armazenamento gerenciado utilizado. Dimensione o cluster RA3 com base na quantidade de dados processada diariamente. Você pode executar clusters que usam os tipos de nó RA3 em uma virtual private cloud (VPC). Não é possível iniciar clusters RA3 no EC2-Classic. Para obter mais informações, consulte Criar um cluster em uma VPC.

O armazenamento gerenciado do Amazon Redshift usa SSDs grandes de alta performance em cada nó RA3 para armazenamento local rápido e Amazon S3 para armazenamento durável de longo prazo. Se os dados em um nó crescerem além do tamanho dos grandes SSDs locais, o armazenamento gerenciado do Amazon Redshift descarrega automaticamente esses dados para o Amazon S3. Você paga a mesma taxa baixa pelo armazenamento gerenciado do Amazon Redshift, independentemente de os dados estarem em SSDs de alta performance ou no Amazon S3. Para workloads que exigem armazenamento crescente, o armazenamento gerenciado permite escalar automaticamente a capacidade de armazenamento do data warehouse separada dos nós de computação.

Os nós DC2 permitem criar data warehouses com uso intensivo de computação e armazenamento SSD local. Você escolhe o número de nós necessários com base no tamanho dos dados e nos requisitos de performance. Os nós DC2 armazenam os dados localmente para alta performance e, conforme o tamanho dos dados cresce, é possível adicionar mais nós de computação para aumentar a capacidade de armazenamento do cluster. Para conjuntos de dados abaixo de 1 TB (compactados), recomendamos os tipos de nós DC2 para obter a melhor performance com o menor preço. Se você espera que os dados cresçam, recomendados o uso dos nós RA3, para que você possa dimensionar computação e armazenamento de forma independente para atingir preço e performance melhores. Você executa clusters que usam os tipos de nó DC2 em uma nuvem privada virtual (VPC). Não é possível iniciar clusters DC2 no EC2-Classic. Para obter mais informações, consulte Criar um cluster em uma VPC.

Os nós DS2 permitem criar grandes data warehouses usando discos rígidos (HDDs) e recomendamos o uso dos nós RA3 em seu lugar. Se você estiver usando nós DS2, consulte Atualizar para os tipos de nó RA3 para obter diretrizes de atualização. Se estiver usando oito ou mais nós de ds2.xlarge ou qualquer número de nós ds2.8xlarge, agora você poderá atualizar para o RA3 para obter 2x mais armazenamento e melhor performance pelo mesmo preço sob demanda.

Os tipos de nó estão disponíveis em diferentes tamanhos. O tamanho do nó e o número de nós determinam o armazenamento total de um cluster. Para obter mais informações, consulte Detalhes do tipo de nó.

Alguns tipos de nó permitem um nó (single-node) ou dois ou mais nós (multi-node). O número mínimo de nós para clusters de alguns tipos de nó é de dois nós. Em um cluster de single-node, o nó é compartilhado para a funcionalidade principal e de computação. Os clusters de nó único não são recomendados para executar workloads de produção. Em um cluster de multi-node, o nó de liderança é separado dos nós de computação. O nó de liderança é o mesmo tipo de nó que os nós de computação. Você só paga pelos nós de computação.

O Amazon Redshift aplica cotas a recursos para cada conta da AWS em cada região da AWS. Uma cota restringe o número de recursos que sua conta pode criar para um determinado tipo de recurso, como nós ou snapshots, dentro de uma região da AWS. Para obter mais informações sobre as cotas padrão que se aplicam aos recursos do Amazon Redshift, consulte Limites do Amazon Redshift na Referência geral da Amazon Web Services. Para solicitar um aumento, envie um Formulário de aumento de limite do Amazon Redshift.

O custo do cluster depende da região da AWS, do tipo de nó, do número de nós e se os nós são reservados com antecedência. Para obter mais informações sobre o custo de nós, consulte a página de Preços do Amazon Redshift.

## Detalhes do tipo de nó

As tabelas a seguir resumem as especificações de nó para cada tipo e tamanho de nó. Os títulos nas tabelas têm estes significados:

- vCPU é o número de CPUs virtuais para cada nó.
- RAM é a quantidade de memória em gibibytes (GiB) para cada nó.
- Fatias por nó padrão é o número de fatias nas quais um nó de computação é particionado quando um cluster é criado ou redimensionado por meio do redimensionamento clássico.

  O número de fatias por nó poderá ser alterado se o cluster for redimensionado usando o redimensionamento elástico. No entanto, o número total de fatias em todos os nós de computação no cluster permanece o mesmo após o redimensionamento elástico.

  Ao criar um cluster com a operação de restauração do snapshot, o número de fatias do cluster resultante pode ser alterado do cluster original se você alterar o tipo de nó.
- Storage é capacidade e o tipo de armazenamento de cada nó.
- O Intervalo de nós é o número mínimo e máximo de nós que o Amazon Redshift suporta para o tipo e tamanho de nó.

> **Note**
>
> Você pode ficar restrito a menos nós, dependendo da cota aplicada à sua conta da AWS na região da AWS selecionada. Para solicitar um aumento, envie um Formulário de aumento de limite do Amazon Redshift.

- Capacidade total é a capacidade de armazenamento total para o cluster se você implantar o número máximo de nós especificado no intervalo de nó.

Tipos de nó RA3

| Tipo de nó | vCPU | RAM (GiB) | Fatias padrão por nó | Limite do armazenamento gerenciado por nó [1] | Intervalo de nós com a criação de cluster | Capacidade total de armazenamento gerenciado [2] |
|---|---|---|---|---|---|---|
| ra3.xlplus (nó único) | 4 | 32 | 2 | 4 TB | 1 | 4 TB[3] |
| ra3.xlplus (vários nós) | 4 | 32 | 2 | 32 TB | 2–16[4] | 1.024 TB[4] |
| ra3.4xlarge | 12 | 96 | 4 | 128 TB | 2–32[5] | 8.192 TB[5] |
| ra3.16xlarge | 48 | 384 | 16 | 128 TB | 2–128 | 16.384 TB |

[1] O limite do armazenamento gerenciado do Amazon Redshift. Esse é um limite fixo.

[2] O limite total de armazenamento gerenciado é o número máximo de nós vezes o limite de armazenamento gerenciado por nó.

[3]Para redimensionar um cluster de nó único para vários nós, somente o redimensionamento clássico é aceito.

[4] Você pode criar um cluster com o tipo de nó ra3.xlplus (vários nós) que tenha até 16 nós. Para clusters de vários nós, é possível redimensionar com redimensionamento elástico até o máximo de 32 nós.

[5] Você pode criar um cluster com o tipo de nó ra3.4xlarge com até 32 nós. Você pode redimensioná-lo com o redimensionamento elástico para um máximo de 64 nós.

Tipos de nós de armazenamento denso

| Tipo de nó | vCPU | RAM (GiB) | Fatias padrão por nó | Armazenamento por nó | Intervalo de nó | Capacidade total |
|---|---|---|---|---|---|---|
| ds2.xlarge | 4 | 31 | 2 | 2 TB HDD | 1–32 | 64 TB |
| ds2.8xlarge | 36 | 244 | 16 | 16 TB HDD | 2–128 | 2 PB |

Tipos de nós de computação densa

| Tipo de nó | vCPU | RAM (GiB) | Fatias padrão por nó | Armazenamento por nó | Intervalo de nó | Capacidade total |
|---|---|---|---|---|---|---|
| dc2.large | 2 | 15 | 2 | NVMe-SSD de 160 GB | 1–32 | 5.12 TB |
| dc2.8xlarge | 32 | 244 | 16 | NVMe-SSD de 2.56 TB | 2–128 | 326 TB |
| dc1.large[1] | 2 | 15 | 2 | 160 GB SSD | 1–32 | 5.12 TB |
| dc1.8xlarge[1] | 32 | 244 | 32 | 2.56 TB SSD | 2–128 | 326 TB |

[1] Recomendamos os tipos de nó DC2 em vez dos tipos de nó DC1. Para obter mais informações sobre como atualizar, consulte Atualizar de tipos de nó DC1 para tipos de nó DC2.

Nomes dos tipos anteriores de nó

Em versões anteriores do Amazon Redshift, certos tipos de nós tinham nomes diferentes. Você pode usar os nomes anteriores na API do Amazon Redshift e na AWS CLI. Contudo, recomendamos que você atualize todos os scripts que façam referência a esses nomes para usarem os nomes atuais. Os nomes atuais e anteriores são conforme se segue.

| Nome atual | Nomes anteriores |
| --- | --- |
| 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 |

## Determinação do número de nós

Como o Amazon Redshift distribui e executa consultas em paralelo em todos os nós de computação de um cluster, você pode aumentar a performance das consultas adicionando nós ao cluster. Quando você executa um cluster de, pelo menos, dois nós de computação, os dados em cada nó são espelhados em discos de outro nó para reduzir o risco de perda de dados.

É possível monitorar a performance da consulta no console do Amazon Redshift e com métricas do Amazon CloudWatch. Também é possível adicionar ou remover nós conforme necessário para alcançar o equilíbrio entre preço e performance para o cluster. Quando você solicita um nó adicional, o Amazon Redshift cuida de todos os detalhes de implantação, balanceamento de carga e manutenção de dados. Para obter mais informações sobre performance do cluster, consulte Monitorar a performance do cluster do Amazon Redshift.

Os nós reservados são adequados para workloads de produção estáveis e oferecem grandes descontos em relação aos nós sob demanda. É possível comprar nós reservados depois de executar experimentos e prova de conceitos para validar a configuração de produção. Para obter mais informações, consulte Comprar nós reservados do Amazon Redshift.

Ao pausar um cluster, você suspende o faturamento sob demanda durante o tempo em que o cluster fica pausado. Durante esse tempo pausado, você só paga pelo armazenamento de backup. Desse modo, você fica livre de planejar e comprar antecipadamente capacidade de data warehouse para atender às suas necessidades e pode gerenciar com economia ambientes para desenvolvimento ou testes.

Para obter informações sobre preço de nós sob demanda e reservados, consulte Preços do Amazon Redshift.

# Uso do EC2-VPC ao criar o cluster

Clusters do Amazon Redshift são executados em instâncias do Amazon EC2 configuradas para o tipo de nó do Amazon Redshift e o tamanho de nó que você seleciona. Crie o cluster usando o EC2-VPC. Se você ainda estiver usando o EC2-Classic, recomendamos usar o EC2-VPC para obter melhor performance e segurança. Para obter mais informações sobre essas plataformas de rede, consulte Plataformas compatíveis no Manual do usuário do Amazon EC2 para instâncias do Linux. As configurações de sua conta da AWS determinam se EC2-VPC ou EC2-Classic estão disponíveis para você.

> **Note**
>
> Para evitar problemas de conexão entre as ferramentas do cliente SQL e o banco de dados do Amazon Redshift, recomendamos fazer uma das duas coisas. Você pode configurar uma regra de entrada que permita aos hosts negociar o tamanho do pacote. Como alternativa, você pode desabilitar os jumbo frames TCP/IP definindo a unidade máxima de transmissão (MTU) para 1500 na interface de rede (NIC) de suas instâncias do Amazon EC2. Para obter mais informações sobre essas abordagens, consulte As consultas parecem travar e, às vezes, não se comunicam com o cluster.

## EC2-VPC

Ao usar EC2-VPC, seu cluster é executado em uma Virtual Private Cloud (VPC) que é logicamente isolada em sua conta da AWS. Se provisionar o cluster no EC2-VPC, você controlará seu acesso associando um ou mais grupos de segurança de VPC ao cluster. Para obter mais informações, consulte Grupos de segurança para sua VPC no Guia do usuário da Amazon VPC.

Para criar um cluster em um VPC, você deve primeiro criar um grupo de sub-rede de cluster do Amazon Redshift, fornecendo informações de sub-rede de seu VPC e, em seguida, fornecer o grupo de sub-rede ao iniciar o cluster. Para obter mais informações, consulte Grupos de sub-rede de cluster do Amazon Redshift.

Para obter mais informações sobre a Amazon Virtual Private Cloud (Amazon VPC), consulte o Página de detalhes do produto Amazon VPC.

# EC2-Classic

A plataforma EC2-Classic será retirada em 15 de agosto de 2022. Recomendamos que você migre os clusters da plataforma EC2-Classic para uma plataforma EC2-VPC. Para obter mais informações, consulte Atualizar um cluster de DS2 no EC2-Classic para EC2-VPC e EC2-Classic Networking is Retiring: Here's How to Prepare (O EC2-Classic está sendo descontinuada: veja como se preparar).

No EC2-Classic, seu cluster é executado em uma única rede plana que você compartilha com outros clientes da AWS. Se você provisionar seu cluster no EC2-Classic, você controla o acesso ao seu cluster associando um ou mais grupos de segurança de cluster do Amazon Redshift ao cluster. Para obter mais informações, consulte Grupos de segurança de clusters do Amazon Redshift.

## Executar um cluster

Sua conta da AWS pode iniciar instâncias de EC2-VPC e EC2-Classic ou apenas EC2-VPC, região por região. Para determinar qual plataforma de redes é compatível com sua conta e depois executar um cluster, faça o seguinte:

1. Decida em qual região da AWS você deseja implantar um cluster. Para conferir uma lista de regiões da AWS nas quais o Amazon Redshift está disponível, consulte Endpoints do Amazon Redshift na Referência geral da Amazon Web Services.
2. Descubra quais plataformas Amazon EC2 sua conta suporta na região da AWS escolhida. Você pode encontrar essas informações no console do Amazon EC2. Para obter instruções detalhadas, consulte Plataformas compatíveis no Manual do usuário do Amazon EC2 para instâncias do Linux.
3. Se a sua conta for compatível com ambas as plataformas, recomendamos a EC2-VPC. Se sua conta for compatível somente com EC2-VPC, você deve implantar seu cluster em VPC.
4. Inicie seu cluster do Amazon Redshift. Você pode criar um cluster usando o console do Amazon Redshift ou usando a API do Amazon Redshift, a AWS CLI ou bibliotecas SDK. Para obter mais informações sobre essas opções e links para a documentação relacionada, consulte O que é o Amazon Redshift?.

# Alarme padrão de espaço em disco

Ao criar um cluster do Amazon Redshift, você pode configurar opcionalmente um alarme do Amazon CloudWatch para monitorar a porcentagem média de espaço em disco que é usado em todos os nós em seu cluster. Nos referiremos a este alarme como o alarme padrão de espaço em disco.

A finalidade do alarme padrão de espaço em disco é ajudá-lo a monitorar a capacidade de armazenamento de seu cluster. Você pode configurar este alarme com base nas necessidades de seu data warehouse. Por exemplo, você pode usar o aviso como um indicador de que talvez seja necessário redimensionar seu cluster. É possível redimensionar selecionando um tipo de nó diferente ou adicionando nós, ou talvez comprando nós reservados para uma expansão futura.

O alarme padrão de espaço em disco é acionado quando o uso de disco atinge ou excede uma porcentagem especificada por determinado número de vezes e por uma duração específica. Por padrão, este alarme é acionado quando a porcentagem que você especifica é alcançada e permanece acima ou naquela porcentagem por cinco minutos ou mais. Você pode editar os valores padrão depois que executar o cluster.

Quando o alarme do CloudWatch é acionado, o Amazon Simple Notification Service (Amazon SNS) envia uma notificação para os destinatários especificados para alertá-los de que o limite de porcentagem foi alcançado. O Amazon SNS usa um tópico para especificar os destinatários e a mensagem que são enviados em uma notificação. Você pode usar um tópico existente do Amazon SNS; caso contrário, um tópico é criado com base nas configurações que você especifica ao iniciar o cluster. Você pode editar o tópico para este alarme depois que executar o cluster. Para obter mais informações sobre a criação de tópicos do Amazon SNS, consulte Conceitos básicos do Amazon Simple Notification Service.

Depois que você executar o cluster, é possível visualizar e editar o alarme a partir da janela Status em Alarmes do CloudWatch. O nome é percentage-disk-space-used-default-**<*string*>**. Você pode abrir o alarme para visualizar o tópico do Amazon SNS ao qual ele está associado e editar as configurações de alarme. Se você não selecionou um tópico existente do Amazon SNS para usar, o que foi criado para você é denominado **<*clustername*>**-default-alarms (**<*recipient*>**); por exemplo, examplecluster-default-alarms (notify@example.com).

Para obter mais informações sobre como configurar e editar o alarme padrão de espaço em disco, consulte Criar um cluster e Criar ou editar um alarme de espaço em disco.

> **Note**
>
> Se você excluir seu cluster, o alarme associado a ele não será excluído, mas não será acionado. Você pode excluir o alarme do console do CloudWatch se não precisar mais dele.

## Status do cluster

O status de cluster exibe o estado atual do cluster. A tabela a seguir fornece uma descrição para cada status de cluster.

| Status | Descrição |
| --- | --- |
| `available` | O cluster está em execução e disponível. |
| `available, prep-for-resize` | O cluster está sendo preparado para redimensionamento elástico. O cluster está em execução e disponível para consultas de leitura e gravação, mas as operações de cluster, como a criação de um snapshot, não estão disponíveis. |
| `available, resize-cleanup` | Uma operação de redimensionamento elástico está concluindo a transferência de dados para os novos nós do cluster. O cluster está em execução e disponível para consultas de leitura e gravação, mas as operações de cluster, como a criação de um snapshot, não estão disponíveis. |
| `cancelling-resize` | A operação de redimensionamento está sendo cancelada. |
| `creating` | O Amazon Redshift está criando o cluster. Para obter mais informações, consulte Criar um cluster. |
| `deleting` | O Amazon Redshift está excluindo o cluster. Para obter mais informaçõ es, consulte Excluir um cluster. |
| `final-snapshot` | O Amazon Redshift está tirando um snapshot final do cluster antes de excluí-lo. Para obter mais informações, consulte Excluir um cluster. |

| Status | Descrição |
| --- | --- |
| `hardware-failure` | O cluster sofreu uma falha de hardware.<br><br>Se você tem um cluster de único nó, o nó não pode ser substituído. Para recuperar seu cluster, restaure um snapshot. Para obter mais informaçõ es, consulte Snapshots e backups do Amazon Redshift. |
| `incompatible-hsm` | O Amazon Redshift não pode se conectar ao módulo de segurança de hardware (HSM). Verifique a configuração de HSM entre o cluster e o HSM. Para obter mais informações, consulte Criptografia para Amazon Redshift usando módulos de segurança de hardware. |
| `incompatible-network` | Há um problema com a configuração de rede subjacente. Certifique-se de que a VPC em que você implementou o cluster existe e que suas configurações estão corretas. Para obter mais informações, consulte Gerenciamento de clusters em uma VPC. |
| `incompatible-parameters` | Há um problema com um ou mais valores de parâmetros no parameter group associado e o valor ou valores de parâmetro não podem ser aplicados. Modifique o parameter group e atualize todos os valores inválidos. Para obter mais informações, consulte Grupos de parâmetros do Amazon Redshift. |
| `incompatible-restore` | Houve um problema ao restaurar o cluster a partir do snapshot. Tente restaurar o cluster novamente com um snapshot diferente. Para obter mais informações, consulte Snapshots e backups do Amazon Redshift. |
| `modifying` | O Amazon Redshift está aplicando mudanças ao cluster. Para obter mais informações, consulte Modificar um cluster. |
| `paused` | O cluster está pausado. Para obter mais informações, consulte Pausar e retomar clusters. |
| `rebooting` | O Amazon Redshift está reinicializando o cluster. Para obter mais informações, consulte Reinicialização de um cluster. |
| `renaming` | O Amazon Redshift está aplicando um novo nome ao cluster. Para obter mais informações, consulte Renomeação de clusters. |

| Status | Descrição |
| --- | --- |
| `resizing` | O Amazon Redshift está redimensionando o cluster. Para obter mais informações, consulte Redimensionamento de um cluster. |
| `rotating-keys` | O Amazon Redshift está alternando as chaves de criptografia para o cluster. Para obter mais informações, consulte Alternância de chave de criptografia no Amazon Redshift. |
| `storage-full` | O cluster alcançou sua capacidade de armazenamento. Redimensione o cluster para adicionar nós ou escolha um tamanho diferente de nó. Para obter mais informações, consulte Redimensionamento de um cluster. |
| `updating-hsm` | O Amazon Redshift está atualizando a configuração do HSM. |

# Considerações sobre o uso de clusters provisionados do Amazon Redshift

Após a criação do cluster for criado, você encontrará informações nesta seção sobre as regiões onde os recursos estão disponíveis, tarefas de manutenção, tipos de nó e limites de uso.

Tópicos

- Considerações sobre região e zona de disponibilidade
- Manutenção do cluster
- Gerenciar limites de uso no Amazon Redshift
- Atributos de rede compatíveis com os nós RA3
- Tipos de nó

## Considerações sobre região e zona de disponibilidade

O Amazon Redshift está disponível em diversas regiões da AWS. Por padrão, o Amazon Redshift provisiona o cluster em uma zona de disponibilidade (AZ) selecionada aleatoriamente na região da AWS escolhida. Todos os nós de cluster são provisionados na mesma zona de disponibilidade.

Opcionalmente, você pode solicitar uma zona de disponibilidade específica se o Amazon Redshift estiver disponível nessa zona. Por exemplo, se você já tem uma instância do Amazon EC2 em

execução em uma zona de disponibilidade, você pode querer criar seu cluster Amazon Redshift na mesma zona para reduzir a latência. Por outro lado, talvez você queira escolher outra zona de disponibilidade para obter maior disponibilidade. O Amazon Redshift pode não estar disponível em todas as zonas de disponibilidade em uma região da AWS.

Para conferir a lista de regiões da AWS nas quais você pode provisionar clusters do Amazon Redshift, consulte Endpoints do Amazon Redshift na Referência geral da Amazon Web Services.

## Manutenção do cluster

O Amazon Redshift realiza manutenção periodicamente para aplicar atualizações ao seu cluster. Durante essas atualizações, seu cluster do Amazon Redshift não está disponível para operações normais. Você tem várias maneiras de controlar como mantemos seu cluster. Por exemplo, você pode controlar quando implantamos atualizações em seus clusters. Também é possível escolher se o cluster executará a versão lançada mais recentemente ou a versão lançada antes da versão lançada mais recentemente. Por fim, você tem a opção de adiar atualizações de manutenção não obrigatórias por um período.

Tópicos


- Janelas de manutenção
- Adiamento da manutenção
- Selecionar acompanhamentos de manutenção do cluster
- Gerenciar versões do cluster
- Reverter a versão do cluster
- Determinar a versão de manutenção de cluster


### Janelas de manutenção

O Amazon Redshift atribui uma janela de manutenção de 30 minutos aleatoriamente a partir de um bloco de 8 horas por região da AWS, ocorrendo em um dia aleatório da semana (de segunda a domingo, inclusive).

Janelas de manutenção padrão

A lista a seguir mostra os blocos de tempo para cada região da AWS a partir da qual as janelas de manutenção padrão são atribuídas:

- Região Leste dos EUA (Norte da Virgínia): 03:00-11:00 UTC

- Região Leste dos EUA (Ohio): 03:00-11:00 UTC
- Região Oeste dos EUA (Norte da Califórnia): 06:00-14:00 UTC
- Região Oeste dos EUA (Oregon): 06:00-14:00 UTC
- Região da África (Cidade do Cabo): 20:00-04:00 UTC
- Região da Ásia-Pacífico (Hong Kong): 13:00-21:00 UTC
- Região Ásia-Pacífico (Haiderabade): 16h30–0h30 UTC
- Região Ásia-Pacífico (Jacarta): 15h – 23h UTC
- Região da Ásia-Pacífico (Melbourne): 12 - 20h UTC
- Região Ásia-Pacífico (Mumbai): 16:30-00:30 UTC
- Região Ásia-Pacífico (Osaka): 13:00-21:00 UTC
- Região Ásia-Pacífico (Seul): 13:00-21:00 UTC
- Região Ásia-Pacífico (Singapura): 14:00-22:00 UTC
- Região Ásia-Pacífico (Sydney): 12:00-20:00 UTC
- Região Ásia-Pacífico (Tóquio): 13:00-21:00 UTC
- Região do Canadá (Central) Região: 03:00-11:00 UTC
- Região Oeste do Canadá (Calgary): das 4h às 12h UTC
- Região da China (Pequim): 13:00-21:00 UTC
- Região da China (Ningxia): 13:00-21:00 UTC
- Região da Europa (Frankfurt): 06:00-14:00 UTC
- Região da Europa (Irlanda): 22:00-06:00 UTC
- Região da Europa (Londres): 22:00-06:00 UTC
- Região da Europa (Milão): 21:00-05:00 UTC
- Região da Europa (Paris): 23:00-07:00 UTC
- Região da Europa (Estocolmo): 23:00-07:00 UTC
- Região Europa (Zurique): 20h–4h UTC
- Região de Israel (Tel Aviv): 20h-4h UTC
- Região Europa (Espanha): 21h–5h UTC
- Região do Oriente Médio (Bahrein): 13:00-21:00 UTC
- Região do Oriente Médio (EAU): 18h00-2h00 UTC

- Região da América do Sul (São Paulo): 19:00-03:00 UTC

Se um evento de manutenção estiver agendado para determinada semana, ele começará durante a janela de manutenção de 30 minutos atribuída. Enquanto o Amazon Redshift está realizando a manutenção, ele encerra todas as consultas ou outras operações que estão em andamento. A maior parte da manutenção é concluída durante a janela de manutenção de 30 minutos, mas algumas tarefas de manutenção podem continuar sendo executadas após o fechamento da janela. Se não há tarefas de manutenção a executar durante a janela de manutenção programada, seu cluster continua a operar normalmente até a próxima janela de manutenção programada.

Você pode alterar a janela de manutenção programada modificando o cluster, seja programaticamente ou usando o console do Amazon Redshift. Você pode encontrar a janela de manutenção e definir o dia e a hora em que ela ocorre para o cluster na guia Manutenção.

É possível que um cluster seja reiniciado fora de uma janela de manutenção. Isso pode ocorrer por alguns motivos. O mais comum é quando um problema é detectado no cluster e as operações de manutenção são executadas para trazê-lo de volta a um estado íntegro. Para obter mais informações, consulte o artigo Por que meu cluster do Amazon Redshift foi reinicializado fora da janela de manutenção?, que fornece detalhes sobre por que isso pode ocorrer.

## Adiamento da manutenção

Para reprogramar a janela de manutenção do cluster, você pode adiar a manutenção em até 45 dias. Por exemplo, se a janela de manutenção do cluster estiver definida para quarta-feira das 8h30 às 9h00 UTC e você precisar acessar o cluster nesse período, será possível adiar a manutenção para um momento posterior.

Se você adiar a manutenção, o Amazon Redshift ainda aplicará atualizações de hardware ou outras atualizações de segurança obrigatórias ao cluster. O cluster não ficará disponível durante essas atualizações.

Se uma atualização de hardware ou outra atualização de segurança obrigatória estiver programada durante a próxima janela de manutenção, o Amazon Redshift enviará notificações antecipadas na categoria Pendente. Para saber mais sobre notificações de eventos pendentes, consulte Notificações de eventos do Amazon Redshift.

Também é possível optar por receber notificações do Amazon Simple Notification Service (Amazon SNS). Para obter mais informações sobre como assinar notificações de eventos do Amazon SNS, consulte Assinar notificações de eventos de cluster do Amazon Redshift.

Se você adiar a manutenção do cluster, a janela de manutenção após o período de adiamento não poderá ser protelada.

> **Note**
>
> Você não pode adiar a manutenção depois que ela foi iniciada.

Para obter mais informações sobre manutenção de cluster, consulte a seguinte documentação:

- Janelas de manutenção
- Gerenciamento de clusters usando o console
- Modificar um cluster

## Selecionar acompanhamentos de manutenção do cluster

Quando o Amazon Redshift lança uma nova versão do cluster, seu cluster é atualizado durante a janela de manutenção. É possível controlar se o cluster será atualizado para a versão mais recente aprovada ou para a versão anterior.

O acompanhamento de manutenção controla qual versão do cluster será aplicada durante uma janela de manutenção. Quando o Amazon Redshift lança uma nova versão do cluster, essa versão é atribuída à trilha atual e a versão anterior é atribuída à trilha posterior. Para definir o acompanhamento de manutenção para o cluster, especifique um dos seguintes valores:

- Atual – Usa a versão de cluster aprovada mais recente.
- Anterior – Usa a versão do cluster antes da versão atual.
- Previsualização – Usa a versão do cluster que contém os novos recursos disponíveis para previsualização.

Por exemplo, suponha que seu cluster esteja executando a versão 1.0.2762 e a versão atual do Amazon Redshift seja 1.0.3072. Se você definir o valor do acompanhamento de manutenção para Current (Atual), o cluster será atualizado para a versão 1.0.3072 (a próxima versão aprovada) durante a próxima janela de manutenção. Se o valor do acompanhamento de manutenção do cluster for definido para Trailing (Anterior), o cluster não será atualizado até que haja uma nova versão após a 1.0.3072.

### Trilhas de demonstração

Uma trilha de Preview (Demonstração) pode não estar disponível para escolha. Ao escolher uma trilha de Preview (Demonstração), um nome de trilha deve ser selecionado. As trilhas de previsualização e seus recursos relacionados são temporários, têm limitações funcionais e podem não conter todos os recursos atuais do Amazon Redshift disponíveis em outros trilhos. Ao trabalhar com trilhas de demonstração:

- Use o novo console do Amazon Redshift ao trabalhar com trilhas de visualização. Por exemplo, quando você cria um cluster para usar com recursos de demonstração.
- Não é possível alternar um cluster de uma trilha de demonstração para outra.
- Não é possível alternar um cluster para uma trilha de demonstração de uma trilha atual ou inicial.
- Não é possível alternar um cluster de uma trilha de prévia para uma trilha atual ou inicial.
- Não é possível restaurar um snapshot criado em uma trilha de demonstração diferente.
- Só é possível usar a trilha de demonstração ao criar um novo cluster ou ao restaurar de um snapshot.
- Não é possível restaurar de um snapshot criado em uma trilha de demonstração diferente ou com uma versão de manutenção do cluster posterior à versão do cluster da trilha de demonstração. Por exemplo, ao restaurar um cluster para uma trilha de demonstração, você só pode usar um snapshot criado em uma versão de manutenção de cluster anterior à da trilha de demonstração.

### Alternar entre acompanhamentos de manutenção

Alterar o acompanhamento de um cluster costuma ser uma decisão única. Você deve ter cuidado ao mudar de acompanhamento. Se você alterar o acompanhamento de manutenção de Trailing (Anterior) para Current (Atual), atualizaremos o cluster para a versão de acompanhamento Current (Atual) durante a próxima janela de manutenção. No entanto, se você alterar o acompanhamento de manutenção do cluster para Trailing (Anterior), não atualizaremos seu cluster até que haja uma nova versão após a versão de acompanhamento Current (Atual).

### Acompanhamento de manutenção e restaurar

Um snapshot herda o acompanhamento de manutenção do cluster de origem. Se você alterar o acompanhamento de manutenção do cluster de origem depois de obter um snapshot, o snapshot e o cluster de origem estarão em acompanhamentos diferentes. Quando você fizer a restauração de um snapshot, o novo cluster estará no acompanhamento de manutenção herdado do cluster de origem. É possível alterar o acompanhamento de manutenção após a conclusão da operação de

restauração. O redimensionamento de um cluster não afeta o acompanhamento de manutenção do cluster.

## Gerenciar versões do cluster

Um acompanhamento de manutenção é uma série de versões. Você pode decidir se o cluster estará no acompanhamento Atual ou no acompanhamento Anterior. Se você colocar seu cluster no acompanhamento Atual, ele sempre será atualizado para a versão mais recente do cluster durante a janela de manutenção. Se você colocar seu cluster no acompanhamento Anterior, ele sempre executará a versão do cluster lançada imediatamente antes da versão lançada mais recentemente.

A coluna Status da versão na lista de clusters do console do Amazon Redshift indica se um de seus clusters está disponível para atualização.

## Reverter a versão do cluster

Se o cluster estiver atualizado com a versão mais recente, você poderá optar por revertê-lo para a versão anterior.

Para obter informações detalhadas sobre os recursos e as melhorias incluídas em cada versão de cluster, consulte Histórico das versões de cluster.

Para reverter para uma versão anterior do cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters.
3. Selecione o cluster a ser revertido.
4. Em Actions (Ações), escolha Roll back cluster version (Reverter versão de cluster). A página Roll back cluster version (Reverter versão de cluster) é exibida.
5. Se houver uma versão disponível para reversão, siga as instruções na página.
6. Escolha Roll back now (Reverter agora).

## Determinar a versão de manutenção de cluster

Você pode determinar o mecanismo do Amazon Redshift e a versão do banco de dados com o console do Amazon Redshift.

Para encontrar a versão de um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters e o nome do cluster na lista para abrir os respectivos detalhes. Os detalhes do cluster são exibidos, podendo incluir as guias Cluster performance (Performance do cluster), Query monitoring (Monitoramento de consultas), Databases (Bancos de dados), Datashares (Unidades de compartilhamento de dados), Schedules (Programação), Maintenance (Manutenção) e Properties (Propriedades).
3. Escolha a guia Manutenção para obter mais detalhes.
4. Na seção Maintenance (Manutenção), localize a Current cluster version (Versão atual do cluster).

> **Note**
>
> Embora o console exiba essas informações em um campo, são dois parâmetros na API do Amazon Redshift, `ClusterVersion` e `ClusterRevisionNumber`. Para obter mais informações, consulte Cluster na Referência da API do Amazon Redshift.

## Gerenciar limites de uso no Amazon Redshift

Você pode definir limites para monitorar e controlar o uso e o custo associado de alguns recursos do Amazon Redshift. Você pode criar limites de uso diário, semanal e mensal e definir ações que o Amazon Redshift executará automaticamente se esses limites forem atingidos. As ações incluem coisas como registrar em log um evento em uma tabela do sistema para registrar o uso que excede seus limites definidos. Outras ações possíveis incluem a geração de alertas com o Amazon SNS e o Amazon CloudWatch para notificar um administrador e desabilitar uso adicional para controlar os custos.

É possível definir limites de uso para cada cluster. Depois que o cluster é criado, você pode definir limites de uso para os seguintes recursos:

- Amazon Redshift Spectrum
- Amazon Redshift Concurrency Scaling
- Compartilhamento de dados do Amazon Redshift entre regiões

Os limites de uso estão disponíveis com a versão 1.0.14677 ou posterior nas regiões da AWS em que o Amazon Redshift Spectrum e o Amazon Redshift Concurrency Scaling estão disponíveis.

Um limite do Redshift Spectrum especifica o limite da quantidade total de dados verificados em incrementos de 1 TB. Um limite de escalabilidade de simultaneidade especifica o limite do tempo total usado pela escalabilidade de simultaneidade em incrementos de 1 minuto. Um limite de compartilhamento de dados entre regiões especifica o limiar da quantidade total de dados verificados em incrementos de 1 TB.

Um limite pode ser especificado para um período diário, semanal ou mensal (usando UTC para determinar o início e o fim do período). Se você criar um limite no meio de um período, o limite será medido desse ponto até o final do período. Por exemplo, se você criar um limite mensal em 15 de março, o primeiro período mensal será medido de 15 de março a 31 de março.

Você pode definir vários limites de uso para cada recurso. Cada limite pode ter uma ação diferente. As ações possíveis incluem o seguinte:

- Registrar na tabela do sistema – essa é a ação padrão. As informações são registradas em log na tabela STL_USAGE_CONTROL. O registro em log é útil ao avaliar o uso passado e ao decidir sobre limites de uso futuros. Para obter mais informações sobre o que é registrado em log, consulte STL_USAGE_CONTROL no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- Alerta — O Amazon Redshift emite métricas do CloudWatch para uso disponível e consumido. Você pode definir até três limites de uso para cada recurso. Se você habilitar a ação de alerta usando o console do Amazon Redshift, um alarme do CloudWatch será criado automaticamente nessas métricas. Opcionalmente, você pode associar uma assinatura do Amazon SNS a esse alarme. Se estiver usando uma operação da AWS CLI ou de API, crie o alarme do CloudWatch manualmente. Quando o limite é atingido, os eventos também serão registrados em log em uma tabela do sistema.
- Desabilitar recurso – Quando o limite é atingido, o Amazon Redshift desabilita o recurso até que a cota seja atualizada para o próximo período (diário, semanal ou mensal). Apenas um limite para cada recurso pode ter a ação de desativar. Os eventos também são registrados em log em uma tabela do sistema, e os alertas podem ser emitidos.

Os limites de uso persistem até que a própria definição de limite de uso ou o cluster seja excluído.

Você pode definir e gerenciar limites de uso com o novo console do Amazon Redshift, a AWS CLI, ou com operações da API do Amazon Redshift. Para definir um limite no console do Amazon

Redshift, navegue até o cluster e escolha Configurar limite de uso para Ações. Para visualizar os limites de uso definidos anteriormente para o cluster, navegue até o cluster e escolha a guia Manutenção e monitoramento na seção Limites de uso. Para visualizar a quantidade de uso disponível e consumida para o cluster, navegue até o cluster. Escolha a guia Performance do cluster e visualize os gráficos para verificar o uso consumido de um recurso.

Você pode usar as operações da CLI do Amazon Redshift a seguir para gerenciar limites de uso. Para obter mais informações, consulte a Referência de comandos da AWS CLI.

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

Você pode usar as operações da API do Amazon Redshift a seguir para gerenciar limites de uso. Para obter mais informações, consulte a Referência de API do Amazon Redshift.

- CreateUsageLimit
- DescribeUsageLimits
- ModifyUsageLimit
- DeleteUsageLimit

Assista ao vídeo a seguir para saber como criar e monitorar limites de uso usando o console do Amazon Redshift: Controles de custos do Amazon Redshift Spectrum e Concurrency Scaling.

## Atributos de rede compatíveis com os nós RA3

Os nós RA3 são compatíveis com um conjunto de recursos de rede indisponíveis para nós DC2 ou DS2. Esta seção fornece uma breve descrição de cada recurso e links para outros documentos:

- Endpoint da VPC de cluster provisionado: quando você cria ou restaura um cluster RA3, o Amazon Redshift usa uma porta dentro dos intervalos 5431-5455 ou 8191-8215. Quando o cluster é configurado como uma porta em um desses intervalos, o Amazon Redshift cria automaticamente um endpoint da VPC para o cluster em sua conta da AWS e anexa um endereço IP privado a ele. Se você definir o cluster como acessível ao público, o Redshift criará um endereço IP elástico na sua conta da AWS e o anexará ao endpoint da endpoint da VPC. Para obter mais informações,

consulte Definir as configurações de comunicação do grupo de segurança para um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor.

- Clusters RA3 de sub-rede única: é possível criar um cluster RA3 com uma única sub-rede, mas ele não pode usar atributos de recuperação de desastres. Uma exceção ocorrerá se você habilitar a realocação do cluster quando a sub-rede não tiver várias zonas de disponibilidade (AZs).
- Clusters RA3 de várias sub-redes e grupos de sub-redes: é possível criar um cluster RA3 com várias sub-redes criando um grupo de sub-redes ao provisionar o cluster na nuvem privada virtual (VPC). Um grupo de sub-redes de cluster permite que você especifique um conjunto de sub-redes na VPC para que o Amazon Redshift crie o cluster em uma delas. Após a criação de um grupo de sub-redes, é possível remover as sub-redes adicionadas anteriormente ou adicionar mais sub-redes. Para obter mais informações, consulte Grupos de sub-rede de cluster do Amazon Redshift.
- Acesso entre contas ou acesso entre endpoints da VPC: é possível acessar um cluster provisionado ou um grupo de trabalho do Amazon Redshift sem servidor configurando um endpoint da VPC gerenciado pelo Redshift. Você pode configurá-la como uma conexão privada entre uma VPC que contém um cluster ou grupo de trabalho e uma VPC na qual você executa uma ferramenta cliente, por exemplo. Desse modo, você pode acessar o data warehouse sem usar endereços IP públicos ou rotear tráfego pela internet. Para obter mais informações, consulte Trabalhando com endpoints da VPC gerenciados por Redshift no Amazon Redshift.
- Relocação de clusters: é possível mover um cluster para outra zona de disponibilidade (AZ) sem perda de dados quando há uma interrupção do serviço. Você o habilita no console. Para ter mais informações, consulte Realocar um cluster.
- Nome de domínio personalizado: é possível criar um nome de domínio personalizado, também conhecido como URL personalizado, para o cluster do Amazon Redshift. É um registro DNS fácil de ler que roteia as conexões do cliente SQL para o endpoint do cluster. Para ter mais informações, consulte Usar um nome de domínio personalizado para conexões de clientes.

## Tipos de nó

Essas seções detalham as tarefas disponíveis para vários tipos de nó.

Tópicos

- Nós RA3
- Nós DC2 e DS2

# Nós RA3

Essas seções detalham as tarefas disponíveis para nós RA3.

Tópicos


- Visão geral
- Atualizar para os tipos de nó RA3


## Visão geral

Recomendamos que você atualize os workloads existentes em execução em clusters do tipo de nó DS2 para os tipos de nó RA3 a fim de aproveitar a performance aprimorada e obter mais capacidade de armazenamento. Os nós RA3 fornecem as seguintes vantagens:

- Eles são flexíveis para aumentar a capacidade computacional sem aumentar os custos de armazenamento. Além disso, eles dimensionam o armazenamento sem provisionar em excesso a capacidade computacional.
- Eles usam SSDs de alta performance para seus dados quentes e Amazon S3 para dados frios. Assim, eles oferecem facilidade de uso, armazenamento econômico e alta performance de consultas.
- Eles usam rede de alta largura de banda construída no AWS Nitro System para reduzir ainda mais o tempo necessário para que os dados sejam descarregados e recuperados do Amazon S3.

Considere escolher tipos de nó RA3 nos seguintes casos:

- Você precisa de flexibilidade para escalar e pagar pela computação separada do armazenamento.
- Você consulta uma fração de seus dados totais.
- Seu volume de dados está crescendo rapidamente ou espera-se que ele cresça rapidamente.
- Você quer a flexibilidade de dimensionar o cluster com base somente em suas necessidades de performance.

Para usar tipos de nó RA3, a região da AWS deverá ser compatível com RA3. Para obter mais informações, consulte Disponibilidade do tipo de nó RA3 nas regiões da AWS.

> **Important**
>
> Você pode usar os tipos de nó ra3.xlplus apenas com o cluster versão 1.0.21262 ou posterior. Você pode visualizar a versão de um cluster existente com o console do Amazon Redshift. Para obter mais informações, consulte Determinar a versão de manutenção de cluster.
>
> Certifique-se de usar o novo console do Amazon Redshift ao trabalhar com tipos de nó RA3. Além disso, para usar tipos de nó RA3 com operações do Amazon Redshift que usam a trilha de manutenção, o valor da trilha de manutenção deve ser definido para uma versão de cluster que suporte RA3. Para obter mais informações sobre o acompanhamento de manutenção, consulte Selecionar acompanhamentos de manutenção do cluster.

Considere o seguinte ao usar tipos de nó RA3 de nó único.

- Há suporte para produtores e consumidores de unidade de compartilhamento de dados.
- Para alterar os tipos de nós, somente o redimensionamento clássico é compatível. Não é possível alterar o tipo de nó com redimensionamento elástico ou restauração de snapshot. Há suporte para os seguintes cenários:
  - Redimensionamento clássico de um ds2.xlarge de 1 nó para um ra3.xlplus de 1 nó e vice-versa.
  - Redimensionamento clássico de um ds2.xlarge de 1 nó para um ra3.xlplus de vários nós e vice-versa.
  - Redimensionamento clássico de um ds2.xlarge de vários nós para um ra3.xlplus de 1 nó e vice-versa.
  - Redimensionamento clássico de um dc2.xlarge de 1 nó para um ra3.xlplus de 1 nó e vice-versa.
  - Redimensionamento clássico de um dc2.xlarge de 1 nó para um ra3.xlplus de vários nós e vice-versa.
  - Redimensionamento clássico de um dc2.xlarge de vários nós para um ra3.xlplus de 1 nó e vice-versa.

### Trabalhar com o armazenamento gerenciado do Amazon Redshift

Com o armazenamento gerenciado do Amazon Redshift, você pode armazenar e processar todos os seus dados no Amazon Redshift enquanto obtém mais flexibilidade para escalar a capacidade de computação e armazenamento separadamente. Você pode continuar a ingerir dados com o comando COPY ou INSERT. Para otimizar a performance e gerenciar o posicionamento automático

de dados nas camadas de armazenamento, o Amazon Redshift tira proveito de otimizações como temperatura do bloco de dados, idade do bloco de dados e padrões de workload. Quando necessário, o Amazon Redshift escla o armazenamento automaticamente para o Amazon S3 sem exigir nenhuma ação manual.

Para obter mais informações sobre os custos de armazenamento, consulte Preços Amazon Redshift.

Gerenciar tipos de nó RA3

Para aproveitar a separação entre a computação e o armazenamento, é possível criar ou atualizar o cluster com o tipo de nó RA3. Para usar os tipos de nó RA3, crie seus clusters em uma virtual private cloud (EC2-VPC).

Para alterar o número de nós do cluster do Amazon Redshift com um tipo de nó RA3, siga um destes procedimentos:

- Adicione ou remova nós com a operação de redimensionamento elástico. Em algumas situações, a remoção de nós de um cluster RA3 não é permitida com o redimensionamento elástico. Por exemplo, quando uma atualização de contagem de nós 2:1 coloca o número de fatias por nó em 32. Para obter mais informações, consulte Redimensionar clusters. Se o redimensionamento elástico não estiver disponível, use o redimensionamento clássico.
- Adicione ou remova nós com a operação clássica de redimensionamento. Escolha essa opção quando estiver redimensionando para uma configuração que não esteja disponível por meio de redimensionamento elástico. O redimensionamento elástico é mais rápido do que o redimensionamento clássico. Para obter mais informações, consulte Redimensionar clusters.

Disponibilidade do tipo de nó RA3 nas regiões da AWS

Os tipos de nós RA3 estão disponíveis apenas nas seguintes regiões da AWS:

- Região Leste dos EUA (Norte da Virgínia) (us-east-1)
- Região Leste dos EUA (Ohio) (us-east-2)
- Região Oeste dos EUA (Norte da Califórnia) us-west-1
- Região Oeste dos EUA (Oregon) us-west-2
- Região da África (Cidade do Cabo) (af-south-1)
- Região da Ásia-Pacífico (Hong Kong) (ap-east-1)
- Região Ásia-Pacífico (Haiderabade) (ap-south-2)

- Região da Ásia-Pacífico (Jakarta) (ap-southeast-3)
- Região da Ásia-Pacífico (Melbourne) (ap-southeast-4)
- Região da Ásia-Pacífico (Mumbai) (ap-south-1)
- Região da Ásia-Pacífico (Osaka) (ap-northeast-3)
- Região da Ásia-Pacífico (Seul) (ap-northeast-2)
- Região da Ásia-Pacífico (Singapura) (ap-southeast-1)
- Região da Ásia-Pacífico (Sydney) (ap-southeast-2)
- Região da Ásia-Pacífico (Tóquio) (ap-northeast-1)
- Região do Canadá (Central) (ca-central-1)
- Região Oeste do Canadá (Calgary) (ca-west-1)
- Região da China (Pequim) (cn-north-1)
- Região da China (Ningxia) (cn-northwest-1)
- Região da Europa (Frankfurt) (eu-central-1)
- Região Europa (Zurique) (eu-central-2)
- Região da Europa (Irlanda) (eu-west-1)
- Região da Europa (Londres) (eu-west-2)
- Região da Europa (Milão) (eu-south-1)
- Região Europa (Espanha) (eu-south-2)
- Região da Europa (Paris) (eu-west-3)
- Região da Europa (Estocolmo) (eu-north-1)
- Região de Israel (Tel Aviv) (il-central-1)
- Região do Oriente Médio (Bahrein) (me-south-1)
- Região do Oriente Médio (EAU) (me-central-1)
- Região da América do Sul (São Paulo) (sa-east-1)
- AWS GovCloud (Leste dos EUA) (us-gov-east-1)
- AWS GovCloud (Oeste dos EUA) (us-gov-wast-1)

### Atualizar para os tipos de nó RA3

Para atualizar o tipo de nó existente para o RA3, você tem as seguintes opções para alterar o tipo de nó:

- Restaurar de um snapshot — O Amazon Redshift usa o snapshot mais recente de seu cluster DS2 ou DC2 e o restaura para criar um novo cluster RA3. Assim que a criação do cluster for concluída (geralmente em minutos), os nós RA3 estarão prontos para executar o workload de produção completo. Como a computação é separada do armazenamento, os dados quentes são trazidos para o cache local em velocidades rápidas graças a uma grande largura de banda de rede. Se você restaurar usando o snapshot DS2 ou DC2 mais recente, o RA3 preservará as informações de blocos quentes do workload DS2 ou DC2 e preencherá o cache local com os blocos mais quentes. Para obter mais informações, consulte Restauração de um cluster usando um snapshot.

  Para manter o mesmo endpoint para seus aplicativos e usuários, você pode renomear o novo cluster RA3 com o mesmo nome do cluster DS2 ou DC2 original. Para renomear o cluster, modifique-o no console do Amazon Redshift ou na operação de API `ModifyCluster`. Para obter mais informações, consulte Renomeação de clusters ou Operação de API `ModifyCluster` na Referência da API do Amazon Redshift.
- Redimensionamento elástico — Redimensiona o cluster usando o redimensionamento elástico. Ao usar o redimensionamento elástico para alterar o tipo de nó, o Amazon Redshift cria automaticamente um snapshot, cria um novo cluster, exclui o cluster antigo e renomeia o novo cluster. A operação de redimensionamento elástico pode ser executada sob demanda ou pode ser programada para execução em um momento futuro. É possível atualizar rapidamente os clusters de tipo de nó DS2 ou DC2 existentes para o RA3 com redimensionamento elástico. Para obter mais informações, consulte Elastic resize (Redimensionamento elástico).

A tabela a seguir mostra recomendações ao atualizar para os tipos de nó RA3. (Essas recomendações também se aplicam a nós reservados.)

As recomendações nesta tabela referem-se aos tipos e tamanhos iniciais dos nós do cluster, mas dependem dos requisitos de computação da workload. Para avaliar melhor seus requisitos, considere a possibilidade de realizar uma prova de conceito (POC) que use o Test Drive para executar possíveis configurações. Em vez de provisionar um cluster para o Redshift sem servidor, provisione-o para a POC de seu data warehouse. Para obter mais informações sobre como conduzir uma prova de conceito, consulte Realizar uma prova de conceito (POC) para o Amazon Redshift no Guia do desenvolvedor do banco de dados do Amazon Redshift.

| Tipo de nó existente | Número de nós existente | Novo tipo de nó recomendado | Ação de atualização |
|---|---|---|---|
| ds2.xlarge | 1 | ra3.xlplus | Crie um cluster ra3.xlplus de 1 nó[1]. |
| ds2.xlarge | 2 | ra3.xlplus | Crie um cluster ra3.xlplus de 2 nós[1]. |
| ds2.xlarge | 3 | ra3.xlplus | Crie um cluster ra3.xlplus de 2 nós[1]. |
| ds2.xlarge | 4 | ra3.xlplus | Crie um cluster ra3.xlplus de 3 nós[1]. |
| ds2.xlarge | 5 | ra3.xlplus | Crie um cluster ra3.xlplus de 4 nós[1]. |
| ds2.xlarge | 6 | ra3.xlplus | Crie um cluster ra3.xlplus de 4 nós[1]. |
| ds2.xlarge | 7 | ra3.xlplus | Crie um cluster ra3.xlplus de 5 nós[1]. |
| ds2.xlarge | 8 | ra3.4xlarge | Crie um cluster ra3.4xlarge de 2 nós[1]. |
| ds2.xlarge | 9 | ra3.4xlarge | Crie um cluster ra3.4xlarge de 3 nós[1]. |

| Tipo de nó existente | Número de nós existente | Novo tipo de nó recomendado | Ação de atualização |
|---|---|---|---|
| ds2.xlarge | 10 | ra3.4xlarge | Crie um cluster ra3.4xlarge de 3 nós[1]. |
| ds2.xlarge | 11-128 | ra3.4xlarge | Crie 1 nó de ra3.4xlarge para cada 4 nós de ds2.xlarge[1]. |
| ds2.8xlarge | 2–15 | ra3.4xlarge | Crie 2 nós de ra3.4xlarge para cada nó de ds2.8xlarge[1]. |
| ds2.8xlarge | 16–128 | ra3.16xlarge | Crie 1 nó de ra3.16xlarge para cada 2 nós de ds2.8xlarge[1]. |
| dc2.8xlarge | 2–15 | ra3.4xlarge | Crie 2 nós de ra3.4xlarge para cada nó de dc2.8xlarge[1]. |
| dc2.8xlarge | 16–128 | ra3.16xlarge | Crie 1 nó de ra3.16xlarge para cada 2 nós de dc2.8xlarge[1]. |
| dc2.large | 1–4 | nenhuma | Mantenha o cluster dc2.large existente. |

| Tipo de nó existente | Número de nós existente | Novo tipo de nó recomendado | Ação de atualização | |
|---|---|---|---|---|
| dc2.large | 5–15 | ra3.xlplus | Crie 3 nós de ra3.xlplus para cada 8 nós de dc2.large[1]. | |
| dc2.large | 16 - 32 | ra3.4xlarge | Crie 1 nó de ra3.4xlarge para cada 8 nós de dc2.large[1,2]. | |

[1]Poderão ser necessários nós adicionais dependendo dos requisitos de workload. Adicione ou remova nós com base nos requisitos de computação da performance de consulta necessária.

[2] Os clusters com o tipo de nó dc2.large são limitados a 32 nós.

O número mínimo de nós para clusters de alguns tipos de nó RA3 é de dois nós. Leve isso em consideração ao criar um cluster RA3.

Atualize os nós reservados DS2 para nós reservados RA3 durante o redimensionamento elástico ou a restauração de snapshots

Se você tiver nós reservados DS2, poderá atualizá-los com o recurso de atualização de nós reservados RA3, usando o console do Amazon Redshift ou a AWS CLI. No console, há duas maneiras de fazer isso.

Uma maneira é atualizar os nós reservados DS2 para RA3 durante um redimensionamento elástico. Se você tiver nós reservados e selecionar nós RA3, o console o orientará pelo processo de atualização de nó reservado. Do ponto de vista técnico, o redimensionamento elástico funciona da mesma forma para nós reservados e nós que não são reservados.

Se você alterar o tamanho do cluster do tamanho recomendado, quando configurar o redimensionamento elástico, a atualização de nós reservados RA3 não estará disponível e não será exibida no console. (Mesmo assim, é possível atualizar os nós reservados DS2 para RA3, mas o redimensionamento não inclui a atualização dos nós reservados RA3 como parte do processo.) Observe também que o tamanho de cluster desejado pode não estar disponível devido a limitações de tamanho de cluster para redimensionamento elástico. Por exemplo, se você tiver um cluster de nó

reservado DS2 de 4 nós, talvez não consiga selecionar um cluster RA3 de 3 nós. Nesse caso, você pode executar um redimensionamento clássico para obter o tamanho de cluster desejado.

Algumas etapas ocorrem após o redimensionamento do cluster. Primeiro, os dados são migrados para o cluster RA3. Em seguida, a concessão de nó reservado DS2 é convertida em uma concessão de nó reservado RA3. Observe que o tempo necessário para a migração dos dados pode variar, dependendo do tamanho do cluster e de o redimensionamento ser elástico ou clássico. No caso de um redimensionamento clássico, é comum que a migração de dados leve várias horas.

Depois de iniciar o redimensionamento, acompanhe o progresso visualizando as mensagens em Events (Eventos), disponível no Painel do Amazon Redshift. Existe uma notificação de evento para o redimensionamento e outra para a atualização do nó reservado. Para obter informações sobre como trabalhar com eventos, consulte Eventos do Amazon Redshift. Após o redimensionamento, o cluster redimensionado ativo aparece no AWS Management Console. Você também pode visualizar a concessão de nó reservado RA3 convertida. Os nós reservados DS2 de origem podem continuar a aparecer no console por cerca de um dia. Eles não são cobrados de você. Não exclua o nó reservado DS2 de origem até verificar que o cluster RA3 está ativo e que a concessão do nó reservado convertida foi gerada.

A outra forma de usar o recurso de atualização de nó reservado RA3 é restaurar a partir de um snapshot. Se você selecionar o tipo de nó RA3 e tiver nós reservados DS2, poderá selecionar o recurso de atualização de nós reservados RA3 nesse ponto. Quando você restaura a partir de um snapshot, ele é restaurado para um cluster de nó reservado RA3. Como mencionado anteriormente, se você escolher um tamanho de cluster diferente do tamanho recomendado, a seleção de atualização de nó reservado RA3 não estará disponível no console.

Para obter mais informações sobre redimensionamento e atualização de clusters, consulte Redimensionar clusters. Lá, você pode encontrar uma descrição detalhada do processo e também respostas sobre o que acontece com o cluster e com os dados quando você os redimensiona. Para obter mais detalhes sobre as etapas do processo de redimensionamento elástico, consulte Elastic resize (Redimensionamento elástico). Para obter mais informações sobre a restauração a partir de um snapshot, consulte Restauração de um cluster usando um snapshot.

Caso tenha mais dúvidas sobre a atualização de nós reservados para o RA3, por exemplo, sobre a atualização de nós reservados DC2 para RA3, entre em contato com o AWS Support. Para obter informações sobre preço de nós sob demanda e reservados, consulte Preços do Amazon Redshift.

Se você já adquiriu nós reservados DS2, entre em contato com a AWS para obter ajuda com a conversão de nós reservados DS2 em nós reservados RA3. Para entrar em contato com a AWS

para obter mais informações, consulte as Instâncias do Amazon Redshift RA3 com armazenamento gerenciado.

## Nós DC2 e DS2

Essas seções detalham as tarefas disponíveis para nós DC2 e DS2.

Tópicos

- Atualizar de tipos de nó DC1 para tipos de nó DC2
- Atualizar um cluster de DS2 no EC2-Classic para EC2-VPC

### Atualizar de tipos de nó DC1 para tipos de nó DC2

Para aproveitar as melhorias de performance, é possível atualizar o cluster DC1 para os tipos de nó DC2.

Os clusters que usam o tipo de nó DC2 devem ser iniciados em uma nuvem privada virtual (EC2-VPC).

Se o cluster DC1 não estiver em uma VPC:

1. Crie um snapshot do cluster DC1. Para obter mais informações, consulte Snapshots e backups do Amazon Redshift.
2. Crie uma VPC ou escolha uma VPC existente em sua conta. Para obter mais informações, consulte Gerenciamento de clusters em uma VPC.
3. Restaure seu snapshot para um novo cluster DC2 no VPC. Para obter mais informações, consulte Restauração de um cluster usando um snapshot.

Se o cluster DC1 já estiver em uma VPC, escolha um dos seguintes métodos:

- Redimensione o cluster DC1 e altere o tipo de nó para DC2 como parte da operação. O cluster fica indisponível por um período durante a operação de redimensionamento. Para obter mais informações, consulte Redimensionar clusters.
- Crie um snapshot do cluster DC1 e restaure o snapshot para um cluster DC2 na VPC. Para obter mais informações, consulte Restauração de um cluster usando um snapshot.

Considere o seguinte ao atualizar os tipos de nós DC1 para DC2.

- Os clusters DC1 100% completos podem não atualizar para um número equivalente de nós DC2. Se houver necessidade de mais espaço em disco, é possível:
  - Redimensionar para uma configuração com mais espaço em disco disponível.
  - Limpe os dados desnecessários ao truncar as tabelas ou ao excluir linhas.
- Os clusters do DC2 não oferecem suporte para redes do EC2-Classic. Se o seu cluster do DC1 não estiver em execução em uma VPC, crie uma para sua migração ao DC2. Para obter mais informações, consulte Gerenciamento de clusters em uma VPC.
- Se você redimensionar o cluster, ele poderá ser colocado no modo somente leitura durante a operação. Para obter mais informações, consulte Redimensionar clusters.
- Se você comprou nós reservados DC1, é possível atualizar os nós reservados DC1 para nós DC2 para o restante do período de vigência. Para obter mais informações sobre como alterar a reserva com a AWS CLI, consulte Atualizar nós reservados com a AWS CLI.
- Se você usar a restauração para atualizar de dc1.large para dc2.large e alterar o número de nós, o snapshot deverá ter sido criado na versão do cluster 1.0.10013 ou posterior.
- Se você usar a restauração para atualizar de dc1.8xlarge para dc2.8xlarge, o snapshot deverá ter sido criado na versão do cluster 1.0.10013 ou posterior.
- Se você usar o redimensionamento elástico para atualizar de DC1 para DC2 e alterar o número de nós, o cluster deverá estar na versão do cluster 1.0.10013 ou posterior.
- Se um snapshot do cluster de dc1.8xlarge para atualização for de um cluster anterior à versão 1.0.10013, primeiro restaure o snapshot do cluster dc1.8xlarge em um novo cluster de dc1.8xlarge com o mesmo número de nós. Em seguida, use um dos seguintes métodos para atualizar o novo dc1.8xlarge:
  - Use um snapshot do novo cluster restaurado para atualizar para dc2.8xlarge.
  - Use o redimensionamento elástico para atualizar o novo cluster restaurado para dc2.8xlarge.

### Atualizar um cluster de DS2 no EC2-Classic para EC2-VPC

Os clusters do Amazon Redshift são executados em instâncias do Amazon EC2 configuradas para o tipo e tamanho de nó do Amazon Redshift que você escolher. Recomendamos que você atualize seu cluster no EC2-Classic para iniciar em uma VPC usando EC2-VPC para obter melhor performance e segurança.

Para atualizar o cluster do DS2 no EC2-Classic para EC2-VPC

1. Crie um snapshot do cluster DC2. Para obter mais informações, consulte Snapshots e backups do Amazon Redshift.
2. Crie uma VPC ou escolha uma VPC existente em sua conta. Para obter mais informações, consulte Gerenciamento de clusters em uma VPC.
3. Restaure o snapshot para um novo cluster DS2 no VPC. Para ter mais informações, consulte Restauração de um cluster usando um snapshot.

# Operações de cluster

Depois que o cluster é criado, há várias operações que poderão ser executadas nele. As operações incluem redimensionamento, pausa, retomada, renomeação e exclusão.

Tópicos


- Redimensionar clusters
- Pausar e retomar clusters
- Renomeação de clusters
- Desativação e exclusão de clusters
- Realocar um cluster
- Snapshots e backups do Amazon Redshift


## Redimensionar clusters

À medida que a sua capacidade e necessidades de desempenho do data warehousing mudam ou aumentam, é possível redimensionar seu cluster para fazer o melhor uso das opções de computação e armazenamento que o Amazon Redshift oferece.

Há dois tipos de operação de redimensionamento:

- Redimensionamento elástico - É possível adicionar ou remover nós do cluster. Também é possível alterar o tipo de nó, como de nós DS2 para nós RA3. Um redimensionamento elástico normalmente é concluído rapidamente, levando dez minutos, em média. Por esse motivo, é recomendável como primeira opção. Quando você executa um redimensionamento elástico, ele redistribui fatias de dados, que são partições que recebem memória e espaço em disco alocados em cada nó. O redimensionamento elástico é apropriado quando você:

  - Adiciona ou reduz nós em um cluster existente, mas não altera o tipo de nó - Isso é comumente chamado de redimensionamento no local. Quando você executa esse tipo de redimensionamento, algumas consultas em execução são concluídas com êxito, mas outras podem ser descartadas como parte da operação.
  - Alterar o tipo de nó de um cluster: quando você altera o tipo de nó, um snapshot é criado e os dados são redistribuídos do cluster de origem para um cluster composto pelo novo tipo de nó. Após a conclusão, as consultas em execução são descartadas. Como acontece com o redimensionamento no local, ele é realizado rapidamente.
- Redimensionamento clássico - É possível alterar o tipo de nó, o número de nós ou ambos, de maneira semelhante ao redimensionamento elástico. O redimensionamento clássico leva mais tempo para ser concluído, mas pode ser útil nos casos em que a alteração na contagem de nós ou no tipo de nó para o qual migrar não se enquadra nos limites do redimensionamento elástico. Isso pode se aplicar, por exemplo, quando a alteração na contagem de nós é muito grande.

Tópicos


- Elastic resize (Redimensionamento elástico)
- Classic resize (Redimensionamento clássico)


## Elastic resize (Redimensionamento elástico)

Uma operação de redimensionamento elástico, quando você adiciona ou remove nós do mesmo tipo, tem os seguintes estágios:

1. O redimensionamento elástico tira um snapshot do cluster. Esse snapshot sempre inclui tabelas sem backup para nós onde for aplicável. (Alguns tipos de nó, como RA3, não têm tabelas sem backup.) Se o cluster não tiver um snapshot recente porque você desabilitou os snapshots automatizados, a operação de backup pode levar mais tempo. Para minimizar o tempo antes do início da operação de redimensionamento, recomendamos que você habilite snapshots automatizados ou crie um snapshot manual antes de iniciar um redimensionamento elástico. Quando você inicia um redimensionamento elástico e uma operação de snapshot está em andamento, o redimensionamento elástico poderá falhar se a operação de snapshot não for concluída em alguns minutos. Para obter mais informações, consulte Snapshots e backups do Amazon Redshift.

2. A operação migra os metadados do cluster. O cluster fica indisponível por alguns minutos. A maioria das consultas é temporariamente pausada e as conexões são mantidas abertas. É possível, no entanto, que algumas consultas sejam descartadas. Esse estágio é curto.
3. As conexões de sessão são restabelecidas e as consultas são retomadas.
4. O redimensionamento elástico redistribui os dados para as fatias do nó no plano de fundo. O cluster está disponível para operações de leitura e gravação, mas algumas consultas podem levar mais tempo para serem executadas.
5. Após a conclusão da operação, o Amazon Redshift envia uma notificação de evento.

Quando você usa o redimensionamento elástico para alterar o tipo de nó, ele funciona de forma semelhante a quando você adiciona ou subtrai nós do mesmo tipo. Primeiro, um snapshot é criado. Um novo cluster de destino é provisionado com os dados mais recentes do snapshot e os dados são transferidos para o novo cluster em segundo plano. Durante esse período, os dados são somente leitura. Quando o redimensionamento está perto de ser concluído, o Amazon Redshift atualiza o endpoint do novo cluster e todas as conexões com o cluster de origem são descartadas.

É improvável que um redimensionamento elástico falhe. No entanto, no caso de falha, a reversão ocorre automaticamente na maioria dos casos, sem a necessidade de intervenção manual.

Se você tiver nós reservados, por exemplo nós reservados DS2, poderá atualizar para nós reservados RA3 quando realizar um redimensionamento. Você pode fazer isso ao executar um redimensionamento elástico ou ao usar o console para restaurar a partir de um snapshot. Este guia de console orientará você durante esse processo. Para obter mais informações sobre a atualização para nós RA3, consulte Atualizar para os tipos de nó RA3.

O redimensionamento elástico não classifica tabelas ou recupera espaço em disco; por isso, não é um substituto para uma operação de vacuum. Para obter mais informações, consulte Vacuum de tabelas.

O redimensionamento elástico tem as seguintes restrições:

- Redimensionamento elástico clusters de compartilhamento de dados: ao adicionar ou subtrair nós em um cluster que é um produtor para compartilhamento de dados, você não pode se conectar a ele por meio dos consumidores enquanto o Amazon Redshift estiver migrando metadados de cluster. Da mesma forma, se você executar um redimensionamento elástico e escolher um novo tipo de nó, o compartilhamento de dados ficará indisponível enquanto as conexões são descartadas e transferidas para o novo cluster de destino. Nos dois tipos de redimensionamento elástico, o produtor fica indisponível por vários minutos.

- Transferência de dados de um snapshot compartilhado: para executar um redimensionamento elástico em um cluster que está transferindo dados de um snapshot compartilhado, pelo menos um backup deve estar disponível para o cluster. Você pode visualizar seus backups na lista de snapshots do console do Amazon Redshift, no comando CLI `describe-cluster-snapshots` ou na operação da API `DescribeClusterSnapshots`.
- Restrição de plataforma: o redimensionamento elástico está disponível apenas para clusters que usam a plataforma EC2-VPC. Para obter mais informações, consulte Uso do EC2-VPC ao criar o cluster.
- Considerações de armazenamento - Certifique-se de que a configuração do novo nó tem armazenamento suficiente para os dados existentes. Talvez seja necessário adicionar nós ou alterar a configuração.
- Tamanho do cluster de origem versus cluster de destino: o número de nós e o tipo de nó para os quais é possível redimensionar com redimensionamento elástico são determinados pelo número de nós no cluster de origem e o tipo de nó escolhido para o cluster redimensionado. Para determinar as possíveis configurações disponíveis, você pode usar o console. Ou você pode usar o comando `describe-node-configuration-options` da AWS CLI com a opção `action-type resize-cluster`. Para obter mais informações sobre o redimensionamento usando o console do Amazon Redshift, consulte Redimensionamento de um cluster.

  O exemplo de comando CLI a seguir descreve as opções de configuração disponíveis. Neste exemplo, o cluster chamado `mycluster` é um cluster `dc2.large` de 8 nós.

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

  Este comando retorna uma lista de opções com os tipos de nós, o número de nós e a utilização do disco recomendados para cada opção. As configurações retornadas podem variar de acordo com o cluster de entrada específico. Você pode escolher uma das configurações retornadas ao especificar as opções do comando CLI `resize-cluster`.
- Teto nos nós adicionais - O redimensionamento elástico tem limites nos nós que é possível adicionar a um cluster. Por exemplo, um cluster dc2 oferece suporte ao redimensionamento elástico até o dobro do número de nós. Para ilustrar, é possível adicionar um nó a um cluster dc2.8xlarge de 4 nós para torná-lo um cluster de 5 nós ou adicionar mais nós até atingir 8.

> **Note**
>
> Os limites de crescimento e redução se baseiam no tipo de nó original e no número de nós do cluster original ou no redimensionamento clássico mais recente. Se um redimensionamento elástico exceder os limites de crescimento ou redução, use um redimensionamento clássico.

Com alguns tipos de nó ra3, você pode aumentar o número de nós até quatro vezes a contagem existente. Especificamente, suponha que seu cluster consiste em nós ra3.4xlarge ou ra3.16xlarge. Em seguida, você pode usar o redimensionamento elástico para aumentar o número de nós em um cluster de 8 nós para 32. Ou você pode escolher um valor abaixo do limite. (Lembre-se de que a capacidade de aumentar o cluster em 4x depende do tamanho do cluster de origem.) Se o cluster tiver nós ra3.xlplus, o limite é duplo.

Todos os tipos de nó ra3 suportam uma diminuição no número de nós para um quarto da contagem existente. Por exemplo, você pode diminuir o tamanho de um cluster com nós ra3.4xlarge de 12 nós para 3, ou para um número acima do mínimo.

A tabela a seguir lista os limites de crescimento e redução para cada tipo de nó que oferece suporte ao redimensionamento elástico.

| Tipos de nó originais | Limite de crescimento | Limite de redução |
|---|---|---|
| ra3.16xlarge | 4x (de 4 a 16 nós, por exemplo) | Para um quarto do número (por exemplo, de 16 a 4 nós) |
| ra3.4xlarge | 4x | Para um quarto do número |
| ra3.xlplus | 2x (de 4 a 8 nós, por exemplo) | Para um quarto do número |
| dc2.8xlarge | 2x | Para a metade do número (por exemplo, de 16 a 8 nós) |
| dc2.large | 2x | Para a metade do número |
| ds2.8xlarge | 2x | Para a metade do número |

| Tipos de nó originais | Limite de crescimento | Limite de redução |
| --- | --- | --- |
| ds2.xlarge | 2x | Para a metade do número |

> **Note**
>
> Escolher tipos de nós legados ao redimensionar um cluster RA3: se você tentar redimensionar de um cluster com nós RA3 para outro tipo de nó, como DC2 ou DS2, uma mensagem de aviso de validação será exibida no console e a operação de redimensionamento não será concluída. Isso ocorre porque o redimensionamento para tipos de nós legados não é compatível. Isso evita que um cliente redimensione para um tipo de nó que está obsoleto ou prestes a ser descontinuado. Isso se aplica tanto ao redimensionamento elástico quanto ao redimensionamento clássico.

## Classic resize (Redimensionamento clássico)

O redimensionamento clássico lida com casos de uso em que a alteração no tamanho do cluster ou no tipo de nó não é compatível com o redimensionamento elástico. Quando você executa um redimensionamento clássico, o Amazon Redshift cria um cluster de destino e migra seus dados e metadados do cluster de origem para ele.

O redimensionamento clássico para RA3 pode fornecer melhor disponibilidade

O redimensionamento clássico foi aprimorado quando o tipo de nó de destino é RA3. Isso é feito usando uma operação de backup e restauração entre o cluster de origem e de destino. Quando o redimensionamento começa, o cluster de origem é reiniciado e fica indisponível por alguns minutos. Depois disso, o cluster fica disponível para operações de leitura e gravação enquanto o redimensionamento continua em segundo plano.

Verificação do cluster

Para garantir que você tenha o melhor desempenho e os melhores resultados ao realizar um redimensionamento clássico para um cluster RA3, preencha esta lista de verificação. Se você não seguir a lista de verificação, talvez não obtenha alguns dos benefícios do redimensionamento clássico com nós RA3, como a capacidade de realizar operações de leitura e gravação.

1. O tamanho dos dados deve estar abaixo de 2 petabytes. (Um petabyte é igual a 1.000 terabytes.) Para validar o tamanho dos dados, crie um snapshot e verifique o tamanho dele. Você também pode executar a seguinte consulta para verificar o tamanho:

   ```
   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;
   ```

   A tabela `svv_table_info` é visível somente para superusuários.

2. Antes de iniciar um redimensionamento clássico, é necessário ter um snapshot manual que tenha, no máximo, 10 horas. Caso você não tenha, crie um snapshot.
3. O snapshot usado para realizar o redimensionamento clássico não pode ser usado para uma restauração de tabela ou outra finalidade.
4. O cluster deve estar em uma VPC.

Operações de classificação e distribuição que resultam do redimensionamento clássico para RA3

Durante o redimensionamento clássico para RA3, as tabelas com distribuição de chaves migradas como distribuição regular são reconvertidas no estilo de distribuição original. A duração disso depende do tamanho dos dados e da ocupação do cluster. As workloads de consulta têm maior prioridade para executar a migração de dados. Para obter mais informações, consulte Estilos de distribuição. As leituras e gravações no banco de dados funcionam durante esse processo de migração, embora possa levar mais tempo para que as consultas sejam concluídas. No entanto, a escalabilidade da simultaneidade pode aumentar o desempenho durante esse momento adicionando recursos para workloads de consulta. Você pode consultar o andamento da migração de dados visualizando resultados das visualizações SYS_RESTORE_STATE e SYS_RESTORE_LOG. Veja mais informações sobre o monitoramento a seguir.

Depois que o cluster é totalmente redimensionado, ocorre o seguinte comportamento de classificação:

- Se o redimensionamento resultar em mais fatias no cluster, as tabelas de distribuição KEY ficarão parcialmente desclassificadas, mas as tabelas EVEN permanecerão classificadas. Além disso, as informações sobre a quantidade de dados classificados podem não estar atualizadas, diretamente

após o redimensionamento. Após a recuperação da chave, a limpeza automática classifica a tabela ao longo do tempo.

- Se o redimensionamento resultar em menos fatias no cluster, as tabelas de distribuição KEY e EVEN ficarão parcialmente sem classificação. A limpeza automática classifica a tabela ao longo do tempo.

Para obter mais informações sobre a limpeza automática de tabelas, consulte Vacuum de tabelas. Para obter mais informações sobre fatias em nós de computação, consulte Arquitetura do sistema de data warehouse.

Etapas clássicas de redimensionamento quando o cluster de destino é RA3

O redimensionamento clássico consiste nas seguintes etapas, quando o tipo de cluster de destino é RA3 e você atende aos pré-requisitos detalhados na seção anterior.

1. A migração inicia do cluster de origem para o cluster de destino. Quando o cluster é provisionado, o Amazon Redshift envia uma notificação de evento de que o redimensionamento foi iniciado. Ele reinicia o cluster existente, que encerra todas as conexões. Se o cluster existente for um cluster produtor de unidade de compartilhamento de dados, as conexões com clusters de consumidores também serão fechadas. A reinicialização leva alguns minutos.

   Observe que qualquer relação de banco de dados, como uma tabela ou visão materializada, criada com `BACKUP NO` não é retida durante o redimensionamento clássico. Para obter mais informações, consulte CRIAR VISÃO MATERIALIZADA.
2. Após a reinicialização, o banco de dados fica disponível para leitura e gravação. Além disso, a unidade de compartilhamento de dados é retomada, o que leva mais alguns minutos.
3. Os dados são migrados para o cluster de destino. Quando o tipo de nó de destino é RA3, as leituras e gravações estão disponíveis durante a migração de dados.
4. Quando o processo de redimensionamento está quase concluído, o Amazon Redshift atualiza para o endpoint do cluster de destino e todas as conexões com o cluster de origem são descartadas. O cluster de destino se torna o produtor da unidade de compartilhamento de dados.
5. O redimensionamento é concluído. O Amazon Redshift envia uma notificação de evento.

Você pode ver o progresso do redimensionamento no console do Amazon Redshift. O tempo necessário para redimensionar um cluster depende da quantidade de dados.

> **Note**
>
> Escolher tipos de nós legados ao redimensionar um cluster RA3: se você tentar redimensionar de um cluster com nós RA3 para outro tipo de nó, como DC2 ou DS2, uma mensagem de aviso de validação será exibida no console e a operação de redimensionamento não será concluída. Isso ocorre porque o redimensionamento para tipos de nós legados não é compatível. Isso evita que um cliente redimensione para um tipo de nó que está obsoleto ou prestes a ser descontinuado. Isso se aplica tanto ao redimensionamento elástico quanto ao redimensionamento clássico.

Monitorar um redimensionamento clássico quando o cluster de destino é RA3

Para monitorar um redimensionamento clássico de um cluster provisionado em andamento, inclusive a distribuição de chaves, use SYS_RESTORE_STATE. Isso mostra a porcentagem concluída da tabela que está sendo convertida. Você deve ser um superusuário para acessar os dados.

Elimine as tabelas desnecessárias ao realizar um redimensionamento clássico. Quando você faz isso, as tabelas existentes podem ser distribuídas mais rapidamente.

Etapas clássicas de redimensionamento quando o cluster de destino não é RA3

O redimensionamento clássico consiste no seguinte, quando o tipo de nó de destino é diferente de RA3, como DS2, por exemplo.

1. A migração inicia do cluster de origem para o cluster de destino. Quando o cluster é provisionado, o Amazon Redshift envia uma notificação de evento de que o redimensionamento foi iniciado. Ele reinicia o cluster existente, que encerra todas as conexões. Se o cluster existente for um cluster produtor de unidade de compartilhamento de dados, as conexões com clusters de consumidores também serão fechadas. A reinicialização leva alguns minutos.

   Observe que qualquer relação de banco de dados, como uma tabela ou visão materializada, criada com `BACKUP NO` não é retida durante o redimensionamento clássico. Para obter mais informações, consulte CRIAR VISÃO MATERIALIZADA.
2. Após a reinicialização, o banco de dados fica disponível somente para leitura. A unidade de compartilhamento de dados é retomada, o que leva mais alguns minutos.
3. Os dados são migrados para o cluster de destino. O banco de dados permanece somente para leitura.

4. Quando o processo de redimensionamento está quase concluído, o Amazon Redshift atualiza para o endpoint do cluster de destino e todas as conexões com o cluster de origem são descartadas. O cluster de destino se torna o produtor da unidade de compartilhamento de dados.
5. O redimensionamento é concluído. O Amazon Redshift envia uma notificação de evento.

Você pode ver o progresso do redimensionamento no console do Amazon Redshift. O tempo necessário para redimensionar um cluster depende da quantidade de dados.

> **Note**
>
> Pode levar dias ou até semanas para redimensionar um cluster com uma grande quantidade de dados quando o cluster de destino não é RA3 ou não atende aos pré-requisitos de um cluster de destino RA3 detalhados na seção anterior.
> Observe também que a capacidade de armazenamento usada para o cluster pode aumentar após um redimensionamento clássico. Esse é o comportamento normal do sistema quando o cluster tem fatias de dados adicionais resultantes do redimensionamento clássico. Esse uso de capacidade adicional pode ocorrer mesmo quando o número de nós no cluster permanece o mesmo.

Redimensionamento elástico versus redimensionamento clássico

A tabela a seguir compara o comportamento entre os dois tipos de redimensionamento.

Redimensionamento elástico versus redimensionamento clássico

| Comportamento | Elastic resize (Redimensionamento elástico) | Classic resize (Redimensionamento clássico) | Comentos |
|---|---|---|---|
| Retenção de dados do sistema | O redimensionamento elástico retém os dados de log do sistema. | O redimensionamento clássico não retém tabelas e dados do sistema. | Se você habilitou o registro em log de |

| Comportamento | Elastic resize (Redimensionamento elástico) | Classic resize (Redimensionamento clássico) | Comentários |
|---|---|---|---|
| | | | auditoria em seu cluster de origem, poderá continuar a acessar os logs no Amazon S3 ou no CloudWatch após um redimensionamento. Você pode manter ou excluir esses conforme a especificação |

| Comportamento | Elastic resize (Redimensionamento elástico) | Classic resize (Redimensionamento clássico) | Comentários |
|---|---|---|---|
| | | | das políticas de dados. |

| Comportamento | Elastic resize (Redimensionamento elástico) | Classic resize (Redimensionamento clássico) | Comentários |
|---|---|---|---|
| Alteração nos tipos de nó | Redimensionamento elástico quando o tipo de nó não muda: o redimensionamento no local e a maioria das consultas são mantidos.<br><br>Redimensionamento elástico, com um novo tipo de nó selecionado: um novo cluster é criado. As consultas são descartadas à medida que o processo de redimensionamento é concluído. | Redimensionamento clássico: um novo cluster é criado. As consultas são descartadas durante o processo de redimensionamento. | |

| Comportamento | Elastic resize (Redimensionamento elástico) | Classic resize (Redimensionamento clássico) | Comentários |
|---|---|---|---|
| Retenção de sessão e consulta | O redimensionamento elástico retém sessões e consultas quando o tipo de nó é o mesmo no cluster de origem e de destino. Se você escolher um novo tipo de nó, as consultas serão descartadas. | O redimensionamento clássico não retém sessões e consultas. As consultas são descartadas. | Quando as consultas são descartadas, é possível esperar uma degradação no desempenho. É melhor realizar uma operação de redimensionamento durante um período de uso leve. |

| Comportamento | Elastic resize (Redimensionamento elástico) | Classic resize (Redimensionamento clássico) | Comentários |
|---|---|---|---|
| Cancelar operação de redimensionamento | Não é possível cancelar um redimensionamento elástico. | Você pode cancelar uma operação de redimensionamento clássico antes de ser concluída, escolhendo Cancelar redimensionamento nos detalhes do cluster no console do Amazon Redshift. | A quantidade de tempo necessária para cancelar um redimensionamento depende do estágio da operação de redimensionamento durante o cancelamento. Quando você fizer isso, cluster não estará disponíve |

| Comportamento | Elastic resize (Redimensionamento elástico) | Classic resize (Redimensionamento clássico) | Comentos |
|---|---|---|---|
| | | | l até que a operação de redimensionamento de cancelamento seja concluída. Se a operação de redimensionamento estiver no estágio final, não será possível cancelá-la.<br><br>Não é possível cancelar o redimensionamento |

| Comportamento | Elastic resize (Redimensionamento elástico) | Classic resize (Redimensionamento clássico) | Comentários |
|---|---|---|---|
| | | | clássico para um cluster RA3. |

Programar um redimensionamento

É possível programar operações de redimensionamento para aumentar a escala verticalmente do cluster a fim de antecipar o alto uso ou para reduzir a escala verticalmente do cluster a fim de economizar custos. O agendamento funciona tanto para redimensionamento elástico quanto para redimensionamento clássico. Agora é possível configurar uma programação no console do Amazon Redshift. Para obter mais informações, consulte Redimensionamento de um cluster, em Gerenciamento de clusters usando o console. Também é possível usar as operações da API do Amazon Redshift ou de AWS CLI para programar um redimensionamento. Para obter mais informações, consulte create-scheduled-action na Referência de comandos da AWS CLI ou CreateScheduledAction na Referência da API do Amazon Redshift.

Snapshot, restauração e redimensionamento

O redimensionamento elástico é o método mais rápido para redimensionar um cluster do Amazon Redshift. Se o redimensionamento elástico não for uma opção para você e precisar de acesso de gravação quase constante ao cluster, use as operações snapshot e redimensionamento clássico descritas na seção a seguir. Essa abordagem requer que todos os dados gravados no cluster de origem depois do snapshot ter sido feito devam ser copiados manualmente para o cluster de destino após a mudança. Dependendo do tempo que a cópia leva, você pode precisar repetir isso várias vezes até que tenha os mesmos dados em ambos os clusters. Depois, é possível fazer a mudança para o cluster de destino. Esse processo poderá ter um impacto negativo sobre consultas existentes até o conjunto de dados completo estar disponível no cluster de destino. No entanto, minimiza o tempo que você não pode gravar no banco de dados.

A abordagem de snapshot, restauração e redimensionamento clássico usa o seguinte processo:

1. Faça um snapshot do cluster existente. O cluster existente é o cluster de origem.
2. Observe a hora em que o snapshot foi tirado. Fazer isso significa que você pode identificar depois o ponto em que precisará reexecutar novamente os processos Extract, Transform, Load (ETL – Extração, transformação, carga) para carregar dados pós-snapshot no banco de dados de destino.
3. Restaure o snapshot em um novo cluster. Este novo cluster é o cluster de destino. Verifique se os dados de exemplo estão no cluster de destino.
4. Redimensione o cluster de destino. Selecione o novo tipo de nó, o número de nós e outras configurações do cluster de destino.
5. Revise as cargas dos processos ETL ocorridos depois que você tiver feito um snapshot do cluster de origem. Certifique-se de recarregar os mesmos dados na mesma ordem no cluster de destino. Se tiver cargas de dados em andamento, repita esse processo várias vezes até os dados serem iguais nos clusters de origem e de destino.
6. Pare todas as consultas em execução no cluster de origem. Para isso, reinicie o cluster ou faça login como um superusuário e use os comandos PG_CANCEL_BACKEND e PG_TERMINATE_BACKEND. Recarregar o cluster é a maneira mais fácil de verificar se o cluster está indisponível.
7. Renomeie o cluster de origem. Por exemplo, renomeie-o de `examplecluster` para `examplecluster-source`.
8. Renomeie o cluster de destino para usar o cluster de origem antes de renomeá-lo. Por exemplo, renomeie o cluster de destino do anterior para `examplecluster`. Deste ponto em diante, todos os aplicativos que usarem o endpoint contendo `examplecluster` se conectarão ao cluster de destino.
9. Exclua o cluster de origem depois de alternar para o cluster de destino e verifique se todos os processos funcionam conforme esperado.

Como alternativa, você pode renomear os clusters de origem e de destino antes de recarregar dados no cluster de destino. Essa abordagem funciona se você não exigir que todos os sistemas e relatórios dependentes sejam atualizados imediatamente com eles para o cluster de destino. Nesse caso, a etapa 6 será movida para o final do processo descrito anteriormente.

O processo rename somente será necessário se você quiser que os aplicativos continuem usando o mesmo endpoint para se conectar ao cluster. Se não precisar disso, você poderá atualizar todos os aplicativos que se conectarem ao cluster para usar o endpoint do cluster de destino sem renomear o cluster.

Existem alguns benefícios em reutilizar um nome de cluster. Primeiro, você não precisa atualizar strings de conexão do aplicativo porque o endpoint não muda, mesmo que o cluster subjacente mude. Em segundo lugar, itens relacionados, como alarmes do Amazon CloudWatch e notificações do Amazon Simple Notification Service (Amazon SNS) estão associados ao nome do cluster. Essa associação significa que você pode continuar usando os mesmos alarmes e notificações configurados para o cluster. Esse uso continuado é basicamente uma preocupação em ambientes de produção nos quais você deseja a flexibilidade para redimensionar o cluster sem reconfigurar itens relacionados, como alarmes e notificações.

## Pausar e retomar clusters

Se você tiver um cluster que só precisa estar disponível em horários específicos, poderá pausar o cluster e retomá-lo posteriormente. Enquanto o cluster estiver pausado, o faturamento sob demanda ficará suspenso. Somente o armazenamento do cluster gerará cobranças. Para obter informações sobre preço, consulte a página de preço do Amazon Redshift.

Quando você pausa um cluster, o Amazon Redshift cria um snapshot, começa a encerrar as consultas e coloca o cluster em um estado de pausa. Se você excluir um cluster pausado sem solicitar um snapshot final, não será possível restaurar o cluster. Não é possível cancelar ou reverter uma pausa ou retomar a operação após ser iniciada.

Você pode pausar e retomar um cluster usando o console do Amazon Redshift, a AWS CLI ou as operações da API do Amazon Redshift.

Você pode agendar ações para pausar e retomar um cluster. Ao usar o novo console do Amazon Redshift para criar uma programação recorrente para pausar e retomar, duas ações programadas são criadas para o intervalo de datas que você escolher. Os nomes das ações agendadas recebem os sufixos `-pause` e `-resume`. O comprimento total do nome deve caber no tamanho máximo de um nome de ação planejada.

Não é possível pausar os seguintes tipos de clusters:

- Clusters do EC2-Classic.
- Clusters que não estão ativos, por exemplo, um cluster que está sendo modificado atualmente.
- Clusters do Hardware security module (HSM – Módulo de segurança de hardware)
- Clusters com snapshots automatizados desativados.

Ao decidir pausar um cluster, considere o seguinte:

- Conexões ou consultas do cluster ficam indisponíveis.
- Você não pode ver as informações de monitoramento de consulta de um cluster pausado no console do Amazon Redshift.
- Não é possível modificar um cluster pausado. Nenhuma das ações agendadas no cluster será realizada. Isso inclui a criação de snapshots, o redimensionamento de clusters e as operações de manutenção do cluster.
- Métricas de hardware não são criadas. Atualize seus alarmes CloudWatch se você tiver alarmes definidos em métricas ausentes.
- Não é possível copiar os snapshots automatizados mais recentes de um cluster pausado para snapshots manuais.
- Enquanto um cluster estiver pausado, ele não poderá ser retomado enquanto a operação de pausa não for concluída.
- Ao pausar um cluster, o faturamento fica suspenso. No entanto, a operação de pausa normalmente é concluída em 15 minutos, dependendo do tamanho do cluster.
- Os logs de auditoria são arquivados e não são restaurados na retomada.
- Depois que um cluster é pausado, pode ser que não haja rastreamentos e logs disponíveis para solucionar problemas que ocorreram antes da pausa.
- As tabelas sem backup no cluster não são restauradas na retomada. Para obter mais informações sobre tabelas sem backup, consulte Excluir tabelas de snapshots.
- Se você estiver gerenciando as credenciais de administrador usando AWS Secrets Manager e pausar o cluster, o segredo do cluster não será excluído e você continuará recebendo a cobrança pelo segredo. Para obter mais informações sobre como gerenciar a senha de administrador do Redshift com o AWS Secrets Manager, consulte Gerenciamento das senhas de administrador do Amazon Redshift usando AWS Secrets Manager.

Ao retomar um cluster, considere o seguinte:

- A versão do cluster retomado é atualizada para a versão de manutenção com base na janela de manutenção do cluster.
- Se você excluir a sub-rede associada a um cluster pausado, poderá ter uma rede incompatível. Nesse caso, restaure o cluster do snapshot mais recente.
- Se você excluir um endereço IP elástico enquanto o cluster estiver pausado, um novo endereço IP elástico será solicitado.

- Se o Amazon Redshift não puder retomar o cluster com sua interface de rede elástica anterior, o Amazon Redshift tenta alocar uma nova.
- Ao retomar um cluster, os endereços IP do nó podem mudar. Pode ser necessário atualizar suas configurações de VPC para oferecer suporte a esses novos endereços IP para recursos como COPY from Secure Shell (SSH) ou COPY from Amazon EMR.
- Se você tentar retomar um cluster que não está pausado, a operação de retomada retornará um erro. Se a operação de retomada fizer parte de uma ação agendada, modifique ou exclua a ação agendada para evitar erros futuros.
- Dependendo do tamanho do cluster, pode demorar vários minutos para retomar o cluster antes que as consultas possam ser processadas. Além disso, a performance da consulta pode ser afetado durante um período, enquanto o cluster passa por reidratação após a conclusão da retomada.

## Renomeação de clusters

Você pode renomear um cluster se quiser que ele use um nome diferente. Como o endpoint para seu cluster inclui o nome do cluster (também referido como o identificador do cluster), o endpoint altera para usar o novo nome após a conclusão da renomeação. Por exemplo, se você tiver um cluster chamado `examplecluster` e renomeá-lo para `newcluster`, o endpoint altera para usar o identificador `newcluster`. Todos os aplicativos que se conectam ao cluster devem ser atualizados com o novo endpoint.

Você poderá renomear um cluster se quiser alterar o cluster aos quais suas aplicações se conectam sem ter que mudar o endpoint nessas aplicações. Nesse caso, você deve primeiro renomear o cluster original e, em seguida, alterar o segundo cluster a fim de reutilizar o nome do cluster original antes da renomeação. Fazer isso é necessário, pois o identificador do cluster deve ser exclusivo em sua conta e região, portanto o cluster original e segundo cluster não podem ter o mesmo nome. Você pode fazer isso se restaurar um cluster de um snapshot e não quiser alterar as propriedades de conexão de nenhum aplicativo dependente.

> **Note**
>
> Se você excluir o cluster original, será responsável pela exclusão de todos os snapshots de cluster indesejados.

Quando você renomeia um cluster, o status do cluster muda para `renaming` até que o processo seja concluído. O nome DNS antigo que era usado pelo cluster é excluído imediatamente, embora ele possa permanecer armazenado em cache por alguns minutos. O novo nome DNS do cluster renomeado entra em vigor dentro de, aproximadamente, 10 minutos. O cluster renomeado não fica disponível até que o novo nome entre em vigor. O cluster será reinicializado e todas as conexões existentes com cluster serão encerradas. Após a conclusão, o endpoint será alterado para usar o novo nome. Por este motivo, você deve interromper a execução de consultas antes de iniciar a renomeação e reiniciá-las após sua conclusão.

Snapshots do cluster são retidos e todos os snapshots associados a um cluster permanecem associados a esse cluster após a renomeação. Por exemplo, suponha que você tenha um cluster que atenda ao seu banco de dados de produção e tenha vários snapshots. Se você renomear o cluster e substituí-lo no ambiente de produção com um snapshot, o cluster que você renomeou ainda terá esses snapshots existentes associados a ele.

Os alarmes do Amazon CloudWatch e as notificações de evento do Amazon Simple Notification Service (Amazon SNS) estão associados ao nome do cluster. Se você renomear o cluster, precisará atualizá-los apropriadamente. Você pode atualizar os alarmes do CloudWatch no console do CloudWatch e atualizar as notificações de eventos do Amazon SNS no console do Amazon Redshift no painel de Eventos. Os dados de carregamento e consulta do cluster continuam a exibir dados de antes e depois da renomeação. Contudo, os dados de performance são reiniciados após a conclusão do processo de renomeação.

Para obter mais informações, consulte Modificar um cluster.

## Desativação e exclusão de clusters

Você pode desativar seu cluster se quiser impedir sua execução e a cobrança de taxas. Quando você desativa um cluster, você pode, opcionalmente, criar um snapshot final. Se você criar um snapshot final, o Amazon Redshift criará um snapshot manual do seu cluster antes de desligá-lo. Você poderá restaurar aquele snapshot se quiser retomar a execução do cluster e a consulta de dados.

Se você não precisa mais do seu cluster e de seus dados, pode desativá-lo sem criar um snapshot final. Nesse caso, o cluster e os dados são excluídos permanentemente. Para obter mais informações sobre a desativação e exclusão de clusters, consulte Excluir um cluster.

Mesmo que você desative seu cluster com um snapshot final manual, todos os snapshots automatizados associados ao cluster serão excluídos quando o cluster for desativado. Todos os

snapshots manuais associados ao cluster são retidos. Quaisquer snapshots manuais que são retidos, incluindo o snapshot final opcional, são cobrados na taxa de armazenamento do Amazon Simple Storage Service se você não tiver outros clusters em execução ao desligar o cluster, ou se você exceder o armazenamento gratuito disponível que é fornecido para o seu executando clusters do Amazon Redshift. Para obter mais informações sobre o custo de armazenamento de snapshots, consulte a página de preço do Amazon Redshift.

A exclusão de um cluster também exclui todos os segredos do AWS Secrets Manager associados.

## Realocar um cluster

Usando a realocação no Amazon Redshift, você permite que o Amazon Redshift mova um cluster para outra zona de disponibilidade (AZ) sem perda de dados ou alterações em suas aplicações. Com a realocação, você pode continuar as operações quando houver uma interrupção do serviço em seu cluster com impacto mínimo.

Quando a realocação de cluster está ativada, o Amazon Redshift pode optar por realocar clusters em algumas situações. Em particular, isso acontece quando os problemas na zona de disponibilidade atual impedem a operação ideal do cluster ou melhoram a disponibilidade do serviço. Você também pode chamar a função de realocação nos casos em que restrições de recursos em uma determinada zona de disponibilidade estão interrompendo as operações de cluster. Um exemplo é a capacidade de retomar ou redimensionar um cluster. O Amazon Redshift oferece o recurso de realocação sem custo adicional.

Quando um cluster do Amazon Redshift é realocado para uma nova zona de disponibilidade, o novo cluster tem o mesmo endpoint que o cluster original. Suas aplicações podem se reconectar ao endpoint e continuar as operações sem modificações ou perda de dados. No entanto, a realocação pode nem sempre ser possível devido a potenciais restrições de recursos em uma determinada zona de disponibilidade.

A realocação de cluster do Amazon Redshift é compatível apenas com os tipos de instância RA3, como ra3.16xlarge, ra3.4xlarge e ra3.xlplus. Os tipos de instância RA3 usam o Redshift Managed Storage (RMS) como uma camada de armazenamento durável. A cópia mais recente dos dados de um cluster está sempre disponível em outras zonas de disponibilidade em uma região da AWS. Em outras palavras, você pode realocar um cluster do Amazon Redshift para outra zona de disponibilidade sem perda de dados.

Quando você ativa a realocação para um cluster, o Amazon Redshift migra o cluster para que fique atrás de um proxy. Isso ajuda a implementar o acesso independente de localização aos recursos

de computação em cluster. A migração faz com que o cluster seja reinicializado. Quando um cluster é realocado para outra zona de disponibilidade, ocorre uma interrupção enquanto o novo cluster é colocado online novamente na nova zona de disponibilidade. No entanto, você não precisa fazer alterações em suas aplicações porque o endpoint do cluster permanece inalterado mesmo depois que o cluster é realocado para a nova zona de disponibilidade.

A realocação do cluster está desabilitada por padrão em todos os clusters RA3. O Amazon Redshift atribui 5439 como porta padrão ao criar um cluster provisionado. Você pode mudar para outra porta do intervalo de portas 5431–5455 ou 8191–8215. (Não mude para uma porta fora dos intervalos. Isso resulta em um erro.) Para alterar a porta padrão de um cluster provisionado, use o console do Amazon Redshift, a AWS CLI ou a API do Amazon Redshift. Para alterar a porta padrão de um grupo de trabalho sem servidor, use a AWS CLI ou a API do Amazon Redshift sem servidor.

Se você ativar a realocação e estiver usando o endereço IP do nó líder para acessar seu cluster, certifique-se de alterar esse acesso. Em vez disso, use o endereço IP associado ao endpoint da Virtual Private Cloud (VPC) do cluster. Para localizar esse endereço IP de cluster, localize e use o endpoint da VPC na seção Rede e segurança da página de detalhes do cluster. Para obter mais detalhes sobre o endpoint da VPC, faça login no console da Amazon VPC.

Você também pode usar o comando `describe-vpc-endpoints` da AWS Command Line Interface(AWS CLI) para obter a interface de rede elástica associada ao endpoint. Você pode usar o comando `describe-network-interfaces` para obter o endereço IP associado. Para obter mais informações sobre os comandos da AWS CLI do Amazon Redshift, consulte Comandos disponíveis na Referência de comandos da AWS CLI.

> **Note**
>
> Como lembrete, a realocação do cluster não é um pré-requisito para configurar recursos de rede do Redshift adicionais, como os usados na recuperação de desastres ou para outros fins. Por exemplo, você pode complementá-lo com a cópia do snapshot entre regiões para proporcionar mais resiliência ao ambiente, embora isso não seja obrigatório. Também não é necessário ativá-lo para habilitar os seguintes recursos:
>
> - Conexão de uma VPC entre contas ou regiões ao Redshift: você pode se conectar a partir de uma nuvem privada virtual (VPC) da AWS a outra que contenha um banco de dados do Redshift. Isso facilita o gerenciamento, por exemplo, do acesso do cliente a partir de contas ou VPCs diferentes, sem precisar dar acesso local à VPC para identidades conectadas ao banco de dados. Para obter mais informações, consulte Connecting to Amazon Redshift Serverless from a Redshift VPC endpoint in another account or region.

- Configuração de um nome de domínio personalizado: você pode criar um nome de domínio personalizado, também conhecido como URL personalizado, para o cluster do Amazon Redshift ou para o grupo de trabalho do Amazon Redshift Serverless, para deixar o nome do endpoint mais fácil de lembrar e simples. Para obter mais informações, consulte Usar nome de domínio personalizado para conexões de clientes.

## Limitações

Ao usar a realocação do Amazon Redshift, esteja ciente das seguintes limitações:

- A realocação de cluster pode não ser possível em todos os cenários devido a potenciais limitações de recursos em uma determinada zona de disponibilidade. Se isso acontecer, o Amazon Redshift não alterará o cluster original.
- A realocação não é compatível com as famílias de instâncias de produtos DC1, DC2 ou DS2.
- Você não pode realizar uma realocação entre regiões da AWS.
- O padrão de realocação do Amazon Redshift é a porta número 5439. Você também pode mudar para outra porta nos intervalos 5431-5455 ou 8191-8215.
- A realocação está disponível nas seguintes regiões:
  - Região Leste dos EUA (Ohio) (us-east-2)
  - Região Leste dos EUA (Norte da Virgínia) (us-east-1)
  - Região Oeste dos EUA (Norte da Califórnia) us-west-1
  - Região Oeste dos EUA (Oregon) us-west-2
  - Região da Ásia-Pacífico (Melbourne) (ap-southeast-4)
  - Região da Ásia-Pacífico (Mumbai) (ap-south-1)
  - Região da Ásia-Pacífico (Seul) (ap-northeast-2)
  - Região da Ásia-Pacífico (Singapura) (ap-southeast-1)
  - Região da Ásia-Pacífico (Sydney) (ap-southeast-2)
  - Região da Ásia-Pacífico (Tóquio) (ap-northeast-1)
  - Região do Canadá (Central) (ca-central-1)
  - Região Oeste do Canadá (Calgary) (ca-west-1)
  - Região da Europa (Frankfurt) (eu-central-1)
  - Região da Europa (Irlanda) (eu-west-1)

- Região da Europa (Londres) (eu-west-2)
- Região da Europa (Paris) (eu-west-3)
- Região da Europa (Estocolmo) (eu-north-1)
- Região de Israel (Tel Aviv) (il-central-1)
- Região da América do Sul (São Paulo) (sa-east-1)

## Ativar a realocação de clusters

Você pode ativar e gerenciar a realocação de clusters pelo console do Amazon Redshift, pela AWS CLI e pela API do Amazon Redshift.

Para ativar a realocação de clusters, defina um grupo de sub-redes que inclua várias zonas de disponibilidade. Se o Amazon Redshift identificar mais de uma zona de disponibilidade acessível, o Amazon Redshift escolherá automaticamente na lista de zonas de disponibilidade acessíveis para realocar o cluster.

Após a conclusão da realocação, você usa o mesmo endpoint para acessar o cluster. O Amazon Redshift exclui os recursos de computação do cluster original e os retorna ao grupo de recursos.

## Gerenciar a realocação usando o console

Você pode gerenciar as configurações de realocação de cluster usando o console do Amazon Redshift.

Ativar a realocação ao criar um cluster

Use o procedimento a seguir para ativar a realocação ao criar um cluster.

Como ativar a realocação para um novo cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters.
3. Escolha Create cluster (Criar cluster) para criar um novo cluster. Para obter mais informações sobre como criar um cluster, consulte Criar um cluster de exemplo do Amazon Redshift no Guia de conceitos básicos do Amazon Redshift.
4. Em Backup, na opção Cluster relocation (Realocação de cluster), escolha Enabled (Ativada). Por padrão, a realocação está desativada.

5. Selecione Create cluster (Criar cluster).

### Modificar a realocação de um cluster existente

Use o procedimento a seguir para alterar a configuração de realocação para um cluster existente.

Para modificar a configuração de realocação para um cluster existente

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters. Os clusters de sua conta na região atual da AWS são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha o nome do cluster que você deseja modificar na lista. A página de detalhes do cluster é exibida.
4. Escolha a guia Manutenção e, em seguida, na guia Detalhes de backup escolha Editar.
5. Em Backup, escolha Enabled (Ativado). Por padrão, a realocação está desativada.
6. Escolha Modify Cluster (Modificar cluster).

### Realocar um cluster

Use o procedimento a seguir para realocar um cluster para outra zona de disponibilidade. Isso é especialmente útil quando você deseja testar sua configuração de rede em zonas de disponibilidade secundárias ou quando você está executando restrições de recursos na zona de disponibilidade atual.

Para realocar um cluster para outra zona de disponibilidade

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters. Os clusters de sua conta na região atual da AWS são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha o nome do cluster que você deseja mover da lista. A página de detalhes do cluster é exibida.
4. Em Ações, escolha Realocar. A página Realocar cluster é exibida.
5. (Opcional) Escolha uma zona de disponibilidade. Se você não escolher uma zona de disponibilidade, o Amazon Redshift escolherá uma para você.

O Amazon Redshift inicia a realocação e exibe o cluster como realocando. Após a conclusão da realocação, o status do cluster muda para disponível.

## Gerenciar a realocação usando a CLI do Amazon Redshift

Você pode gerenciar as configurações para realocação de cluster usando a interface de linha de comando (CLI) da AWS

Com a AWS CLI, o comando de exemplo a seguir cria um cluster do Amazon Redshift chamado **`mycluster`** com a realocação ativada.

```
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
```

Se o cluster atual estiver usando uma porta diferente, você precisará modificá-lo para usar a porta 5431-5455 ou 8191-8215 antes de tentar ativar a realocação. O padrão é 5439. O comando de exemplo a seguir modifica a porta caso seu cluster não use uma do intervalo fornecido.

```
aws redshift modify-cluster --cluster-identifier mycluster --port 5439
```

O comando de exemplo a seguir inclui o parâmetro availability-zone-relocation no cluster do Amazon Redshift.

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

O comando de exemplo a seguir desativa o parâmetro availability-zone-realocation no cluster do Amazon Redshift.

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

O comando de exemplo a seguir invoca a realocação no cluster do Amazon Redshift.

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

# Snapshots e backups do Amazon Redshift

Tópicos


- Visão geral dos snapshots
- Snapshots automatizados
- Programações de snapshots automatizados
- Formato da programação de snapshot
- Snapshots manuais
- Gerenciar armazenamento de snapshots
- Excluir tabelas de snapshots
- Copiar snapshots para outra região da AWS
- Restauração de um cluster usando um snapshot
- Restaurar uma tabela de um snapshot
- Compartilhar snapshots
- Gerenciamento de snapshots usando o console
- Gerenciar snapshots usando a AWS CLI e a API do Amazon Redshift
- Trabalhar com AWS Backup


## Visão geral dos snapshots

Snapshots são backups pontuais de um cluster. Existem dois tipos de snapshots: automatizado e manual. O Amazon Redshift armazena esses snapshots internamente no Amazon S3 usando uma conexão Secure Sockets Layer (SSL) criptografada.

O Amazon Redshift tira automaticamente snapshots incrementais que rastreiam as alterações no cluster desde o snapshot automatizado anterior. Os snapshots automatizados retêm todos os dados necessários para restaurar um cluster a partir de um snapshot. Você pode criar uma programação de snapshot para controlar quando snapshots automatizados são tirados ou tirar um snapshot manual a qualquer momento.

Quando você restaura a partir de um snapshot, o Amazon Redshift cria um novo cluster e disponibiliza o novo cluster antes que todos os dados sejam carregados, para que você possa começar a consultar o novo cluster imediatamente. O cluster transmite dados sob demanda do snapshot em resposta a consultas ativas e carrega os dados restantes em segundo plano.

Ao iniciar um cluster, você pode definir o período de retenção para snapshots automatizados e manuais. Você pode alterar o período de retenção padrão para snapshots automatizados e manuais, modificando o cluster. É possível alterar o período de retenção do snapshot manual ao criar o snapshot ou modificando o snapshot.

Você pode monitorar o progresso de snapshots visualizando os detalhes do snapshot no AWS Management Console ou chamando describe-cluster-snapshots na CLI ou a ação de API DescribeClusterSnapshots. Para um snapshot em andamento, eles exibem informações como o tamanho do snapshot incremental, a taxa de transferência, o tempo decorrido e o tempo estimado restante.

Para garantir que seus backups estejam sempre disponíveis para o cluster, o Amazon Redshift armazena snapshots em um bucket do Amazon S3 do gerenciado internamente pelo Amazon Redshift. Para gerenciar cobranças de armazenamento, avalie de quantos dias você precisa para manter snapshots automatizados e configure o período de retenção de acordo. Exclua todos os snapshots manuais dos quais você não precisa mais. Para obter mais informações sobre o custo do armazenamento de backup, consulte a página de Preços do Amazon Redshift.

Trabalhar com snapshots e backups no Amazon Redshift sem servidor

O Amazon Redshift sem servidor, do mesmo modo que um cluster provisionado, permite que você faça um backup como uma representação pontual dos objetos e dos dados no namespace. Existem dois tipos de backup no Amazon Redshift sem servidor: snapshots criados manualmente e pontos de recuperação criados automaticamente pelo Amazon Redshift sem servidor. Você pode encontrar mais informações sobre como trabalhar com snapshots para o Amazon Redshift sem servidor em Trabalhar com snapshots e pontos de recuperação.

Também é possível restaurar um snapshot de um cluster provisionado para um namespace sem servidor. Para obter mais informações, consulte Restaurar um namespace com tecnologia sem servidor usando um snapshot.

## Snapshots automatizados

Quando snapshots automatizados são ativados para um cluster, o Amazon Redshift tira snapshots desse cluster periodicamente. Por padrão, o Amazon Redshift tira um snapshot a cada oito horas ou depois de cada 5 GB por nó de alterações de dados, o que ocorrer primeiro. Se o seu volume de dados for maior que 5 GB * número de nós, o menor tempo entre a criação automatizada de snapshots será de 15 minutos. Você também pode criar uma programação de snapshot para controlar quando snapshots automatizados são tirados. Se você estiver usando cronogramas

personalizados, o tempo mínimo entre os snapshots automatizados será de uma hora. Os snapshots automatizados são ativados por padrão quando você cria um cluster.

Os snapshots automatizados são excluídos ao final de um período de retenção. O período de retenção padrão é de um dia, mas você pode modificá-lo usando o console do Amazon Redshift ou programaticamente usando a API ou CLI do Amazon Redshift.

Para desativar snapshots automatizados, defina o período de retenção como zero. Se você desativar os snapshots automatizados, o Amazon Redshift para de tirar snapshots e exclui todos os snapshots automatizados existentes para o cluster. Não é possível desabilitar snapshots automatizados para tipos de nó RA3. Você pode definir um período de retenção automatizado do tipo de nó RA3 de 1 a 35 dias.

Somente o Amazon Redshift pode excluir um snapshot automatizado; você não pode excluí-lo manualmente. O Amazon Redshift exclui snapshots automatizados no final do período de retenção de um snapshot, quando você desativa os snapshots automatizados para o cluster ou quando exclui o cluster. O Amazon Redshift retém o snapshot automatizado mais recente até que você desabilite os snapshots automatizados ou exclua o cluster.

Se quiser manter um snapshot automatizado por um período mais longo, você poderá criar uma cópia dele como um snapshot manual. O snapshot automatizado será mantido até o final do período de retenção, mas o snapshot manual correspondente será retido até você excluí-lo manualmente ou até o final do período de retenção.

## Programações de snapshots automatizados

Para controlar com precisão quando snapshots são tirados, você pode criar uma programação de snapshot e anexá-la a um ou mais clusters. Quando você modifica uma programação de snapshot, a programação é modificada para todos os clusters associados. Se um cluster não tem uma programação de snapshot anexada, o cluster usa a programação padrão de snapshot automatizado.

Uma programação de snapshot é um conjunto de regras de programação. Você pode definir uma regra de programação simples com base em um intervalo especificado, como a cada 8 ou 12 horas. Você também pode adicionar regras para tirar snapshots em certos dias da semana, em horários específicos ou durante períodos específicos. As regras também podem ser definidas usando expressões cron semelhantes ao Unix

## Formato da programação de snapshot

No console do Amazon Redshift, você pode criar uma programação de snapshot. Você pode anexar uma programação a um cluster para acionar a criação de um snapshot do sistema. Uma programação pode ser associada a vários clusters, e você pode criar várias definições cron em uma programação para acionar um snapshot.

Você pode definir uma programação para seus snapshots usando uma sintaxe cron. A definição dessas programações usa uma sintaxe cron modificada do tipo Unix. Especifique o horário em Tempo Universal Coordenado (UTC). Você pode criar programações com frequência máxima de uma hora e precisão mínima de um minuto.

As expressões cron modificadas do Amazon Redshift têm 3 campos obrigatórios, separados por espaço em branco.

Sintaxe

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

| Campos | Valores | Curingas |
|---|---|---|
| Minutos | 0–59 | , - * / |
| Horas | 0–23 | , - * / |
| Dia do mês | 1–31 | , - * ? / L W |
| Mês | 1-12 ou JAN-DEZ | , - * / |
| Dia da semana | 1-7 ou SUN-SAT | , - * ? L # |
| Ano | 1970–2199 | , - * / |

Curingas

- A , (vírgula) curinga inclui valores adicionais. No campo `Day-of-week`, `MON,WED,FRI` incluirá segunda-feira, quarta-feira e sexta-feira. Os valores totais são limitados a 24 por campo.
- O - (traço) curinga especifica intervalos. No campo `Hour`, 1–15 incluiria as horas 1 a 15 do dia especificado.

- O * (asterisco) curinga inclui todos os valores no campo. No campo `Hours`, * incluirá cada hora.
- A / (barra) curinga especifica incrementos. No campo `Hours`, você pode inserir **`1/10`** para especificar a cada décima hora, a partir da primeira hora do dia (por exemplo, 01:00, 11:00 e 21:00).
- O curinga ? (interrogação) especifica um ou outro. No campo `Day-of-month`, você pode inserir 7 e, se não se importar com qual dia da semana era o sétimo, pode inserir ? no campo Dia da semana.
- O curinga L nos campos `Day-of-month` ou `Day-of-week` especifica o último dia do mês ou da semana.
- O curinga W no campo `Day-of-month` especifica um dia da semana. No campo `Day-of-month`, `3W` especifica o dia mais próximo do terceiro dia da semana do mês.
- O curinga # no campo Dia da semana especifica uma determinada instância do dia da semana definido dentro de um mês. Por exemplo, 3#2 seria a segunda terça-feira do mês: o 3 refere-se a terça-feira, porque é o terceiro dia de cada semana, e o 2 refere-se ao segundo dia desse tipo dentro do mês.

> **Note**
>
> Se você usar um caractere “#”, poderá definir apenas uma expressão no campo do dia da semana. Por exemplo, "3#1,6#3" não é válido porque é interpretado como duas expressões.

Limites

- Não é possível especificar os campos `Day-of-month` e `Day-of-week` na mesma expressão cron. Se você especificar um valor em um dos campos, deverá usar um ? (ponto de interrogação) no outro.
- Os cronogramas de snapshot não são compatíveis com as seguintes frequências:
  - Snapshots programados com frequência superior a 1 por hora.
  - Snapshots programados com frequência inferior a 1 por dia (24 horas).

  Se você tem programações sobrepostas que resultam na programação de snapshots em uma janela de 1 hora, o resultado é um erro de validação.

Ao criar uma programação, você pode usar os seguintes exemplos de strings cron.

| Minutos | Horas | Dia da semana | Significado | | | |
|---|---|---|---|---|---|---|
| 0 | 14-20/1 | TER | A cada hora entre 14h e 20h na terça-feira. | | | |
| 0 | 21 | SEG-SEX | Todas as noites, às 21h, de segunda a sexta-feira. | | | |
| 30 | 0/6 | SÁB-DOM | Incremento a cada 6 horas no sábado e domingo, a partir de 30 minutos após meia-noite (00:30) daquele dia. Isso resulta em um snapshot às [00:30, 06:30, 12:30 e 18:30] de cada dia. | | | |
| 30 | 12/4 | * | Incremento a cada 4 horas, a partir de 12:30 de cada dia. O resultado é [12:30, 16:30, 20:30]. | | | |

Por exemplo, para executar em uma programação de um incremento a cada 2 horas, a partir de 15:15 de cada dia. O resultado é [15:15, 17:15, 19:15, 21:15, 23:15] , especifique:

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

Você pode criar várias definições de programação cron em uma programação. Por exemplo, o seguinte comando da AWS CLI contém duas programações cron em uma programação.

```
create-snapshot-schedule --schedule-identifier "my-test" --schedule-definition "cron(0
 17 SAT,SUN)" "cron(0 9,17 MON-FRI)"
```

## Snapshots manuais

Você poderá obter um snapshot manual a qualquer momento. Por padrão, os snapshots manuais são retidos indefinidamente, mesmo depois que você exclui o cluster. Você pode especificar o período de retenção ao criar um snapshot manual ou pode alterar o período de retenção modificando o snapshot. Para obter mais informações sobre como alterar o período de retenção, consulte Alterar o período de retenção do snapshot manual.

Se um snapshot for excluído, você não poderá iniciar operações novas que referenciem esse snapshot. Porém, se estiver em andamento, uma operação de restauração será executada até a conclusão.

O Amazon Redshift tem uma cota que limita o número total de snapshots manuais que você pode criar; esta cota é por conta da AWS por região da AWS. A cota padrão está listada em Cotas e limites no Amazon Redshift.

## Gerenciar armazenamento de snapshots

Como os snapshots acumulam encargos de armazenamento, é importante que você os exclua quando não precisar mais deles. O Amazon Redshift exclui snapshots automatizados e manuais no final de seus respectivos períodos de retenção de snapshots. Você também pode excluir snapshots manuais usando o AWS Management Console ou com o comando da CLI batch-delete-cluster-snapshots.

É possível alterar o período de retenção do snapshot manual modificando as configurações do snapshot manual.

Você pode obter informações sobre quanto armazenamento seus snapshots estão consumindo usando o console do Amazon Redshift ou usando o comando da CLI describe-storage.

## Excluir tabelas de snapshots

Por padrão, todas as tabelas permanentes definidas pelo usuário são incluídas em snapshots. Se uma tabela, como uma tabela temporária, não precisar de backup, você poderá reduzir significativamente o tempo necessário para criar snapshots e restaurá-los. Você também reduz o espaço de armazenamento no Amazon S3 usando uma tabela sem backup. Para criar uma tabela

sem backup, inclua o parâmetro BACKUP NO ao criar a tabela. Para obter mais informações, consulte CREATE TABLE e CREATE TABLE AS no Guia do desenvolvedor de banco de dados do Amazon Redshift.

## Copiar snapshots para outra região da AWS

Você pode configurar o Amazon Redshift para copiar automaticamente os snapshots (automatizado ou manual) de um cluster para outra região da AWS. Quando um snapshot é criado na região da AWS primária do cluster, ele é copiado para uma região da AWS secundária. As duas regiões da AWS são conhecidas respectivamente como região da AWS de origem e região da AWS de destino. Se você armazenar uma cópia de seus snapshots em outra região da AWS, poderá restaurar seu cluster a partir de dados recentes se algo afetar a região da AWS primária. Você pode configurar seu cluster para copiar snapshots para apenas uma região da AWS de destino por vez. Para conferir a lista de regiões do Amazon Redshift, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

Ao habilitar o Amazon Redshift para copiar automaticamente os snapshots para outra região da AWS, você especifica a região da AWS de destino para onde copiar os snapshots. Para snapshots automatizados, você também pode especificar o período de retenção para mantê-los na região da AWS de destino. Depois que um snapshot automatizado é copiado para a região da AWS de destino e atinge o período de retenção lá, ele é excluído da região da AWS de destino. Ao fazer isso, você mantém o uso do snapshot baixo. Para manter os snapshots automatizados por um período mais curto ou mais longo na região da AWS de destino, altere este período de retenção.

O período de retenção que você define para snapshots automatizados que são copiados para a região da AWS de destino é separado do período de retenção para snapshots automatizados na região da AWS de origem. O período de retenção padrão para snapshots copiados é sete dias. Esse período de sete dias somente se aplica a snapshots automatizados. Nas regiões da AWS de origem e destino, os snapshots manuais são excluídos no final do período de retenção do snapshot ou quando você os exclui manualmente.

Você pode desativar a cópia automática do snapshot de um cluster a qualquer momento. Quando você desativa esse recurso, os snapshots não são mais copiados da região da AWS de origem para a região da AWS de destino. Todos os snapshots automatizados copiados para a região da AWS de destino são excluídos à medida que atingem o limite do período de retenção, a menos que você crie cópias de snapshot manuais deles. Esses snapshots manuais e quaisquer snapshots manuais que foram copiados da região da AWS de destino são mantidos na região da AWS de destino até que você os exclua manualmente.

Para alterar a região da AWS de destino para a qual você copia os snapshots , primeiro desative o recurso de cópia automática. Em seguida, reative-o, especificando a nova região da AWS de destino.

Depois que um snapshot é copiado para a região da AWS de destino, ele se torna ativo e disponível para fins de restauração.

Para copiar snapshots de clusters criptografados pelo AWS KMS para outra região da AWS, crie uma concessão para o Amazon Redshift para usar uma chave gerenciada pelo cliente na região da AWS de destino. Em seguida, escolha essa concessão ao habilitar a cópia de snapshots na região da AWS de origem. Para obter mais informações sobre como configurar concessões de cópia do snapshot, consulte Copiar snapshots criptografados pelo AWS KMS para outra região da AWS.

## Restauração de um cluster usando um snapshot

Um snapshot contém dados de todos os bancos de dados em execução no cluster. Ele também contém informações sobre seu cluster, inclusive o número de nós, tipo de nós e o nome de usuário administrador. Se você restaurar seu cluster a partir de um snapshot, o Amazon Redshift usa as informações do cluster para criar um novo cluster. Em seguida, ele restaura todos os bancos de dados dos dados do snapshot.

Para o novo cluster criado a partir do snapshot original, você pode escolher a configuração, como o tipo e o número de nós. O cluster é restaurado na mesma região da AWS e em uma zona de disponibilidade aleatória escolhida pelo sistema, a menos que você especifique outra zona de disponibilidade em sua solicitação. Ao restaurar um cluster a partir de um snapshot, você poderá escolher um acompanhamento de manutenção compatível para o novo cluster.

> **Note**
>
> Quando você restaura um snapshot para um cluster com outra configuração, o snapshot deve ser obtido em um cluster com a versão 1.0.10013 ou posterior.

Quando uma restauração está em andamento, os eventos geralmente são emitidos na seguinte ordem:

1. RESTORE_STARTED — REDSHIFT-EVENT-2008 enviado quando o processo de restauração começa.
2. RESTORE_SUCCEEDED — REDSHIFT-EVENT-3003 enviado quando o novo cluster foi criado.

   O cluster está disponível para consultas.

3. DATA_TRANSFER_COMPLETED — REDSHIFT-EVENT-3537 enviado quando a transferência de dados é concluída

> **Note**
>
> Os clusters RA3 emitem apenas os eventos RESTORE_STARTED e RESTORE_SUCCEEDED. Não há transferência de dados explícita a ser feita depois que um RESTORE for bem-sucedido porque os tipos de nó RA3 armazenam dados no armazenamento gerenciado do Amazon Redshift. Com os nós RA3, os dados são continuamente transferidos entre os nós RA3 e o armazenamento gerenciado do Amazon Redshift como parte do processamento normal de consultas. Os nós RA3 armazenam dados quentes localmente e mantêm blocos consultados com menos frequência no armazenamento gerenciado do Amazon Redshift automaticamente.

Você pode monitorar o andamento de uma restauração chamando a operação de API DescribeClusters ou exibindo os detalhes do cluster no AWS Management Console. Para uma restauração em andamento, eles exibem informações como o tamanho dos dados do snapshot, a taxa de transferência, o tempo decorrido e o tempo estimado restante. Para obter uma descrição dessas métricas, acesse RestoreStatus.

Você não pode usar um snapshot para restaurar o estado anterior de um cluster ativo.

> **Note**
>
> Quando você restaurar um snapshot em um novo cluster, o security group e o parameter group padrão serão usados, a menos que você especifique valores diferentes.

Talvez você queira restaurar um snapshot para um cluster com uma configuração diferente por estas razões:

- Quando um cluster é composto por tipos de nós menores e você deseja consolidá-lo em um tipo maior com menos nós.
- Quando você monitorou seu workload e determinou a necessidade de migrar para um tipo de nó com mais CPU e armazenamento.
- Quando você deseja medir a performance de workloads de teste com tipos de nós diferentes.

A restauração tem as seguintes restrições:

- A nova configuração de nó deve ter armazenamento suficiente para os dados existentes. Mesmo quando você adiciona nós, sua nova configuração pode não ter armazenamento suficiente por causa da maneira como os dados são redistribuídos.
- A operação de restauração verifica se o snapshot foi criado em uma versão de cluster compatível com a versão de cluster do novo cluster. Se o novo cluster tiver um nível de versão muito cedo, a operação de restauração falhará e reporta mais informações em uma mensagem de erro.
- As configurações possíveis (número de nós e tipo de nó) que você pode restaurar são determinadas pelo número de nós no cluster original e pelo tipo de nó de destino do novo cluster. Para determinar as possíveis configurações disponíveis, você pode usar o console do Amazon Redshift ou o comando da AWS CLI `describe-node-configuration-options` com `action-type restore-cluster`. Para obter mais informações sobre a restauração usando o console do Amazon Redshift, consulte Restauração de um cluster usando um snapshot.

As etapas a seguir consideram um cluster com muitos nós e o consolida em um tipo de nó maior com um número menor de nós usando a AWS CLI. Para este exemplo, começamos com um cluster de origem de 24 nós `ds2.xlarge`. Nesse caso, suponha que já tenhamos criado um snapshot desse cluster e deseje restaurá-lo para um tipo de nó maior.

1. Execute o seguinte comando para obter os detalhes de um cluster `ds2.xlarge` de 24 nós.

```
aws redshift describe-clusters --region eu-west-1 --cluster-identifier
 mycluster-123456789012
```

2. Execute o seguinte comando para obter os detalhes do snapshot.

```
aws redshift describe-cluster-snapshots --region eu-west-1 --snapshot-identifier
 mycluster-snapshot
```

3. Execute o seguinte comando para descrever as opções disponíveis para esse snapshot.

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

   Este comando retorna uma lista de opções com os tipos de nós, o número de nós e a utilização do disco recomendados para cada opção. Para este exemplo, o comando anterior lista as seguintes

configurações de nós possíveis. Optamos por fazer a restauração para um cluster `ds2.8xlarge` de três nós.

```
{
    "NodeConfigurationOptionList": [
        {
            "EstimatedDiskUtilizationPercent": 65.26134808858235,
            "NodeType": "ds2.xlarge",
            "NumberOfNodes": 24
        },
        {
            "EstimatedDiskUtilizationPercent": 32.630674044291176,
            "NodeType": "ds2.xlarge",
            "NumberOfNodes": 48
        },
        {
            "EstimatedDiskUtilizationPercent": 65.26134808858235,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 3
        },
        {
            "EstimatedDiskUtilizationPercent": 48.94601106643677,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 4
        },
        {
            "EstimatedDiskUtilizationPercent": 39.156808853149414,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 5
        },
        {
            "EstimatedDiskUtilizationPercent": 32.630674044291176,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 6
        }
    ]
}
```

4. Execute o comando a seguir para restaurar o snapshot para a configuração do cluster que escolhemos. Após a restauração desse cluster, temos o mesmo conteúdo que o cluster de origem, mas os dados foram consolidados em três nós `ds2.8xlarge`.

```
aws redshift restore-from-cluster-snapshot --region eu-west-1 --snapshot-identifier
 mycluster-snapshot --cluster-identifier mycluster-123456789012-x --node-type
 ds2.8xlarge --number-of-nodes 3
```

Se você tiver nós reservados, por exemplo nós reservados DS2 ou DC2, poderá atualizar para nós reservados RA3. Faça isso para restaurar a partir de um snapshot ou para executar um redimensionamento elástico. Você pode usar o console se orientar nesse processo. Para obter mais informações sobre a atualização para nós RA3, consulte Atualizar para os tipos de nó RA3.

## Restaurar uma tabela de um snapshot

Você pode restaurar uma única tabela de um snapshot, em vez de restaurar um cluster inteiro. Ao restaurar uma única tabela de um snapshot, você especifica o snapshot, o banco de dados, o esquema e o nome da tabela de origem, além do banco de dados e esquema de origem e do nome de uma nova tabela para a tabela restaurada.

O nome da nova tabela não pode ser o nome de uma tabela existente. Para substituir uma tabela existente por uma tabela restaurada de um snapshot, renomeie ou ignore a tabela existente antes de restaurar a tabela do snapshot.

A tabela de destino é criada usando-se as definições de coluna da tabela de origem, os atributos da tabela e os atributos da coluna, exceto as chaves externas. Para evitar conflitos por causa de dependências, a tabela de destino não herda chaves externas da tabela de origem. Todas as dependências, como visualizações ou permissões concedidas na tabela de origem, não são aplicadas à tabela de destino.

Se o proprietário da tabela de origem existir, esse usuário de banco de dados será o proprietário da tabela restaurada, desde que o usuário tenha permissões suficientes para se tornar o proprietário de uma relação no banco de dados e no esquema especificados. Do contrário, a tabela restaurada será de propriedade do usuário administrador que foi criado quando o cluster foi iniciado.

A tabela restaurada retorna ao estado em que estava no momento em que o backup foi feito. Isso inclui regras de visibilidade de transação definidas pela adesão do Amazon Redshift ao isolamento serializável, o que significa que os dados serão imediatamente visíveis para transações em andamento iniciadas após o backup.

Restaurar uma tabela de um snapshot tem as seguintes limitações:

- Você pode restaurar uma tabela somente no cluster atual, em execução ativa, e de um snapshot feito desse cluster.
- Você pode restaurar somente uma tabela por vez.
- Você não pode restaurar uma tabela de um snapshot de cluster feito antes de um cluster ser redimensionado. Uma exceção é que você pode restaurar uma tabela após um redimensionamento elástico se o tipo de nó não for alterado.
- Todas as dependências, como visualizações ou permissões concedidas na tabela de origem, não são aplicadas à tabela de destino.
- Se a segurança no nível da linha estiver ativada para uma tabela que está sendo restaurada, o Amazon Redshift restaurará a tabela com a segurança no nível da linha ativada.

Para restaurar uma tabela de um snapshot

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters e o cluster que você deseja usar para restaurar uma tabela.
3. Em Actions (Ações), escolha Restore table (Restaurar tabela) para exibir a página Restore table (Restaurar tabela).
4. Insira informações sobre qual snapshot, tabela de origem e tabela de destino usar e escolha Restore table (Restaurar tabela).

Example Exemplo: restaurar uma tabela de um snapshot usando a AWS CLI

O exemplo a seguir usa o comando `restore-table-from-cluster-snapshot` da AWS CLI para restaurar a tabela `my-source-table` do esquema `sample-database` no `my-snapshot-id`. Você pode usar o comando `describe-table-restore-status` da AWS CLI para revisar o status da operação de restauração. O exemplo restaura o snapshot para o cluster `mycluster-example` com o nome de uma nova tabela `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
```

## Compartilhar snapshots

Você pode compartilhar um snapshot manual existente com outras contas de clientes da AWS, autorizando o acesso ao snapshot. Você pode autorizar até 20 para cada snapshot e 100 para cada chave do AWS Key Management Service (AWS KMS). Ou seja, se você tiver 10 snapshots criptografados com uma única chave KMS, poderá autorizar 10 contas da AWS para restaurar cada snapshot ou outras combinações que adicionem até 100 contas e não excedam 20 contas para cada snapshot. Uma pessoa conectada como usuário em uma das contas autorizadas pode então descrever o snapshot ou restaurá-lo para criar um novo cluster do Amazon Redshift em sua conta. Por exemplo, se você usar contas de cliente da AWS separadas para produção e teste, um usuário poderá fazer login usando a conta de produção e compartilhar um snapshot com usuários na conta de teste. Alguém conectado como um usuário da conta de teste poderá restaurar o snapshot a fim de criar um novo cluster de propriedade da conta de teste para fins de teste ou trabalho de diagnóstico.

Um snapshot manual é propriedade permanente da conta de cliente da AWS em que foi criado. Somente usuários na conta proprietária do snapshot podem autorizar outras contas a acessar o snapshot ou revogar autorizações. Os usuários nas contas autorizadas somente podem descrever ou restaurar qualquer snapshot que tenha sido compartilhado com eles; eles não podem copiar nem excluir snapshots que tenham sido compartilhadas com eles. Uma autorização permanecerá em vigor até o proprietário do snapshot revogá-la. Se uma autorização for revogada, o usuário sido autorizado anteriormente perderá a visibilidade do snapshot e não poderá iniciar ações novas referenciando o snapshot. Se a conta estiver no processo de restauração do snapshot quando o acesso for revogado, a restauração será executada até ser concluída. Você não poderá excluir um snapshot enquanto ele tiver autorizações ativas; você deve revogar primeiramente todas as autorizações.

As contas de clientes da AWS estão sempre autorizadas para acessar snapshots de propriedade da conta. As tentativas de autorizar ou revogar acesso para a conta do proprietário receberão um erro. Você não pode restaurar nem descrever um snapshot de propriedade de uma conta do cliente da AWS inativa.

Depois que você tiver autorizado o acesso a uma conta do cliente da AWS, nenhum usuário nessa conta poderá realizar ações no snapshot, a menos que assuma um perfil com políticas que permitam isso.

- Os usuários na conta do proprietário do snapshot podem autorizar e revogar o acesso a um snapshot apenas se assumirem um perfil com uma política do IAM que permita a execução dessas ações com uma especificação de recurso que inclua o snapshot. Por exemplo, a política a seguir permite que um usuário na conta da AWS `012345678912` autorize outras contas a acessarem um snapshot chamado `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"
          ]
    }
  ]
}
```

- Os usuários em uma conta da AWS com a qual um snapshot foi compartilhado não podem realizar ações nesse snapshot, a menos que tenham permissões referentes a essas ações. É possível fazer isso atribuindo a política a um perfil e assumindo o perfil.
  - Para listar ou descrever um snapshot, eles devem ter uma políticas IAM que permita a ação `DescribeClusterSnapshots`. O seguinte código mostra um exemplo:

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

```
}
```

- Para restaurar um snapshot, um usuário deve assumir um perfil com uma política do IAM que permita a ação `RestoreFromClusterSnapshot` e tenha um elemento de recurso que abranja tanto o cluster que está tentando criar quanto o snapshot. Por exemplo, se um usuário na conta `012345678912` tiver um snapshot compartilhado `my-snapshot20130829` com a conta `219876543210`, para criar um cluster restaurando o snapshot, um usuário na conta `219876543210` deve assumir um perfil com uma política como a seguinte:

```
{
  "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"
          ]
    }
  ]
}
```

- Depois que o acesso a um snapshot tiver sido removido de uma conta da AWS, nenhum usuário nessa conta poderá acessar o snapshot. Isso ocorre mesmo que essas contas tenham políticas do IAM que permitam ações no recurso do snapshot compartilhado anteriormente.

## Gerenciamento de snapshots usando o console

O Amazon Redshift tira snapshots incrementais e automáticos de seus dados periodicamente e os salva no Amazon S3. Além disso, você pode capturar snapshots manuais de seus dados sempre que desejar. Nesta seção, você pode descobrir como gerenciar seus snapshots no console do Amazon Redshift. Para obter mais informações sobre snapshots, consulte Snapshots e backups do Amazon Redshift.

Todas as tarefas de snapshot no console do Amazon Redshift começam na lista de snapshots. Você pode filtrar a lista usando um intervalo de tempo, o tipo de snapshot e o cluster associado

ao snapshot. Além disso, você pode classificar a lista por data, tamanho e tipo de snapshot. Dependendo do tipo de snapshot selecionado, você pode ter diferentes opções disponíveis para trabalhar com o snapshot.

Tópicos


- Criar uma programação de snapshot
- Criação de um snapshot manual
- Alterar o período de retenção do snapshot manual
- Excluir snapshots manuais
- Copiar um snapshot automatizado
- Restauração de um cluster usando um snapshot
- Restaurar um namespace com tecnologia sem servidor usando um snapshot
- Compartilhamento de um snapshot de cluster
- Configuração de cópia de snapshots entre regiões para um cluster não criptografado
- Configurar a cópia de snapshot entre regiões para um cluster criptografado pelo AWS KMS
- Alteração do período de retenção para a cópia de snapshots entre regiões


## Criar uma programação de snapshot

Para controlar com precisão quando snapshots são tirados, você pode criar uma programação de snapshot e anexá-la a um ou mais clusters. Você pode anexar uma programação quando criar um cluster ou modificando o cluster. Para ter mais informações, consulte Programações de snapshots automatizados.

Para criar uma programação de snapshot

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, Snapshots e a guia Snapshot schedules (Programações de snapshots). As programações de snapshots são exibidas.
3. Escolha Add schedule (Adicionar programação) para exibir a página para adicionar uma programação.
4. Insira as propriedades da definição da programação e escolha Add schedule (Adicionar programação).

5. Na página exibida, você pode anexar clusters à sua nova programação de snapshots e escolher OK.

### Criação de um snapshot manual

Você pode criar um snapshot manual de um cluster a partir da lista de snapshots da forma a seguir. Ou então, você pode gerar um snapshot de um cluster no painel de configuração do cluster. Para ter mais informações, consulte Criar um snapshot de um cluster.

Para criar um snapshot manual

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, Snapshots e a guia Create snapshot (Criar snapshot). A página de snapshot para criação de um snapshot manual é exibida.
3. Insira as propriedades da definição do snapshot e escolha Create snapshot (Criar snapshot). Pode levar algum tempo para o snapshot estar disponível.

### Alterar o período de retenção do snapshot manual

É possível alterar o período de retenção do snapshot manual modificando as configurações do snapshot.

Para alterar o período de retenção do snapshot manual

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, Snapshots e o snapshot manual a ser alterado.
3. Em Actions (Ações), escolha Manual snapshot settings (Configurações de snapshot manual) para exibir as propriedades do snapshot manual.
4. Insira as propriedades revisadas da definição do snapshot e escolha Save (Salvar).

### Excluir snapshots manuais

Você pode excluir os snapshots manuais selecionando um ou mais snapshots na lista de snapshots.

Para excluir um snapshot manual

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, Snapshots e o snapshot a ser excluído.
3. Em Actions (Ações), escolha Delete snapshot (Excluir snapshot) para excluir o snapshot.
4. Confirme a exclusão dos snapshots listados e escolha Delete (Excluir).

## Copiar um snapshot automatizado

Snapshots automatizados são excluídos automaticamente quando seus períodos de retenção expiram, quando você desabilita snapshots automatizados ou quando você exclui um cluster. Se você deseja armazenar um snapshot automatizado, pode copiá-lo para um snapshot manual.

Para copiar um snapshot automatizado

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, Snapshots e o snapshot a ser copiado.
3. Em Actions (Ações), escolha Copy automated snapshot (Copiar snapshot automatizado) para copiar o snapshot.
4. Atualize as propriedades do novo snapshot e escolha Copy (Copiar).

## Restauração de um cluster usando um snapshot

Quando você restaura um cluster a partir de um snapshot, o Amazon Redshift cria um novo cluster com todos os dados do snapshot no novo cluster.

Para restaurar um cluster a partir de um snapshot

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, Snapshots e o snapshot a ser restaurado.
3. Escolha Restore from snapshot (Restaurar de snapshot) para visualizar a Cluster configuration (Configuração do cluster) e os valores de Cluster details (Detalhes do cluster) do novo cluster a ser criado usando as informações do snapshot.

4. Atualize as propriedades do novo cluster e escolha Restore cluster from snapshot (Restaurar cluster de snapshot).

Se o AWS Secrets Manager não estava gerenciando a senha de administrador do cluster, é possível fazer com que ele gerencie o cluster restaurado escolhendo Gerenciar credenciais de administrador no AWS Secrets Manager na seção Configuração do cluster e especificando uma chave KSM. Do contrário, o cluster será restaurado com as credenciais de administrador que ele tinha no momento em que o snapshot foi tirado. Você poderá atualizar as credenciais de administrador do cluster na página de detalhes do cluster depois de restaurá-lo.

Se o AWS Secrets Manager gerenciou a senha de administrador do cluster no momento em que a captura de tela foi feita, você deve continuar usando o AWS Secrets Manager para gerenciar a senha de administrador. Você poderá se recusar a usar um segredo depois de restaurar o cluster atualizando as credenciais de administrador do cluster na página de detalhes do cluster.

Se você tiver nós reservados, por exemplo nós reservados DS2 ou DC2, poderá atualizar para nós reservados RA3. Faça isso para restaurar a partir de um snapshot ou para executar um redimensionamento elástico. Você pode usar o console se orientar nesse processo. Para obter mais informações sobre a atualização para nós RA3, consulte Atualizar para os tipos de nó RA3.

Restaurar um namespace com tecnologia sem servidor usando um snapshot

A restauração de um namespace com tecnologia sem servidor de um snapshot substitui todos os bancos de dados do namespace por bancos de dados no snapshot. Para obter mais informações sobre snapshots e com tecnologia sem servidor, consulte Trabalhar com snapshots e pontos de recuperação. O Amazon Redshift converte automaticamente tabelas com chaves intercaladas em chaves compostas quando você restaura um snapshot de cluster provisionado para um namespace do Amazon Redshift sem servidor. Para obter mais informações sobre chaves de classificação, consulte Trabalhar com chaves de classificação.

Para restaurar um snapshot de cluster provisionado para um namespace de tecnologia sem servidor:

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, Snapshots e escolha o snapshot a ser copiado.
3. Selecione Restore from snapshot (Restaurar a partir do snapshot), Restore to serverless endpoint (Restaurar para endpoint com tecnologia sem servidor).
4. Escolha o namespace para o qual você deseja fazer a restauração.

5. Confirme que você deseja restaurar a partir do snapshot. Escolha restore (restaurar). Essa ação substitui todos os bancos de dados no namespace de tecnologia sem servidor pelos dados do cluster provisionado.

### Compartilhamento de um snapshot de cluster

Você pode autorizar outros usuários a acessar um snapshot manual que você possui e, mais tarde, revogar este acesso quando ele não for mais necessário.

#### Como compartilhar um snapshot com outra conta da

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, Snapshots e o snapshot manual a ser compartilhado.
3. Em Actions (Ações), escolha Manual snapshot settings (Configurações de snapshot manual) para exibir as propriedades do snapshot manual.
4. Insira a conta, ou contas, com a qual compartilhar na seção Manage access (Gerenciar o acesso) e escolha Save (Salvar).

#### Considerações de segurança para compartilhamento de snapshots criptografados

Quando você fornece acesso a um snapshot criptografado, o Redshift exige que a chave gerenciada pelo cliente do AWS KMS usada para criar o snapshot seja compartilhada com a conta ou as contas que estão realizando a restauração. Se a chave não for compartilhada, a tentativa de restaurar o snapshot resultará em um erro de acesso negado. A conta de recebimento não precisa de nenhuma permissão extra para restaurar um snapshot compartilhado. Quando você autoriza o acesso ao snapshot e compartilha a chave, a identidade que autoriza o acesso deve ter permissões `kms:DescribeKey` na chave usada para criptografar o snapshot. Essa permissão é descrita com mais detalhes em Permissões do AWS KMS. Para obter mais informações, consulte DescribeKey na documentação de referência de API do Amazon Redshift.

A política de chave gerenciada pelo cliente pode ser atualizada programaticamente ou no console do AWS Key Management Service.

#### Permitir acesso à chave do AWS KMS para um snapshot criptografado

Para compartilhar a chave gerenciada pelo cliente do AWS KMS para um snapshot criptografado, atualize a política de chaves realizando as seguintes etapas:

1. Você pode fazer uma atualização com o nome do recurso da Amazon (ARN) da conta da AWS com a qual você está compartilhando como `Principal` na política de chaves do KMS.
2. Permitir a ação `kms:Decrypt`.

No exemplo de política de chaves a seguir, o usuário `111122223333` é o proprietário da chave do KMS, e o usuário `444455556666` é a conta com a qual a chave é compartilhada. Essa política de chaves concede à conta da AWS acesso ao exemplo de chave do KMS incluindo o ARN da identidade da conta-raiz da AWS para o usuário `444455556666` como `Principal` da política e permitindo a ação `kms:Decrypt`.

```
{
    "Id": "key-policy-1",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/KeyUser",
                    "arn:aws:iam::444455556666:root"
                ]
            },
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Depois que o acesso é concedido à chave do KMS gerenciada pelo cliente, a conta que restaura o snapshot criptografado deve criar um usuário ou função do AWS Identity and Access Management (IAM), se ainda não tiver. Além disso, essa conta da AWS também deve anexar uma política do IAM a esse usuário ou função do IAM que permita que eles restaurem um snapshot do banco de dados criptografado usando a chave do KMS.

Para obter mais informações sobre como conceder acesso a uma chave do AWS KMS, consulte Permitir que usuários de outras contas usem uma chave do KMS, no Guia do desenvolvedor do AWS Key Management Service.

Para ter uma visão geral das principais políticas, consulte Como o Amazon Redshift usa o AWS KMS.

Configuração de cópia de snapshots entre regiões para um cluster não criptografado

Você pode configurar o Amazon Redshift para copiar snapshots de um cluster para outra região da AWS. Para configurar a cópia de snapshot entre regiões, você precisa habilitar este recurso de cópia para cada cluster e configurar onde copiar os snapshots e por quanto tempo manter os snapshots automatizados ou manuais copiados na região da AWS de destino. Quando a cópia entre regiões é habilitada para um cluster, todos os novos snapshots manuais e automatizados são copiados para a região da AWS especificada. Os nomes dos snapshots copiados são prefixados com **`copy:`**.

Como configurar um snapshot entre regiões

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, depois selecione o cluster para o qual você deseja mover snapshots.
3. Em Ações, escolha Configurar snapshots entre regiões.

   A caixa de diálogo “Configurar entre regiões” é exibida.
4. Em Copiar snapshots, escolha Sim.
5. Em Região da AWS de destino, escolha a região da AWS para a qual deseja copiar os snapshots.
6. Em Período de retenção de snapshot automatizado (dias), escolha o número de dias durante os quais deseja que os snapshots automatizados sejam retidos na região da AWS de destino antes de serem excluídos.
7. Em Período de retenção de snapshot manual, escolha o valor que representa o número de dias durante os quais você deseja que os snapshots manuais sejam retidos na região da AWS de destino antes de serem excluídos. Se escolher Valor personalizado, o período de retenção deve ser entre 1 e 3653 dias.
8. Escolha Salvar.

Configurar a cópia de snapshot entre regiões para um cluster criptografado pelo AWS KMS

Ao iniciar um cluster do Amazon Redshift, você pode optar por criptografá-lo com uma chave raiz do AWS Key Management Service (AWS KMS). As chaves AWS KMS são específicas para uma região

da AWS. Se você deseja habilitar a cópia de snapshot entre regiões para um cluster criptografado pelo AWS KMS, você deve configurar uma concessão de cópia de snapshot para uma chave raiz na região da AWS de destino. Ao fazer isso, você permite que o Amazon Redshift execute operações de criptografia na região da AWS de destino.

O procedimento a seguir descreve o processo de habilitação de cópia de snapshot entre regiões para um cluster criptografado pelo AWS KMS. Para obter mais informações sobre criptografia no Amazon Redshift e concessões de cópia de snapshot, consulte Copiar snapshots criptografados pelo AWS KMS para outra região da AWS.

Para configurar um snapshot entre regiões para um cluster criptografado pelo AWS KMS

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, depois selecione o cluster para o qual você deseja mover snapshots.
3. Em Ações, escolha Configurar snapshots entre regiões.

   A caixa de diálogo “Configurar entre regiões” é exibida.
4. Em Copiar snapshots, escolha Sim.
5. Em Região da AWS de destino, escolha a região da AWS para a qual deseja copiar os snapshots.
6. Em Período de retenção de snapshot automatizado (dias), escolha o número de dias durante os quais deseja que os snapshots automatizados sejam retidos na região da AWS de destino antes de serem excluídos.
7. Em Período de retenção de snapshot manual, escolha o valor que representa o número de dias durante os quais você deseja que os snapshots manuais sejam retidos na região da AWS de destino antes de serem excluídos. Se escolher Valor personalizado, o período de retenção deve ser entre 1 e 3653 dias.
8. Escolha Salvar.

Alteração do período de retenção para a cópia de snapshots entre regiões

Após configurar uma cópia de snapshot entre regiões, talvez você queira alterar as configurações. Você pode, facilmente, alterar o período de retenção selecionando um novo número de dias e salvando as alterações.

> **Warning**
>
> Não é possível modificar a região da AWS de destino após a configuração da cópia do snapshot entre regiões.
> Se você deseja copiar snapshots para uma região da AWS diferente, primeiro desative a cópia de snapshot entre regiões. Em seguida, reative-o com uma nova região de destino da AWS e período de retenção. Todos os snapshots automatizados são excluídos depois que você desabilita a cópia de snapshots entre regiões. Portanto, você deve determinar se há algum que você queira manter e copiá-los para snapshots manuais antes de desabilitar a cópia de snapshots entre regiões.

Como modificar um snapshot entre regiões

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters e o cluster para o qual você deseja modificar snapshots.
3. Em Actions (Ações), escolha Configure cross-region snapshot (Configurar snapshot entre regiões) para exibir as propriedades do snapshot.
4. Insira as propriedades revisadas da definição do snapshot e escolha Save (Salvar).

## Gerenciar snapshots usando a AWS CLI e a API do Amazon Redshift

Você pode usar as operações da CLI do Amazon Redshift a seguir para gerenciar snapshots.

- authorize-snapshot-access
- copy-cluster-snapshot
- create-cluster-snapshot
- delete-cluster-snapshot
- describe-cluster-snapshots
- disable-snapshot-copy
- enable-snapshot-copy
- modify-snapshot-copy-retention-period
- restore-from-cluster-snapshot

- revoke-snapshot-access

Você pode usar as ações da API do Amazon Redshift a seguir para gerenciar snapshots.

- AuthorizeSnapshotAccess
- CopyClusterSnapshot
- CreateClusterSnapshot
- DeleteClusterSnapshot
- DescribeClusterSnapshots
- DisableSnapshotCopy
- EnableSnapshotCopy
- ModifySnapshotCopyRetentionPeriod
- RestoreFromClusterSnapshot
- RevokeSnapshotAccess

Para obter mais informações sobre snapshots do Amazon Redshift, consulte Snapshots e backups do Amazon Redshift.

## Trabalhar com AWS Backup

AWS Backup é um serviço totalmente gerenciado que ajuda você a centralizar e automatizar a proteção de dados nos serviços da AWS, na nuvem e em ambientes on-premises.

Usando o AWS Backup para o Amazon Redshift, você pode configurar políticas de proteção de dados e monitorar a atividade para diferentes recursos do Amazon Redshift em um só lugar. Você também pode criar e armazenar snapshots em clusters provisionados do Amazon Redshift. Isso permite automatizar e consolidar as tarefas de backup que antes eram feitas separadamente, sem nenhum processo manual.

Um backup, ou ponto de recuperação, representa o conteúdo de um recurso, como um cluster do Amazon Redshift, em determinado momento. Um backup geralmente se refere aos diferentes backups em serviços da AWS, como snapshots do Amazon Redshift. O AWS Backup salva backups em cofres de backups, que você pode organizar de acordo com suas necessidades de negócios. Os termos ponto de recuperação e backup são usados de forma intercambiável. Para obter mais informações sobre o AWS Backup, consulte Trabalhar com backups.

O Amazon Redshift é integrado nativamente com o AWS Backup. Isso permite que você defina planos de backup e atribua recursos do Amazon Redshift aos planos de backup. O AWS Backup automatiza a criação de snapshots manuais do Amazon Redshift e os armazena com segurança em um cofre de backups criptografado designado por você no plano de backup. Para obter informações sobre os cofres, consulte Trabalhar com cofres de backups. No plano de backup, você pode definir a frequência do backup, a janela do backup, o ciclo de vida ou o cofre do backup. Para obter informações sobre planos de backup, consulte Gerenciar backups usando planos de backup.

Tópicos

- Considerações ao usar o AWS Backup com o Amazon Redshift
- Gerenciar o AWS Backup com o Amazon Redshift

## Considerações ao usar o AWS Backup com o Amazon Redshift

As seções a seguir descrevem as considerações e limitações para usar o AWS Backup com o Amazon Redshift.

### Considerações ao usar o AWS Backup com o Amazon Redshift

Veja a seguir considerações para usar o AWS Backup com o Amazon Redshift:

- O AWS Backup para Amazon Redshift está disponível quando tanto o AWS Backup como o Amazon Redshift estão disponíveis nas mesmas Regiões da AWS. Para obter informações sobre onde o AWS Backup está disponível, consulte Disponibilidade de recursos por Regiões da AWS.
- Para começar a usar o AWS Backup, verifique se você cumpre todos os pré-requisitos. Para obter mais informações, consulte Pré-requisitos.
- Aceite a adoção do serviço AWS Backup. As escolhas de adoção se aplicam à conta e Região da AWS específicas. Pode ser necessário optar pela adoção em várias regiões usando a mesma conta. Para obter mais informações, consulte Conceitos básicos 1: Adoção do serviço.
- No console do Amazon Redshift, você pode criar snapshots manuais e automatizados. O AWS Backup só oferece suporte a snapshots manuais no momento.
- Depois de usar o AWS Backup para gerenciar as configurações de snapshots, você não poderá continuar gerenciando as configurações de snapshots manuais usando o Amazon Redshift. Em vez disso, poderá continuar gerenciando as configurações usando um plano do AWS Backup. Para obter mais informações, consulte Gerenciar backups usando planos de backup.
- Para economizar custos de armazenamento ao fazer backup de buckets do Amazon S3 com versionamento, recomendamos que você defina uma regra de validade do ciclo de vida. Para obter

informações sobre como especificar uma regra de ciclo de vida, consulte o Exemplo 6: Especificar uma regra de ciclo de vida para um bucket com versionamento. Se você não definir um período de validade do ciclo de vida, os custos de armazenamento do Amazon Redshift poderão aumentar, pois o AWS Backup manterá todas as versões dos dados do Amazon Redshift.

### Limitações

Veja a seguir limitações para usar o AWS Backup no Amazon Redshift:

- Você não pode usar o AWS Backup para gerenciar snapshots automatizados do Amazon Redshift. Para gerenciar snapshots automatizados, use etiquetas. Para obter informações sobre a marcação de recursos, consulte Marcação de recursos no Amazon Redshift.
- O AWS Backup não oferece suporte ao Amazon Redshift Serverless.

### Gerenciar o AWS Backup com o Amazon Redshift

Para proteger os recursos em seus clusters provisionados do Amazon Redshift, você pode usar o console do AWS Backup ou usar programaticamente a API do AWS Backup ou a AWS Command Line Interface (AWS CLI). Quando você precisar recuperar um recurso, poderá usar o console do AWS Backup ou a AWS CLI para localizar e recuperar o recurso necessário. Para obter mais informações, consulte AWS Command Line Interface.

Ao usar o AWS Backup para o Amazon Redshift, você pode executar as seguintes ações:

- Criar backups periódicos que iniciam automaticamente os snapshots do Amazon Redshift. Os backups periódicos são úteis para atender às suas necessidades de retenção de dados a longo prazo. Para obter mais informações, consulte Backups do Amazon Redshift.
- Automatizar o agendamento e a retenção de backups configurando planos de backup de modo centralizado.
- Restaurar um cluster para o backup salvo de sua escolha. Você define com que frequência quer fazer backup de seus recursos. Para obter mais informações, consulte Restaurar um cluster do Amazon Redshift.

## Configuração da implantação multi-AZ

O Amazon Redshift é compatível com várias implantações (Multi-AZ) das zonas de disponibilidade de clusters RA3 provisionados. Ao usar implantações multi-AZ, o data warehouse do Amazon

Redshift pode continuar operando em cenários de falha nos quais um evento inesperado acontece em uma zona de disponibilidade. Uma implantação multi-AZ implanta recursos computacionais em duas zonas de disponibilidade (AZs) e esses recursos computacionais podem ser acessados por meio de um único endpoint. Em caso de falha de uma zona de disponibilidade inteira, os recursos computacionais restantes na segunda zona de disponibilidade permanecem disponíveis para continuar processando workloads. O Amazon Redshift cobra as mesmas taxas de computação por hora para RA3 ao executar um data warehouse multi-AZ. Os custos de armazenamento permanecem os mesmos, pois são compartilhados em todas as zonas de disponibilidade e na Região da AWS.

Atualmente, o Amazon Redshift é compatível com o objetivo de ponto de recuperação (RPO) zero, o que permite que os dados sejam atualizados em caso de falha. Com a implantação multi-AZ, o Amazon Redshift aprimora ainda mais os recursos de recuperação existentes e reduz o objetivo de tempo de recuperação (RTO). Isso é possível porque uma implantação multi-AZ consegue se recuperar mais rapidamente de uma falha ou de um desastre, elevando o Acordo de Serviço (SLA) do Amazon Redshift para 99,99%, em comparação com 99,9% com um data warehouse Single-AZ.

## Configuração de uma implantação multi-AZ

Para configurar uma implantação multi-AZ, selecione a opção Multi-AZ e especifique o número de nós de computação a serem provisionados em cada zona de disponibilidade. O Amazon Redshift implanta automaticamente recursos computacionais iguais em duas zonas de disponibilidade e todos os recursos computacionais estão sempre disponíveis para processamento de leitura e gravação durante a operação normal. Isso permite que uma implantação multi-AZ atue como um único data warehouse com um único endpoint, eliminando a necessidade de alterações na aplicação quando ocorre um desastre. Embora uma implantação Multi-AZ processe uma consulta individual usando os recursos computacionais residentes em apenas uma zona de disponibilidade, ela pode distribuir automaticamente o processamento de várias consultas simultâneas para ambas as zonas de disponibilidade a fim de aumentar o throughput geral para workloads de alta simultaneidade.

Você também pode converter um data warehouse single-AZ existente em um data warehouse multi-AZ, ou vice-versa. Tudo permanece o mesmo, exceto por recursos computacionais adicionais serem provisionados na segunda zona de disponibilidade. Ao migrar para multi-AZ de um cluster single-AZ existente, talvez você precise dobrar o número de nós de cluster necessários para facilitar a manutenção do desempenho de uma única consulta. A maioria das workloads observa um aumento no throughput do processamento de consultas com um data warehouse multi-AZ, pois há o dobro da quantidade de recursos computacionais disponíveis.

Em caso de falha em uma zona de disponibilidade, o Amazon Redshift continuará operando usando automaticamente os recursos na zona de disponibilidade restante. No entanto, as conexões do usuário poderão ser perdidas e deverão ser restabelecidas. Além disso, as consultas que estavam sendo executadas na zona de disponibilidade podem falhar e precisam ser repetidas. No entanto, você pode se reconectar ao cluster e reprogramar consultas imediatamente, e o Amazon Redshift vai processar as consultas na zona de disponibilidade restante. As consultas emitidas durante ou após a ocorrência de uma falha poderão sofrer atrasos no tempo de execução enquanto o data warehouse multi-AZ estiver se recuperando.

> **Note**
>
> Para obter melhor desempenho e mais disponibilidade, é recomendável usar SNAPSHOT ISOLATION com os clusters multi-AZ. Para obter mais informações, consulte CREATE DATABASE.

## Limitações

Um data warehouse multi-AZ tem os mesmos recursos funcionais de um data warehouse single-AZ, exceto pelas seguintes limitações que se aplicam a um data warehouse multi-AZ:

- Você não pode criar um data warehouse multi-AZ não criptografado. Não se esqueça de adicionar uma criptografia ao criar um novo data warehouse multi-AZ, converter um data warehouse single-AZ em um data warehouse multi-AZ ou converter um data warehouse single-AZ em um data warehouse multi-AZ.
- Não é possível criar uma implantação multi-AZ de nó único para nenhum dos tipos de instância RA3. Escolha dois ou mais nós por zona de disponibilidade ao criar uma implantação multi-AZ.
- As integrações ETL zero não são compatíveis em data warehouses de destino configurados para implantação multi-AZ.
- O Amazon Redshift não dá suporte a uma configuração de sub-rede compatível com menos de três zonas de disponibilidade. Em outras palavras, o grupo de sub-redes configurado exige mais três sub-redes.
- Não é possível realocar uma implantação multi-AZ para outra zona de disponibilidade. A realocação será determinada e realizada automaticamente pelo Amazon Redshift ao usar a implantação multi-AZ.
- Você não pode pausar nem retomar uma implantação multi-AZ.

- Você não pode executar a implantação multi-AZ fora dos intervalos de portas compatíveis de 5431 a 5455 e de 8191 a 8215.
- Você não pode usar visualizações STL, SVCS, SVL, SVV, STV com implantações multi-AZ, pois elas só dão suporte a visualizações de monitoramento do sistema (visualizações SYS_*). Altere as consultas de monitoramento para usar visualizações de monitoramento do sistema (visualizações SYS_*).
- Não é possível anexar um endereço IP elástico a um cluster existente com o Multi-AZ habilitado.
- Não é possível converter um cluster com um endereço IP elástico anexado de Single-AZ em Multi-AZ.
- A implantação multi-AZ do Amazon Redshift está disponível nas seguintes Regiões da AWS:
  - Leste dos EUA (Ohio) (us-east-2)
  - Leste dos EUA (Norte da Virgínia) (us-east-1)
  - Oeste dos EUA (Oregon) (us-west-2)
  - África (Cidade do Cabo) (af-south-1)
  - Ásia-Pacífico (Hong Kong) (ap-east-1)
  - Ásia-Pacífico (Hyderabad) (ap-south-2)
  - Ásia-Pacífico (Jacarta) (ap-southeast-3)
  - Ásia-Pacífico (Melbourne) (ap-southeast-4)
  - Ásia-Pacífico (Mumbai) (ap-south-1)
  - Ásia-Pacífico (Osaka) (ap-northeast-3)
  - Ásia-Pacífico (Seul) (ap-northeast-2)
  - Ásia-Pacífico (Singapura) (ap-southeast-1)
  - Ásia-Pacífico (Sydney) (ap-southeast-2)
  - Ásia Pacific (Tóquio) (ap-northeast-1)
  - Canadá (Central) (ca-central-1)
  - Europa (Frankfurt) (eu-central-1)
  - Europa (Irlanda) (eu-west-1)
  - UE (Milão) (eu-south-1)
  - Europa (Paris) (eu-west-3)
  - Europa (Espanha) (eu-south-2)
  - UE (Estocolmo) (eu-north-1)

- Europa (Zurique) (eu-central-2)
- Israel (Tel Aviv) (il-central-1)
- Oriente Médio (Bahrein) (me-south-1)
- Oriente Médio (EAU) (me-central-1)

Tópicos


- Gerenciar a implantação multi-AZ
- Failover da implantação multi-AZ
- Monitoramento de consultas para multi-AZ


## Gerenciar a implantação multi-AZ

O multi-AZ do Amazon Redshift oferece suporte a duas zonas de disponibilidade ao mesmo tempo. O Amazon Redshift seleciona automaticamente as zonas de disponibilidade com base na configuração do grupo de sub-redes selecionado. Você pode converter um data warehouse de zona de disponibilidade única existente em uma implantação multi-AZ ou restaurar um snapshot para configurá-la como um data warehouse multi-AZ.

Usando o console do Amazon Redshift, você pode criar implantações multi-AZ facilmente. Para criar uma implantação multi-AZ usando o console do Amazon Redshift, selecione a opção Multi-AZ ao criar o data warehouse. Especifique o número de nós de computação necessários em uma única zona de disponibilidade, e o Amazon Redshift implantará o número de nós em cada uma das duas zonas de disponibilidade. Todos os nós serão usados no processamento dos workloads de leitura e gravação durante uma operação normal. Você também pode usar o comando `create-cluster` da AWS CLI para criar um novo data warehouse multi-AZ usando o parâmetro `multi-az`.

Você pode converter um data warehouse single-AZ existente em um data warehouse multi-AZ. Você pode usar o console do Amazon Redshift ou o comando `modify-cluster` da AWS CLI usando o parâmetro `multi-az`. Ou você pode restaurar de um snapshot para configurar um data warehouse single-AZ em um data warehouse multi-AZ usando o console do Amazon Redshift ou o comando `restore-from-cluster-snapshot` da AWS CLI usando o parâmetro `multi-az`.

A implantação multi-AZ oferece suporte somente aos tipos de nó RA3 que usam o Amazon Redshift Managed Storage (RMS). O Amazon Redshift armazena dados no RMS, que usa o Amazon S3 e pode ser acessado em todas as zonas de disponibilidade em uma Região da AWS, sem precisar replicar os dados no Amazon Redshift.

## Configurar multi-AZ ao criar um cluster

Você pode configurar a implantação multi-AZ ao criar um cluster usando o console do Amazon Redshift ou a AWS Command Line Interface.

Usar o console

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, Provisioned clusters dashboard (Painel de clusters provisionados) e Clusters. Os clusters de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha o botão Criar cluster para abrir a página do cluster.
4. Insira as propriedades do cluster. Para obter informações gerais sobre como criar clusters, consulte Criar um cluster.
5. Escolha um dos tipos de nó RA3 na lista suspensa Node type (Tipo de nó). A opção de configuração AZ só permanece disponível quando você escolhe um tipo de nó RA3.
6. Em Configuração AZ, escolha Multi-AZ.
7. Em Número de nós por AZ, insira pelo menos dois nós para o cluster.
8. Você tem a opção de carregar dados de amostra ou adicionar dados próprios:
   - Em Sample data (Dados de exemplo), escolha Load sample data (Carregar dados de exemplo) para carregar o conjunto de dados de exemplo em seu cluster do Amazon Redshift. O Amazon Redshift carrega o Tickit do conjunto de dados de exemplo para o banco de dados dev padrão e o esquema public. O Amazon Redshift carrega automaticamente o conjunto de dados de exemplo no cluster do Amazon Redshift. Você pode começar usando o editor de consulta v2 para consultar dados.
   - Para adicionar dados próprios ao cluster do Amazon Redshift, siga as etapas em Trazer seus próprios dados para o Amazon Redshift.
9. Role para baixo até Additional configurations (Configurações adicionais), expanda Network and security (Rede e segurança) e aceite o Cluster subnet group (Grupo de sub-redes do cluster) padrão ou escolha outro. Se você escolher outro grupo de sub-redes do cluster, verifique se existem três zonas de disponibilidade no grupo de sub-redes selecionado.
10. Em Additional configurations (Configurações adicionais), expanda Database configurations (Configurações do banco de dados).

11. Para usar uma chave AWS KMS personalizada, e não a chave AWS Key Management Service padrão, clique em Personalizar as configurações de criptografia em Criptografia do banco de dados.
12. Em Choose an KMS key (Escolher uma chave do KMS), selecione uma chave do AWS Key Management Service ou insira um ARN. Ou clique em Criar uma chave do AWS Key Management Service no console do AWS Key Management Service. Para obter mais informações sobre como criar chaves KMS, consulte Criar chaves no Guia do desenvolvedor do AWS Key Management Service.
13. Clique em Create cluster. Quando a criação do cluster for bem-sucedida, você poderá visualizar os detalhes na página de detalhes do cluster. Você pode usar seu cliente SQL para carregar e consultar dados.

Usando a AWS Command Line Interface

Para configurar multi-AZ ao criar um cluster usando a AWS Command Line Interface

- Na AWS CLI, use o comando `create-cluster` e o parâmetro `multi-az` da maneira a seguir.

```
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
```

## Conversão de um data warehouse single-AZ em um data warehouse multi-AZ

Durante a conversão de um data warehouse single-AZ em um data warehouse multi-AZ, o data warehouse permanecerá altamente disponível com uma garantia SLA de 99,99%. O desempenho de uma consulta individual continuará o mesmo com um data warehouse multi-AZ. Para workloads

de mais simultaneidade, você verá um aumento no throughput geral, pois o Amazon Redshift pode executar solicitações usando recursos computacionais em duas zonas de disponibilidade.

> **Note**
>
> O Amazon Redshift não permitirá a você dividir recursos computacionais existentes durante a conversão de single-AZ em multi-AZ, ou vice-versa. Essa operação não é compatível para manter um desempenho consistente de consultas individuais.

Usar o console

Para converter um cluster single-AZ em um data warehouse multi-AZ usando o console

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, Provisioned clusters dashboard (Painel de clusters provisionados) e Clusters. Os clusters de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha o cluster que você deseja converter em uma implantação multi-AZ. A página de detalhes do cluster é exibida.
4. Em Ações, escolha Ativar Multi-AZ. O resumo da modificação é exibida. Clique em Ativar Multi-AZ.
5. Quando houver um erro, faça o seguinte e clique em Ativar Multi-AZ.
   - Criptografia do cluster: escolha Propriedades para editar as configurações de criptografia na seção Configuração do banco de dados, na guia Propriedades da página de detalhes do cluster.
   - Grupo de sub-redes: escolha Grupo de sub-redes para editar as configurações do grupo de sub-redes do cluster clicando no link do grupo de sub-redes. Se você escolher outro grupo de sub-redes do cluster, verifique se existem três zonas de disponibilidade no grupo de sub-redes selecionado.
   - Configurações da porta: escolha Propriedades para editar a configuração da porta na seção Configuração do banco de dados, na guia Propriedades da página de detalhes do cluster.
6. Você pode usar seu cliente SQL para carregar e consultar dados.

Usando a AWS Command Line Interface

- Na AWS CLI, use o comando `modify-cluster` e o parâmetro `multi-az` da maneira a seguir.

```
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
```

## Conversão de um data warehouse multi-AZ em um data warehouse single-AZ

Durante a conversão de um data warehouse multi-AZ em um data warehouse single-AZ, o data warehouse não vai obter a garantia SLA de 99,99% oferecida pelo multi-AZ. O desempenho de uma consulta individual permanecerá o mesmo, mas o throughput geral será afetado porque os recursos computacionais na segunda zona de disponibilidade não estarão disponíveis. Você tem a opção de habilitar a escalabilidade simultânea para escalar automaticamente o throughput tendo em vista um desempenho consistente, mesmo com o single-AZ.

> **Note**
>
> O Amazon Redshift não permitirá a você dividir recursos computacionais existentes durante a conversão de single-AZ em multi-AZ, ou vice-versa. Essa operação não é compatível para manter um desempenho consistente de consultas individuais.

Usar o console

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, Provisioned clusters dashboard (Painel de clusters provisionados) e Clusters. Os clusters de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha o cluster que você deseja converter em uma implantação multi-AZ. A página de detalhes do cluster é exibida.
4. Em Ações, escolha Desativar Multi-AZ. O resumo da modificação é exibida. Clique em Desativar Multi-AZ.

Usando a AWS Command Line Interface

- Na AWS CLI, use o comando `modify-cluster` e o parâmetro `no-multi-az` da maneira a seguir.

```
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
```

Depois de convertido em single-AZ, o data warehouse perderá a garantia do SLA de 99,99. O throughput geral também será afetado. Quando as alterações forem salvas, você poderá visualizar os detalhes na página de detalhes do cluster.

## Redimensionamento de um data warehouse multi-AZ

Você pode redimensionar um data warehouse multi-AZ e especificar vários nós ou um tipo de nó diferentes da configuração atual do data warehouse.

Usar o console

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, Provisioned clusters dashboard (Painel de clusters provisionados) e Clusters. Os clusters de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha o cluster no qual você deseja redimensionar o data warehouse multi-AZ. A página de detalhes do cluster é exibida.
4. Em Actions (Ações), escolha Resize (Redimensionar). A página Resize cluster (Redimensionar cluster) é exibida.
5. Siga as instruções na página. Você pode redimensionar o cluster agora, uma vez em um momento específico, ou aumentar e diminuir o tamanho do cluster definindo uma programação.
6. Em Novas configurações, escolha um dos tipos de nó RA3 na lista suspensa Tipo de nó.
7. Clique em Redimensionar cluster.

Usando a AWS Command Line Interface

Para redimensionar um data warehouse multi-AZ usando a AWS Command Line Interface

- Na AWS CLI, use o comando `resize-cluster` para alterar o número de nós de uma única zona de disponibilidade da maneira a seguir.

```
aws redshift resize-cluster \
    --cluster-identifier test-maz-11
    --cluster-type multi-node
    --node-type ra3.4xlarge
    --number-of-nodes 6
```

## Configuração de multi-AZ para um data warehouse restaurado a partir de um snapshot

Você também pode criar um cluster multi-AZ o restaurando a partir de um snapshot.

Usar o console

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, Snapshots e escolha o snapshot a ser copiado.
3. Escolha Restore snapshot (Restaurar snapshot) e Restore to a provisioned cluster (Restaurar em um cluster provisionado).
4. Insira as propriedades do cluster. Para obter informações gerais sobre como criar clusters, consulte Criar um cluster.
5. Escolha um dos tipos de nó RA3 na lista suspensa Node type (Tipo de nó). A opção de configuração AZ só permanece disponível quando você escolhe um tipo de nó RA3.
6. Em Configuração AZ, escolha Multi-AZ.
7. Em Número de nós por AZ, insira pelo menos dois nós para o cluster.
8. Você tem a opção de carregar dados de amostra ou adicionar dados próprios:
    - Em Sample data (Dados de exemplo), escolha Load sample data (Carregar dados de exemplo) para carregar o conjunto de dados de exemplo em seu cluster do Amazon Redshift. O Amazon Redshift carrega o Tickit do conjunto de dados de exemplo para o banco de dados dev padrão e o esquema public. O Amazon Redshift carrega automaticamente o conjunto de

dados de exemplo no cluster do Amazon Redshift. Você pode começar usando o editor de consulta v2 para consultar dados.

- Para adicionar dados próprios ao cluster do Amazon Redshift, siga as etapas em Trazer seus próprios dados para o Amazon Redshift.

9. Role para baixo até Additional configurations (Configurações adicionais), expanda Network and security (Rede e segurança) e aceite o Cluster subnet group (Grupo de sub-redes do cluster) padrão ou escolha outro. Se você escolher outro grupo de sub-redes do cluster, verifique se existem três zonas de disponibilidade no grupo de sub-redes selecionado.
10. Em Additional configurations (Configurações adicionais), expanda Database configurations (Configurações do banco de dados).
11. Em Database encryption (Criptografia do banco de dados), para usar uma chave do KMS personalizada diferente da chave do AWS Key Management Service padrão, clique em Customize encryption settings (Personalizar configurações de criptografia). Esta opção está desmarcada por padrão.
12. Em Choose an KMS key (Escolher uma chave do KMS), selecione uma chave do AWS Key Management Service ou insira um ARN. Ou clique em Criar uma chave do AWS Key Management Service no console do AWS Key Management Service. Para obter mais informações sobre como criar chaves KMS, consulte Criar chaves no Guia do desenvolvedor do AWS Key Management Service.
13. Clique em Restore cluster from snapshot (Restaurar cluster de um snapshot). Quando a restauração do cluster for bem-sucedida, você poderá visualizar os detalhes na página de detalhes do cluster.

Usando a AWS Command Line Interface

- Na AWS CLI, use o comando `restore-from-cluster-snapshot` da maneira a seguir.

```
aws redshift restore-from-cluster-snapshot
--region eu-west-1
--multi-az
--snapshot-identifier test-snap1
--cluster-identifier test-saz-11
--endpoint-url https://redshift.eu-west-1.amazonaws.com/
```

# Failover da implantação multi-AZ

O data warehouse multi-AZ é uma coleção de recursos computacionais implantados simultaneamente em duas zonas de disponibilidade. Os recursos computacionais implantados na zona de disponibilidade primária são conhecidos como computação primária e aqueles nas zonas de disponibilidade secundárias são conhecidos como computação secundária. Um data warehouse multi-AZ pode se recuperar automaticamente sem nenhuma intervenção do usuário durante um evento improvável, como uma zona de disponibilidade ou falha na infraestrutura. O processo de recuperação envolve o failover da computação primária para a computação secundária e a designação de recursos computacionais secundários como primários. Além disso, novos recursos computacionais secundários são provisionados em uma terceira zona de disponibilidade. O processo de recuperação automática é medido em termos de RTO e RPO.

- Objetivo de tempo de recuperação (RTO): tempo que um sistema leva para retornar a um estado de trabalho após um desastre. Em outras palavras, o RTO mede o tempo de inatividade.
- Objetivo de ponto de recuperação (RPO) — quantidade de dados que podem ser perdidos (medidos no tempo). Para um data warehouse multi-AZ do Amazon Redshift, o RPO normalmente é zero, pois todos os dados são armazenados no Amazon Redshift Managed Storage (RMS), apoiado pelo Amazon Simple Storage Service, que é altamente durável e permanece disponível por padrão.

> **Note**
>
> O desempenho de uma consulta individual não vai mudar depois da ocorrência de um failover. O throughput geral do data warehouse será reduzido por um curto período por causa da indisponibilidade de recursos computacionais em uma das zonas de disponibilidade. No entanto, o Amazon Redshift vai adquirir automaticamente capacidade em outra zona de disponibilidade para garantir que a mesma capacidade de processamento do data warehouse seja restaurada.

Além do processo de recuperação automática, você também pode acionar esse processo manualmente para o data warehouse usando a opção Computação primária de failover. Você pode usar essa abordagem para testar como o multi-AZ ajudaria a aplicação a obter disponibilidade mais alta e continuidade melhor.

Usar o console

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. Execute um destes procedimentos:
   - No menu de navegação, escolha Clusters. Em Clusters, escolha um cluster. A página de detalhes do cluster é exibida.
   - No painel de clusters, escolha um cluster.
3. Em Ações, escolha Computação primária de failover.
4. Quando aparecer um prompt, clique em Confirm (Confirmar).

Usando a AWS Command Line Interface

- Na AWS CLI, use o comando `failover-primary-compute` da maneira a seguir.

```
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
```

Depois que a operação acima for confirmada, o Amazon Redshift vai realizar as mesmas etapas como uma recuperação automática em uma zona de disponibilidade ou falha na infraestrutura. O processo vai indisponibilizar os nós de computação na zona de disponibilidade primária, e os recursos computacionais na zona de disponibilidade secundária vão ser designados como computação primária. Quando a recuperação do cluster é concluída com êxito, a implantação multi-AZ permanece disponível. O data warehouse multi-AZ também vai provisionar automaticamente novos nós de computação em outra zona de disponibilidade assim que ele estiver disponível.

Durante esse processo, o status do cluster no console é exibido como “em modificação” durante todo o tempo, pois o cluster se recupera e se reconfigura automaticamente de volta à configuração de implantação multi-AZ. O cluster poderá aceitar novas conexões imediatamente. As conexões existentes e as consultas em trânsito poderão ser perdidas. Você poderá repeti-las imediatamente.

# Monitoramento de consultas para multi-AZ

Você pode visualizar informações sobre consultas executadas nos últimos 7 dias, independentemente do tipo, tamanho e status (pausar ou retomar) do seu cluster.

## Visualização de consultas e cargas para data warehouses multi-AZ

As informações mostradas na página Queries and loads (Consultas e cargas) são preenchidas com informações das tabelas de sistema do Amazon Redshift (visualizações SYS_*). Essas informações permitem que você exiba informações adicionais sobre suas consultas e oferecem 7 dias de retenção. O diagnóstico de consultas fica mais rápido, permitindo que você filtre dados por banco de dados, nome de usuário ou tipo de instrução SQL. Para ver esses filtros e informações adicionais para todas as consultas executadas, observe os seguintes pré-requisitos:

- Você deve se conectar a um banco de dados escolhendo Connect to database (Conectar-se a um banco de dados).
- Seu usuário do banco de dados deve ter os perfis sys:operator ou sys:monitor e permissões para realizar o monitoramento de consultas. Para obter informações sobre os perfis do sistema, consulte as Perfis do Amazon Redshift definidos pelo sistema no Guia do desenvolvedor de bancos de dados do Amazon Redshift.

Você verá esses filtros e informações de consulta adicionais ao se conectar a um banco de dados.

Como exibir dados de performance de consultas em Queries and loads

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Queries and loads (Consultas e cargas) para exibir a lista de consultas de sua conta.
3. Talvez seja necessário conectar-se a um banco de dados para ver um filtro adicional. Se necessário, clique em Connect to database (Conectar-se a um banco de dados) e siga as instruções para se conectar a um banco de dados.

   Por padrão, a lista exibe consultas de todos os seus clusters nas últimas 24 horas. É possível alterar o escopo da data exibida no console.

Como exibir dados de performance de consultas em Query monitoring

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters. Em Clusters, selecione um cluster.
3. Escolha Query monitoring (Monitoramento de consultas).
4. Dependendo da configuração ou versão do seu cluster, talvez você precise se conectar a um banco de dados para ver filtros adicionais. Se necessário, clique em Connect to database (Conectar-se a um banco de dados) e siga as instruções para se conectar a um banco de dados.

## Monitorar uma consulta em uma implantação multi-AZ

Uma implantação multi-AZ usa recursos de computação que são implantados em ambas as zonas de disponibilidade e podem continuar operando caso os recursos em determinada zona de disponibilidade fiquem indisponíveis. Todos os recursos de computação serão usados o tempo todo. Isso permite a operação completa em duas zonas de disponibilidade de forma ativa-ativa para operações de leitura e gravação.

Você pode consultar visualizações SYS_ no esquema pg_catalog para monitorar o tempo de execução da consulta em uma implantação multi-AZ. As visualizações SYS_ exibem atividades do tempo de execução de consultas ou estatísticas de clusters primários e secundários. Para obter uma lista de visualizações de monitoramento, consulte Monitoring views.

Siga estas etapas para monitorar o tempo de execução da consulta para cada zona de disponibilidade na implantação multi-AZ:

1. Navegue até o console do Amazon Redshift, conecte-se ao banco de dados em sua implantação multi-AZ e execute consultas por meio do editor de consultas.
2. Execute qualquer consulta de exemplo na implantação multi-AZ do Amazon Redshift.
3. Para uma implantação multi-AZ, você pode identificar uma consulta e a zona de disponibilidade em que ela é executada usando a coluna compute_type na tabela SYS_QUERY_HISTORY. primary representa consultas executadas no cluster primário na implantação multi-AZ, enquanto secondary representa consultas executadas no cluster secundário na implantação multi-AZ.

   A consulta a seguir usa a coluna compute_type para monitorar uma consulta.

```
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;
```

### Encerramento de uma consulta para clusters

Encerramento de uma consulta para clusters

O procedimento é aplicável a clusters multi-AZ e single-AZ.

Para encerrar uma consulta

Você também pode usar a página Queries (Consultas) para encerrar uma consulta em andamento no momento.

Seu usuário do banco de dados deve ter o perfil sys:operator e permissões para encerrar uma consulta em execução. Para obter informações sobre os perfis do sistema, consulte as Perfis do Amazon Redshift definidos pelo sistema no Guia do desenvolvedor de bancos de dados do Amazon Redshift.

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Queries and loads (Consultas e cargas) para exibir a lista de consultas de sua conta.
3. Escolha a consulta em execução que você deseja encerrar na lista e escolha Terminate query (Encerrar consulta).

## Gerenciamento de clusters usando o console

Para criar, modificar, redimensionar, excluir, reinicializar e fazer backup de clusters, use a seção Clusters no console do Amazon Redshift.

Para visualizar clusters

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

2. No menu de navegação, escolha Clusters. Os clusters de sua conta na região atual da AWS são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista. Se você não tiver nenhum cluster, escolha Create cluster (Criar cluster) para criar um.
3. Escolha o nome do cluster na lista para visualizar mais detalhes sobre o cluster.

Tópicos


- Criar um cluster
- Criar cluster de visualização prévia
- Modificar um cluster
- Excluir um cluster
- Reinicialização de um cluster
- Redimensionamento de um cluster
- Atualizar a versão de um cluster
- Informações sobre a configuração de clusters
- Obter uma visão geral do status de clusters
- Criar um snapshot de um cluster
- Criar ou editar um alarme de espaço em disco
- Utilização dos dados de performance do cluster


## Criar um cluster

Antes de criar um cluster, leia Visão geral do do Amazon Redshift e Clusters e nós no Amazon Redshift.

Para criar um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters. Os clusters de sua conta na região atual da AWS são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha Create cluster (Criar cluster) para criar um cluster.
4. Siga as instruções na página do console para inserir as propriedades de Cluster configuration (Configuração do cluster).

A etapa a seguir descreve um console do Amazon Redshift que está sendo executado em uma Região da AWS compatível com tipos de nó RA3. Para conferir a lista de Regiões da AWS compatíveis com tipos de nó RA3, consulte Visão geral dos tipos de nó RA3 no Guia de gerenciamento do Amazon Redshift.

Se você não souber o tamanho do cluster, escolha Ajude-me a escolher. Isso inicia uma calculadora de dimensionamento que faz perguntas sobre o tamanho e as características de consulta dos dados que você planeja armazenar em seu data warehouse. Se você souber o tamanho necessário do cluster (ou seja, o tipo de nó e o número de nós), escolha Eu escolherei. Em seguida, escolha o Tipo de nó e número de Nós para dimensionar seu cluster para a prova de conceito.

> **Note**
>
> Se sua organização for elegível e seu cluster estiver sendo criado em uma Região da AWS em que o Amazon Redshift sem servidor não está indisponível, você poderá criar um cluster no programa de teste gratuito do Amazon Redshift. Escolha Produção ou Teste gratuito para responder à pergunta Para que você está planejando usar esse cluster? Ao escolher Teste gratuito, você crie uma configuração com o tipo de nó dc2.large. Para obter mais informações sobre a escolha de um teste gratuito, consulte Teste gratuito do Amazon Redshift. Para obter uma lista de Regiões da AWS nas quais o Amazon Redshift sem servidor está disponível, consulte os endpoints listados para a API do Redshift sem servidor na Referência geral da Amazon Web Services.

5. Na seção Configuração do banco de dados, especifique um valor para Nome do usuário administrador. Em Senha do administrador, é possível escolher uma das seguintes opções:

   - Gere uma senha: use uma senha gerada pelo Amazon Redshift.
   - Adicionar manualmente uma senha de administrador: use a própria senha.
   - Gerenciar credenciais de administrador no AWS Secrets Manager: o Amazon Redshift usa AWS Secrets Manager para gerar e gerenciar a senha de administrador. O uso do AWS Secrets Manager para gerar e gerenciar o segredo da senha incorre em uma taxa. Para obter informações sobre definição de preços do AWS Secrets Manager, consulte Definição de preços do AWS Secrets Manager.

6. (Opcional) Siga as instruções na página do console para inserir as propriedades deCluster permissions (Permissões do cluster). Forneça permissões de cluster se seu cluster precisar acessar outros serviços da AWS para você, por exemplo, para carregar dados do Amazon S3.
7. Para criar o cluster, escolha Create cluster (Criar cluster). Podem ser necessários alguns minutos para preparar o cluster para ser usado.

## Configurações adicionais

Ao criar um cluster, é possível especificar propriedades adicionais para personalizá-lo. Você pode encontrar mais detalhes sobre algumas dessas propriedades na lista a seguir.

Tipo de endereço IP

Escolha o tipo de endereço IP para o cluster. É possível optar por fazer com que os recursos só se comuniquem via protocolo de endereçamento IPv4 ou escolher o modo de pilha dupla, o que permite que os recursos se comuniquem via IPv4 e IPv6. Esse recurso só está disponível nas regiões GovCloud (EUA-Leste) da AWS e GovCloud (EUA-Oeste) da AWS. Para obter mais informações sobre regiões da AWS, consulte Regions and Availability Zones.

Nuvem privada virtual (VPC)

Escolha uma VPC que tenha um grupo de sub-redes do cluster. Depois que o cluster for criado, o grupo de sub-redes do cluster não poderá ser alterado.

Grupos de parâmetros

Selecione um parameter group de cluster para associar ao cluster. Se você não selecionar um, o cluster usará um parameter group padrão.

Criptografia

Selecione se deseja criptografar todos os dados no cluster e nos snapshots. Se você deixar a configuração padrão, None, a criptografia não será habilitada. Se desejar habilitar a criptografia, escolha se deseja usar o AWS Key Management Service (AWS KMS) ou um módulo de segurança de hardware (HSM) e defina as configurações relacionadas. Para obter mais informações sobre criptografia no Amazon Redshift, consulte Criptografia de banco de dados do Amazon Redshift.

- KMS

  Selecione Usar o AWS Key Management Service (AWS KMS) se quiser habilitar a criptografia e usar o AWS KMS para gerenciar a chave de criptografia. Escolha também a tecla para usar.

É possível escolher uma chave padrão, uma chave da conta atual ou uma chave de outra conta.

> **Note**
>
> Se você desejar usar uma chave de outra conta da AWS, insira o nome do recurso da Amazon (ARN) da chave a ser utilizada. É preciso ter permissão para usar a chave. Para obter mais informações sobre acesso às chaves no AWS KMS, consulte Controlar o acesso às chaves no Guia do desenvolvedor do AWS Key Management Service.

Para obter mais informações sobre criptografia AWS KMS no Amazon Redshift, consulte Criptografia de banco de dados do Amazon Redshift usando AWS KMS.

- HSM

  Escolha HSM se deseja habilitar a criptografia e usar o módulo de segurança de hardware (HSM) para gerenciar sua chave de criptografia.

  Se você escolher HSM, selecione os valores em HSM Connection (Conexão HSM) e HSM Client Certificate (Certificado do cliente HSM). Esses valores são necessários para que o Amazon Redshift e o HSM formem uma conexão confiável pela qual a chave do cluster pode ser passada. A conexão HSM e o certificado do cliente devem ser configurados no Amazon Redshift antes de iniciar um cluster. Para obter mais informações sobre como configurar conexões de HSM e certificados do cliente, consulte Criptografia para Amazon Redshift usando módulos de segurança de hardware.

Maintenance track (Acompanhamento de manutenção)

É possível escolher se a versão usada do cluster é a Current (Atual), Trailing (Inicial) ou, algumas vezes, a trilha Preview (Demonstração).

Monitoramento

Você pode escolher se deseja criar alarmes CloudWatch.

Configure cross-region snapshot (Configurar snapshots entre regiões)

É possível escolher se deseja habilitar snapshots entre regiões.

Automated Snapshot Retention Period (Período de retenção de snapshot automático)

Você pode escolher o número de dias para reter esses snapshots dentro de 35 dias. Se o tipo de nó for DC2 ou DS2, você poderá escolher zero (0) dia para não criar snapshots automáticos.

Manual snapshot retention period (Período de retenção de snapshot manual)

Você pode escolher o número de dias ou `Indefinitely` para reter esses snapshots.

## Criar cluster de visualização prévia

Você pode criar um cluster do Amazon Redshift em Preview (Pré-visualização) para testar novos recursos do Amazon Redshift. Você não pode usar esses recursos em produção nem mover seu cluster de Preview (Pré-visualização) para um cluster de produção ou um cluster em outra faixa. Para conferir os termos e condições da pré-visualização, consulte Betas e pré-visualizações nos Termos de serviços da AWS.

Como criar um cluster em Preview (pré-visualização)

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, Provisioned clusters dashboard (Painel de clusters provisionados) e Clusters. Os clusters de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Um banner é exibido na página da lista Clusters que apresenta a pré-visualização. Escolha o botão Create preview cluster (Criar cluster de pré-visualização) para abrir a página de criação de cluster.
4. Insira as propriedades do cluster. Escolha a Preview track (Faixa de pré-visualização) que contém os recursos que deseja testar. Recomendamos inserir um nome que indique que o cluster está em uma faixa de pré-visualização. Escolha opções para o cluster, incluindo opções rotuladas como -preview (-pré-visualização), para os recursos que deseja testar. Para obter informações gerais sobre a criação de clusters, consulte Criar um cluster no Guia de gerenciamento do Amazon Redshift.
5. Escolha Criar cluster para criar um cluster em pré-visualização.

> **Note**
>
> A faixa `preview_2023` é a faixa de pré-visualização mais recente disponível. Essa faixa só dá suporte à criação de clusters com tipos de nó RA3. Os tipos de nó DC2 e DS2 e qualquer tipo de nó mais antigo não são compatíveis.

6. Quando seu cluster de pré-visualização estiver disponível, use seu cliente SQL para carregar e consultar dados.

Para obter informações sobre a visualização em grupos de trabalho do Redshift Serverless, consulte Criar visualização prévia de grupo de trabalho.

## Modificar um cluster

Ao modificar um cluster, as alterações nas seguintes opções são aplicadas automaticamente:

- VPC security groups (Grupos de segurança da VPC)
- Publicly accessible
- Admin user password (Senha do usuário administrador)
- Conexão HSM
- HSM Client Certificate
- Detalhes da manutenção
- Snapshot preferences (Preferências de snapshot)

As alterações nas seguintes opções serão implementadas somente depois que o cluster for reiniciado:

- Identificador de Cluster

  O Amazon Redshift reinicia o cluster automaticamente quando você altera o Identificador de cluster.
- Enhanced VPC routing

  O Amazon Redshift reinicia o cluster automaticamente quando você altera o Roteamento aprimorado da VPC.
- Grupo de parâmetros do cluster

- Tipo de endereço IP

  Esse recurso só está disponível nas regiões GovCloud (EUA-Leste) da AWS e GovCloud (EUA-Oeste) da AWS. Para obter mais informações sobre regiões da AWS, consulte Regions and Availability Zones.

Se você diminuir o período de retenção de snapshot automatizado, os snapshots automatizados existentes cujas configurações estejam fora do novo período de retenção serão excluídos. Para ter mais informações, consulte Snapshots e backups do Amazon Redshift.

Para obter mais informações sobre as propriedades do cluster, consulte Configurações adicionais.

Como modificar um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters.
3. Escolha o cluster a ser modificado.
4. Selecione a opção Editar. A página Editar cluster é exibida.
5. Atualize as propriedades do cluster. Algumas das propriedades que você pode modificar são:

   - Identificador de Cluster
   - Retenção de snapshots
   - Realocação de cluster

   Para editar configurações de Rede e segurança, Manutenção e Configurações do banco de dados, o console fornece links para a guia de detalhes do cluster apropriada.
6. Escolha Salvar alterações.

## Excluir um cluster

Se você não precisa mais de seu cluster, é possível excluí-lo. Se você pretende disponibilizar um novo cluster com os mesmos dados e configuração daquele que você está excluindo, precisará de um snapshot manual. Usando um snapshot manual, você poderá restaurar o snapshot posteriormente e continuar usando o cluster. Se você excluir seu cluster e não criar um snapshot manual final, os dados do cluster serão excluídos. Em ambos os casos, os snapshots automatizados

são excluídos depois que o cluster é excluído, mas todos os snapshots manuais são mantidos até que você os exclua. Pode haver uma cobrança de taxas de armazenamento do Amazon Simple Storage Service para snapshots manuais, dependendo da quantidade de armazenamento disponível para os snapshots do Amazon Redshift para seus clusters. Para ter mais informações, consulte Desativação e exclusão de clusters.

A exclusão de um cluster também exclui todos os segredos do AWS Secrets Manager associados.

Para excluir um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters.
3. Escolha o cluster a ser excluído.
4. Em Ações, escolha Excluir. A página Delete cluster (Excluir cluster) é exibida.
5. Escolha Delete Cluster (Excluir cluster).

## Reinicialização de um cluster

Quando você reinicializa um cluster, o status do cluster é definido como `rebooting` e um evento de cluster será criado quando a reinicialização for concluída. Todas as modificações pendentes do cluster são aplicadas nesta reinicialização.

Para reinicializar um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters.
3. Escolha o cluster a ser reiniciado.
4. Em Actions (Ações), escolha Reboot cluster (Reiniciar cluster). A página Reboot cluster (Reinicializar cluster) é exibida.
5. EscolhaReboot cluster (Reinicializar cluster).

## Redimensionamento de um cluster

Ao redimensionar um cluster, você especifica vários nós ou tipos de nó diferentes da configuração atual do cluster. Enquanto o cluster está no processo de redimensionamento, não é possível executar consultas que façam operações de gravação ou leitura/gravação no cluster. Somente a leitura de consultas é possível.

Para obter mais informações sobre o redimensionamento de clusters, incluindo uma demonstração do processo de redimensionamento de clusters usando diferentes abordagens, consulte Redimensionar clusters.

Para redimensionar um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters.
3. Escolha o cluster a ser redimensionado.
4. Em Actions (Ações), escolha Resize (Redimensionar). A página Resize cluster (Redimensionar cluster) é exibida.
5. Siga as instruções na página. Você pode redimensionar o cluster agora, uma vez em um momento específico, ou aumentar e diminuir o tamanho do cluster definindo uma programação.
6. Dependendo das suas opções, escolha Resize now (Redimensionar agora) ou Schedule resize (Agendar redimensionamento).

Se você tiver nós reservados, por exemplo nós reservados DS2, poderá atualizar para nós reservados RA3. Faça isso usando o console para restaurar a partir de um snapshot ou para executar um redimensionamento elástico. Você pode usar o console se orientar nesse processo. Para obter mais informações sobre a atualização para nós RA3, consulte Atualizar para os tipos de nó RA3.

## Atualizar a versão de um cluster

É possível atualizar a versão de manutenção de um cluster que tem um valor Release Status (Status da versão) de New release available (Nova versão disponível). Ao atualizar a versão de manutenção, você pode optar por atualizar imediatamente ou atualizar na próxima janela de manutenção.

> **Important**
>
> Se você atualizar imediatamente, o cluster ficará offline até que a atualização seja concluída.

Para atualizar um cluster para uma nova versão

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters.
3. Escolha o cluster a ser atualizado
4. Em Actions (Ações), escolha Upgrade cluster version (Atualizar versão de cluster). A página Upgrade cluster version (Atualizar versão de cluster) é exibida.
5. Siga as instruções na página.
6. Escolha Upgrade cluster version (Atualizar versão de cluster).

## Informações sobre a configuração de clusters

Para exibir informações sobre um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters e o nome do cluster na lista para abrir os respectivos detalhes. Os detalhes do cluster são exibidos, podendo incluir as guias Cluster performance (Performance do cluster), Query monitoring (Monitoramento de consultas), Databases (Bancos de dados), Datashares (Unidades de compartilhamento de dados), Schedules (Programação), Maintenance (Manutenção) e Properties (Propriedades).
3. Escolha cada guia para visualizar mais detalhes.

## Obter uma visão geral do status de clusters

Para visualizar o status de um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

2. No menu de navegação, escolha Clusters.
3. Visualize o status do cluster na coluna Status.

## Criar um snapshot de um cluster

Para criar um snapshot de um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters.
3. Escolha o cluster do qual criar um snapshot.
4. Em Actions (Ações), escolha Create snapshot (Criar snapshot). A página Create snapshot (Criar snapshot) é exibida.
5. Siga as instruções na página.
6. Escolha Criar snapshot.

## Criar ou editar um alarme de espaço em disco

Para criar um alarme de uso de espaço em disco de um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Alarms (Alarmes).
3. Em Actions (Ações), escolha Create alarm (Criar alarme). A página Create alarm (Criar alarme) é exibida.
4. Siga as instruções na página.
5. Selecione Criar alarme.

## Utilização dos dados de performance do cluster

No console, é possível trabalhar com a performance do cluster na guia Cluster performance (Performance do cluster) da página de detalhes do cluster.

# Gerenciar clusters usando a AWS CLI e a API do Amazon Redshift

Você pode usar as operações de AWS CLI a seguir para gerenciar clusters no Amazon Redshift.

- cancel-resize
- create-cluster
- delete-cluster
- describe-clusters
- describe-cluster-versions
- describe-node-configuration-options
- describe-orderable-cluster-options
- describe-resize
- modify-cluster
- pause-cluster
- reboot-cluster
- resize-cluster
- resume-cluster

Você pode usar as operações de API do Amazon Redshift a seguir para gerenciar clusters.

- CancelResize
- CreateCluster
- DeleteCluster
- DescribeClusters
- DescribeClusterVersions
- DescribeNodeConfigurationOptions
- DescribeResize
- DescribeOrderableClusterOptions
- ModifyCluster
- PauseCluster

- RebootCluster
- ResizeCluster
- ResumeCluster

# Gerenciamento de clusters em uma VPC

Tópicos


- Visão geral
- Criar um cluster em uma VPC
- Gerenciar grupos de segurança da VPC de um cluster
- Definir as configurações de comunicação do grupo de segurança para um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor
- Como o Amazon Redshift funciona com o compartilhamento de VPC para recursos da AWS
- Grupos de sub-rede de cluster do Amazon Redshift


## Visão geral

O Amazon Redshift oferece suporte às plataformas EC2-VPC e EC2-Classic para lançar um cluster em uma nuvem privada virtual (VPC) baseada no serviço Amazon VPC. Para obter mais informações, consulte Uso do EC2-VPC ao criar o cluster.

> **Note**
>
> O Amazon Redshift dá suporte ao lançamento de clusters em VPCs de locação dedicada. Para obter mais informações, consulte Instâncias dedicadas no Manual do usuário do Amazon VPC.

Ao provisionar um cluster em VPC, você precisa fazer o seguinte:

- Fornecer informações sobre a VPC.

  Ao solicitar que o Amazon Redshift crie um cluster em seu VPC, você deve fornecer suas informações de VPC criando um grupo de sub-rede de cluster. Essas informações incluem o ID da VPC e uma lista de sub-redes em sua VPC. Ao iniciar um cluster, você fornece o grupo de sub-

rede do cluster para que o Amazon Redshift possa provisionar seu cluster em uma das sub-redes no VPC. Para obter mais informações sobre como criar grupos de sub-redes no Amazon Redshift, consulte Grupos de sub-rede de cluster do Amazon Redshift. Para obter mais informações sobre como configurar o VPC, consulte Conceitos básicos do Amazon VPC no Guia de conceitos básicos do Amazon VPC.

- Como opção, configure as opções acessíveis publicamente.

  Se você configurar o cluster para ser acessível publicamente, o Amazon Redshift usará um endereço IP elástico como endereço IP externo. Um endereço IP elástico é um endereço IP estático. Com ele, você pode alterar a configuração subjacente sem afetar o endereço IP usado pelos clientes para se conectarem ao cluster. Essa abordagem pode ser útil em situações como uma recuperação depois de uma falha. A criação de um endereço IP elástico depende da sua configuração de realocação de zona de disponibilidade. Existem duas opções:

  1. Se você tiver a realocação de zona de disponibilidade ativada e quiser habilitar o acesso público, não especifique um endereço IP elástico. Um endereço IP elástico gerenciado pelo Amazon Redshift será atribuído. Estará associado à sua conta da AWS.
  2. Se a realocação de zona de disponibilidade estiver desativada e você quiser habilitar o acesso público, poderá optar por criar um endereço IP elástico para a VPC no Amazon EC2 antes de iniciar o cluster do Amazon Redshift. Se você não criar um endereço IP, o Amazon Redshift fornecerá um endereço IP elástico para a VPC. Esse endereço IP elástico será gerenciado pelo Amazon Redshift e não estará associado à sua conta da AWS.

  Para obter mais informações, consulte Endereços de IP elásticos no Manual do usuário do Amazon EC2 para instâncias do Linux.

  Em alguns casos, você pode ter um cluster acessível publicamente em uma VPC ao qual você deseja conectar-se usando o endereço IP privado de dentro da VPC. nesse caso, defina os seguintes parâmetros da VPC como `true`:

  - `DNS resolution`
  - `DNS hostnames`

  Suponha que você tem um cluster acessível publicamente em uma VPC, mas que não defina esses parâmetros como `true` na VPC. Nesses casos, as conexões feitas de dentro da VPC são resolvidas para o endereço IP elástico do cluster e não para endereço IP privado. Recomendamos definir esses parâmetros como `true` e usamos o endereço IP privado para um cluster acessível publicamente durante a conexão internamente na VPC. Para obter mais informações, consulte Usar DNS com a VPC no Guia do usuário da Amazon VPC.

> **Note**
>
> Se houver um cluster acessível publicamente em uma VPC, as conexões de dentro da VPC continuarão a usar o endereço IP elástico para conectar-se ao cluster até que você redimensione o cluster. Isso ocorre mesmo com os parâmetros anteriores definidos. Todos os novos clusters seguirão o novo comportamento de usar o endereço IP privado ao conectar-se ao cluster acessível publicamente de dentro da mesma VPC.

O endereço IP elástico é um endereço IP externo para acesso ao cluster de fora de uma VPC. Não está relacionado aos endereços IP públicos do nó do cluster e aos endereços IP privados que são exibidos no console do Amazon Redshift em Detalhes de conexão. Os endereços IP de nó do cluster públicos e privados são exibidos, independentemente do cluster ser acessível publicamente ou não. Eles só são usados em determinadas circunstâncias para configurar regras de entrada no host remoto. Essas circunstâncias ocorrem quando você carrega dados de uma instância do Amazon EC2 ou outro host remoto usando uma conexão Secure Shell (SSH). Para obter mais informações, consulte Etapa 1: Recuperar a chave pública do cluster e os endereços IP do nó do cluster, no Guia do desenvolvedor de banco de dados do Amazon Redshift.

A opção de associar um cluster a um endereço IP elástico está disponível quando você cria o cluster ou restaura-o de um snapshot. Em alguns casos, você pode desejar associar o cluster a um endereço IP elástico ou alterar um endereço IP elástico que está associado ao cluster. Para anexar um endereço de IP elástico após a criação do cluster, primeiro atualize o cluster para que não seja publicamente acessível e, em seguida, torne-o publicamente acessível e adicione um endereço de IP elástico na mesma operação.

- Associe um security group da VPC.

  Em seguida, você concede acesso de entrada usando um security group da VPC. Esse security group da VPC deve dar acesso pela porta do banco de dados para o cluster, de maneira que você possa se conectar usando ferramentas cliente SQL. Você pode configurar isso com antecedência ou adicionar regras depois que iniciar o cluster. Para obter mais informações, consulte Definir as configurações de comunicação do grupo de segurança para clusters do Amazon Redshift, que fornece orientação sobre a configuração de regras de entrada e saída entre um cliente e um cluster provisionado ou um grupo de trabalho do Amazon Redshift sem servidor. Outro recurso que ajuda você a entender os grupos de segurança é Segurança na sua VPC no Manual do usuário

do Amazon VPC. Observe que não é possível usar os grupos de segurança de cluster do Amazon Redshift para conceder acesso de entrada ao cluster.

Para obter mais informações sobre como trabalhar com clusters em uma VPC, consulte Criar um cluster em uma VPC.

Restaurar um snapshot de um cluster na VPC

Um snapshot de um cluster na VPC pode ser restaurado somente em uma VPC, e não externamente à VPC. Você pode restaurá-lo na mesma VPC ou em outra VPC na conta. Para obter mais informações sobre snapshots, consulte Snapshots e backups do Amazon Redshift.

## Criar um cluster em uma VPC

Veja a seguir as etapas gerais como você pode implantar um cluster na nuvem privada virtual (VPC).

Para criar um cluster em uma VPC

1. Configure uma VPC.

   Você poderá criar o cluster na VPC padrão da conta, se a conta tiver uma, ou em uma VPC criada. Para obter mais informações, consulte Uso do EC2-VPC ao criar o cluster. Para criar uma VPC, consulte Criar uma VPC no Guia do usuário da Amazon VPC. Anote o identificador da VPC, a sub-rede e a zona de disponibilidade da sub-rede. Você precisará dessas informações ao iniciar o cluster.

   > **Note**
   >
   > Você deve ter pelo menos uma sub-rede definida na VPC, de maneira que possa adicioná-la ao grupo de sub-redes do cluster na próxima etapa. Para obter mais informações sobre como adicionar sub-redes à sua VPC, consulte Adição de uma sub-rede à VPC no Manual do usuário do Amazon VPC.

2. Crie um grupo de sub-redes de clusters do Amazon Redshift para especificar qual sub-rede o cluster do Amazon Redshift pode usar na VPC.

   Você pode criar um grupo de sub-rede de cluster usando o console do Amazon Redshift ou programaticamente. Para obter mais informações, consulte Grupos de sub-rede de cluster do Amazon Redshift.

3. Autorize o acesso de conexões de entrada em um grupo de segurança da VPC que você associa ao cluster.

   É possível habilitar um cliente fora da VPC (na Internet púbica) para conectar-se ao cluster. Para fazer isso, você associa o cluster a um grupo de segurança da VPC que concede acesso de entrada à porta que você usou ao iniciar o cluster. Para obter mais informações sobre regras de grupo de segurança, consulte Regras de grupo de segurança no Manual do usuário do Amazon VPC.
4. Siga as etapas em Conceitos básicos do Amazon Redshift no Guia de conceitos básicos do Amazon Redshift para criar um cluster. Faça as seguintes modificações ao criar seu cluster:

   - Para exibir a seção Additional configurations (Configurações adicionais), desative Use defaults (Usar padrões).
   - Na seção Network and security (Rede e segurança), especifique a Virtual private cloud (VPC) [Nuvem privada virtual (VPC)], o Cluster subnet group (Grupo de sub-rede do cluster) e o VPC security group (Grupo de segurança da VPC) que você configurou.

Agora você está pronto para usar o cluster. Você pode seguir as etapas de Conceitos básicos para testar o cluster fazendo upload dos dados de exemplo e testando consultas de exemplo.

## Gerenciar grupos de segurança da VPC de um cluster

Quando você provisiona um cluster do Amazon Redshift, ele é bloqueado por padrão para que ninguém tenha acesso a ele. Para conceder a outros usuários acesso de entrada a um cluster do Amazon Redshift, você associa o cluster a um grupo de segurança. Se você estiver na plataforma EC2-VPC, poderá usar um grupo de segurança do Amazon VPC existente ou definir um novo. Depois, você o associa a um cluster, conforme descrito a seguir. Se estiver na plataforma EC2-Classic, você vai definir um security group de cluster e associá-lo a um cluster. Para obter mais informações sobre como usar security groups de cluster na plataforma EC2-Classic, consulte Grupos de segurança de clusters do Amazon Redshift.

Um security group da VPC consiste em um conjunto de regras que controlam o acesso a uma instância na VPC, como o cluster. Acesso ao conjunto de regras individuais baseado em intervalos de endereços IP ou em outros security groups da VPC. Quando você associa um security group da VPC a um cluster, as regras definidas no security group da VPC controlam o acesso ao cluster.

Cada cluster que você provisiona na plataforma EC2-VPC tem um ou mais grupos de segurança do Amazon VPC associados a ele. O Amazon VPC fornece um grupo de segurança da VPC chamado

padrão, criado automaticamente quando você cria a VPC. Cada cluster iniciado por você na VPC será associado automaticamente ao security group da VPC padrão se você não especificar um security group da VPC diferente ao criar o cluster. Você pode associar um security group da VPC a um cluster ao criar um cluster ou associar um security group da VPC depois modificando o cluster.

A tabela a seguir descreve as regras padrão do security group da VPC padrão.

| **Inbound** | | | |
|---|---|---|---|
| **Source** | **Protocol** | **Port Range** | **Comments** |
| The security group ID (sg-*xxxxxxxx*) | All | All | Allow inbound traffic from instances assigned to the same security group |
| **Outbound** | | | |
| **Destination** | **Protocol** | **Port Range** | **Comments** |
| 0.0.0.0/0 | All | All | Allow all outbound traffic |

Você pode alterar as regras para o grupo de segurança VPC padrão conforme necessário para seu cluster do Amazon Redshift.

Se o grupo de segurança da VPC padrão for suficiente, você não precisará criar mais. Porém, você também pode criar os security groups da VPC adicionais para gerenciar melhor o acesso de entrada ao cluster. Por exemplo, suponha que você esteja executando um serviço em um cluster do Amazon Redshift e tenha vários níveis de serviço diferentes que fornece aos seus clientes. Se não quiser conceder o mesmo acesso em todos os níveis de serviço, você poderá criar grupos de segurança da VPC separados, um para cada nível de serviço. Em seguida, você poderá associar esses security groups da VPC ao cluster.

É possível criar até 100 grupos de segurança de VPC para uma VPC e associar um grupo de segurança de VPC a muitos clusters. No entanto, só é possível associar até cinco grupos de segurança de VPC a um determinado cluster.

O Amazon Redshift aplica as alterações a um grupo de segurança da VPC imediatamente. Assim, se você tiver associado o security group da VPC a um cluster, as regras de acesso ao cluster de entrada no security group da VPC atualizadas serão aplicadas imediatamente.

Você pode criar e modificar grupos de segurança da VPC em https://console.aws.amazon.com/vpc/. Você também pode gerenciar grupos de segurança da VPC programaticamente usando a AWS CLI, a CLI do Amazon EC2 e o AWS Tools for Windows PowerShell. Para obter mais informações sobre como trabalhar com grupos de segurança da VPC, consulte Grupos de segurança para sua VPC no Manual do usuário do Amazon VPC.

# Definir as configurações de comunicação do grupo de segurança para um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor

Este tópico ajuda você a configurar grupos de segurança para rotear e receber o tráfego de rede adequadamente. Veja abaixo alguns casos de uso comuns:

- Você ativa a acessibilidade pública para um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshfit sem servidor, mas ele não está recebendo tráfego. Para isso, é necessário configurar uma regra de entrada para permitir que o tráfego chegue pela internet.
- O cluster ou o grupo de trabalho não está acessível ao público e você usa o grupo de segurança da VPC padrão pré-configurado do Redshift a fim de permitir tráfego de entrada. No entanto, você precisa usar um grupo de segurança diferente do padrão, e esse grupo de segurança personalizado não permite tráfego de entrada. É necessário configurá-lo para permitir a comunicação.

As seções a seguir ajudam você a escolher a resposta correta para cada caso de uso e mostra como configurar o tráfego de rede de acordo com seus requisitos. Opcionalmente, você pode usar as etapas para configurar a comunicação de outros grupos de segurança privados.

> **Note**
>
> Na maioria dos casos, as configurações de tráfego de rede não são definidas automaticamente no Amazon Redshift. Isso ocorre porque eles podem variar consideravelmente, dependendo se a origem do tráfego é a internet ou um grupo de segurança privado, e porque os requisitos de segurança variam.

## Acessibilidade pública com configuração de grupo de segurança padrão ou personalizado

Se você estiver criando ou já tiver um cluster ou grupo de trabalho, execute as etapas de configuração a seguir para torná-lo acessível ao público. Isso se aplica tanto quando você escolhe o grupo de segurança padrão quanto um grupo de segurança personalizado:

1. Encontre as configurações de rede:

- Para um cluster provisionado do Amazon Redshift, escolha a guia Propriedades e, em Configurações de rede e segurança, selecione a VPC para o cluster.
- Para um grupo de trabalho do Amazon Redshift sem servidor, escolha Configuração do grupo de trabalho. Escolha o grupo de trabalho na lista. Em seguida, em Acesso a dados, no painel Rede e segurança, escolha Editar.

2. Configure o gateway da Internet e a tabela de rotas para a VPC. Você inicia a configuração escolhendo a VPC pelo nome. O painel da VPC é aberto. Para se conectar a um cluster ou um grupo de trabalho acessível ao público pela internet, um gateway da Internet deve estar associado à tabela de rotas. Você pode configurar isso escolhendo Tabelas de rotas no painel da VPC. Confirme se o destino do gateway da Internet está definido com a origem 0.0.0.0/0 ou um CIDR de IP público. A tabela de rotas deve estar associada à VPC em que o cluster reside. Para obter mais informações sobre como configurar o acesso à internet para uma VPC, conforme descrito aqui, consulte Habilitar acesso à Internet na documentação da Amazon VPC. Para obter mais informações sobre como configurar uma tabela de rotas, consulte Configurar tabelas de rotas.
3. Depois de configurar o gateway da Internet e a tabela de rotas, retorne às configurações de rede do Redshift. Abra o acesso de entrada escolhendo o grupo de segurança e, em seguida, selecionando as Regras de entrada. Escolha Editar regras de entrada.
4. Escolha o Protocolo e a Porta para a regra de entrada, de acordo com seus requisitos, para permitir o tráfego de clientes. Para um cluster RA3, selecione uma porta dentro dos intervalos 5431-5455 ou 8191-8215. Quando terminar, salve cada regra.
5. Edite a configuração Publicamente acessível para habilitá-la. É possível fazer isso pelo menu Ações do cluster ou do grupo de trabalho.

Quando você ativa a configuração de acesso público, o Redshift cria um endereço IP elástico. É um endereço IP estático associado à sua conta da AWS. Clientes fora da VPC podem usá-lo para se conectar.

Para obter mais informações sobre como configurar o grupo de segurança, consulte Grupos de segurança de clusters do Amazon Redshift.

Você pode testar suas regras conectando-se a um cliente. Faça o que está descrito a seguir se estiver se conectando ao Amazon Redshift sem servidor. Depois de concluir a configuração da rede, conecte-se à ferramenta do cliente, como o Amazon Redshift RSQL. Usando seu domínio do Amazon Redshift Serverless como host, insira o seguinte:

```
rsql -h workgroup-name.account-id.region.amazonaws.com -U admin -d dev -p 5439
```

## Acessibilidade privada com configuração de grupo de segurança padrão ou personalizado

Quando você não se comunica pela internet com o cluster ou grupo de trabalho, isso é chamado de acesso privado. Se você escolheu o grupo de segurança padrão ao criá-lo, o grupo de segurança inclui as seguintes regras de comunicação padrão:

- Uma regra de entrada que permite tráfego de todos os recursos atribuídos a esse grupo de segurança.
- Uma regra de saída que permite todo tráfego de saída. O destino dessa regra é 0.0.0.0/0. Na notação de Encaminhamento Entre Domínios Sem Classificação (CIDR), ele representa todos os endereços IP possíveis.

Você pode visualizar as regras no console selecionando o grupo de segurança para o cluster ou grupo de trabalho.

Se o cluster, o grupo de trabalho e o cliente usarem o grupo de segurança padrão, não será necessária nenhuma configuração adicional para permitir o tráfego de rede. Mas, se você excluir ou alterar alguma regra no grupo de segurança padrão do Redshift ou do cliente, isso não se aplicará mais. Nesse caso, você deve configurar regras para permitir a comunicação de entrada e saída. Uma configuração de grupo de segurança comum é a seguinte:

- Para uma instância do Amazon EC2 do cliente:
  - Uma regra de entrada que permite o endereço IP do cliente.
  - Uma regra de saída que permite o intervalo de endereços IP (bloco CIDR) de todas as sub-redes fornecidas para uso do Redshift. Ou você pode especificar 0.0.0.0/0, que são todos os intervalos de endereços IP.
- Para o cluster ou grupo de trabalho do Redshift:
  - Uma regra de entrada que permite o grupo de segurança do cliente.
  - Uma regra de saída que permite tráfego para 0.0.0.0/0. Normalmente, uma regra de saída permite todo tráfego de saída. Opcionalmente, você pode adicionar uma regra de saída para permitir o tráfego para o grupo de segurança do cliente. Nesse caso opcional, uma regra de saída nem sempre é necessária, porque o tráfego de resposta de cada solicitação pode chegar

à instância. Para obter mais detalhes sobre o comportamento de solicitações e respostas, consulte Grupos de segurança no Manual do usuário do Amazon VPC.

Se você alterar a configuração de qualquer sub-rede ou grupo de segurança especificado para uso do Redshift, talvez seja necessário alterar as regras de tráfego adequadamente para manter a comunicação aberta. Para obter mais informações sobre a criação de regras de entrada e saída, consulte Blocos CIDR da VPC no Manual do usuário do Amazon VPC. Para obter informações sobre como se conectar ao Amazon Redshift sem servidor, consulte Configurar conexões no Amazon Redshift.

## Como o Amazon Redshift funciona com o compartilhamento de VPC para recursos da AWS

O compartilhamento de VPC permite que você crie recursos de aplicações da AWS, como instâncias do Amazon EC2 e outros serviços da AWS, em uma nuvem privada virtual (VPC). A conta que possui a VPC (a proprietária) compartilha uma ou mais sub-redes com outras contas (participantes) que pertencem à mesma organização da AWS. Isso descreve como você pode criar e usar um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor em uma VPC compartilhada.

Os benefícios do compartilhamento de VPC incluem que você não precisa gerenciar tantas VPCs e isso pode ajudar a simplificar sua rede. O benefício específico para administradores e usuários do Amazon Redshift é que os recursos do Redshift podem operar de forma produtiva na VPC compartilhada. Para obter mais informações sobre o compartilhamento de VPC, consulte Compartilhar sua VPC com outras contas, que dá mais detalhes sobre os benefícios do compartilhamento de VPC e como ele funciona.

### Como usar os recursos de data warehouse do Amazon Redshift em uma VPC compartilhada

Em primeiro lugar, é importante entender que um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor não pode ficar visível para os participantes em uma sub-rede compartilhada. Mas isso não impede que os participantes trabalhem com o banco de dados do proprietário em uma VPC compartilhada. Isso é mais bem detalhado nas etapas a seguir.

Antes de criar um cluster provisionado do Amazon Redshift em uma VPC compartilhada, você deve criar um grupo de sub-redes que pretende usar para o Amazon Redshift. Isso deve incluir as sub-redes da VPC compartilhada que você deseja usar. Ao criar o cluster do Amazon Redshift, você

deve escolher essa sub-rede e especificar o grupo de segurança da VPC compartilhada. Da mesma forma, você precisa especificar as sub-redes compartilhadas e o grupo de segurança que criou na VPC compartilhada ao criar o grupo de trabalho e o banco de dados Amazon Redshift sem servidor. Depois de configurar as sub-redes, execute estas etapas para configurar os recursos do Redshift no ambiente compartilhado:

1. O proprietário da VPC cria um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor, usando uma sub-rede na VPC compartilhada.
2. O proprietário da VPC disponibiliza o cluster ou o grupo de trabalho em um cenário entre VPCs. As etapas são descritas em Trabalhando com endpoints da VPC gerenciados por Redshift no Amazon Redshift para um cluster provisionado ou em Conexão com o Amazon Redshift Serverless por um endpoint da VPC gerenciado pelo Amazon Redshift para o Amazon Redshift sem servidor. Ao habilitar a disponibilidade entre VPCs, o banco de dados pode ser disponibilizado para os usuários na mesma conta da AWS ou em outras contas.
3. Entretanto, com o compartilhamento de VPCs, um proprietário pode compartilhar uma sub-rede com um participante, e este pode criar um cluster do Amazon Redshift ou um grupo de trabalho Amazon Redshift sem servidor na sub-rede. No entanto, nesse caso, o proprietário não pode visualizar um recurso do Amazon Redshift criado por um participante. O cluster ou grupo de trabalho deve ser disponibilizado habilitando a disponibilidade entre VPCs da mesma forma descrita na etapa anterior.

## Notas de uso dos recursos do Amazon Redshift em uma VPC compartilhada

Observe os seguintes comportamentos em relação ao uso do Amazon Redshift em uma sub-rede compartilhada:

- Conforme detalhado na seção anterior, o proprietário da VPC não pode compartilhar um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor com um participante por meio do compartilhamento de VPC. No entanto, o participante pode criar um cluster ou grupo de trabalho do Amazon Redshift sem servidor na sub-rede do proprietário. Nesse caso, por meio do compartilhamento de VPCs, o Amazon Redshift não é visível para o proprietário.
- O proprietário da VPC não pode visualizar, atualizar ou excluir um cluster provisionado do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor que o participante cria na sub-rede compartilhada.
- Não há permissões disponíveis para que outra conta da AWS possa acessar os recursos do Amazon Redshift que você cria na VPC compartilhada.

# Grupos de sub-rede de cluster do Amazon Redshift

## Visão geral

Crie um grupo de sub-redes de clusters se estiver disponibilizando seu cluster na nuvem privada virtual (VPC). Para obter mais informações sobre VPC, consulte a página de detalhes do produto Amazon VPC.

Sua VPC pode ter uma ou mais sub-redes, um subconjunto de endereços IP dentro da VPC, que permite o agrupamento de recursos com base nas necessidades operacionais e de segurança. O grupo de sub-redes de clusters permite que você especifique um conjunto de sub-redes em sua VPC. Ao provisionar um cluster, você fornece o grupo de sub-redes e o Amazon Redshift cria o cluster em uma das sub-redes do grupo.

Para obter mais informações sobre como criar uma VPC, acesse a documentação Manual do usuário do Amazon VPC.

Após ter criado um grupo de sub-redes, é possível remover as sub-redes adicionadas anteriormente ou adicionar mais sub-redes. O Amazon Redshift fornece operações de API para a criação, modificação ou exclusão de um grupo de sub-redes de clusters. Essas operações também podem ser executadas no console.

## Gerenciamento de grupos de sub-redes de cluster usando o console

Você pode gerenciar seus grupos de sub-rede de cluster usando o console do Amazon Redshift. Você pode criar, gerenciar ou excluir um grupo de sub-redes de clusters. Para todas as tarefas, comece a partir da lista de grupos de sub-redes de clusters. Você deve selecionar um grupo de sub-redes de clusters para gerenciar.

É possível provisionar um cluster em uma das sub-redes fornecidas no grupo de sub-redes. O grupo de sub-redes do cluster permite que você especifique um conjunto de sub-redes em sua nuvem privada virtual (VPC).

Criação de um grupo de sub-redes de clusters

É preciso ter pelo menos um grupo de sub-redes de clusters definido para disponibilizar um cluster em uma VPC.

Para criar um grupo de sub-redes de clusters

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Configurations (Configurações) e Subnet groups (Grupos de sub-redes). A lista de grupos de sub-redes é exibida.
3. Choose Create cluster subnet group (Criar grupo de sub-redes do cluster) para exibir a página de criação.
4. Insira informações para o grupo de sub-redes incluindo as sub-redes a serem adicionadas.
5. Escolha Create cluster subnet group (Criar grupo de sub-redes do cluster) para criar o grupo com a sub-redes escolhidas.

Modificação de um grupo de sub-redes de clusters

Para modificar um grupo de sub-redes de clusters

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Configurations (Configurações) e Subnet groups (Grupos de sub-redes). A lista de grupos de sub-redes é exibida.
3. Escolha o grupo de sub-redes a ser modificado.
4. Em Actions (Ações), escolha Modify (Modificar) para exibir os detalhes do grupo de sub-redes.
5. Atualize as informações do grupo de sub-redes.
6. Escolha Save (Salvar) para modificar o grupo.

Em alguns casos, são necessárias etapas adicionais para alterar ou remover sub-redes. Por exemplo, o artigo Como faço para mover um cluster provisionado do Amazon Redshift para uma sub-rede diferente? do Centro de Conhecimentos da AWS descreve um caso de uso que abrange a movimentação de um cluster.

Exclusão de um grupo de sub-redes de clusters

Não é possível excluir um grupo de sub-redes de cluster que esteja sendo usado por um cluster.

Para excluir um grupo de sub-redes de clusters

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Configurations (Configurações) e Subnet groups (Grupos de sub-redes). A lista de grupos de sub-redes é exibida.
3. Escolha o grupo de sub-redes a ser excluído e escolha Delete (Excluir).

### Gerenciar grupos de sub-rede de cluster usando a AWS CLI e a API do Amazon Redshift

Você pode usar as seguintes operações da CLI do Amazon Redshift para gerenciar grupos de sub-redes de cluster.

- create-cluster-subnet-group
- delete-cluster-subnet-group
- describe-cluster-subnet-groups
- modify-cluster-subnet-group

Você pode usar as seguintes operações de API do Amazon Redshift para gerenciar grupos de sub-rede de cluster.

- CreateClusterSubnetGroup
- DeleteClusterSubnetGroup
- DescribeClusterSubnetGroups
- ModifyClusterSubnetGroup

## Histórico das versões de cluster

O Amazon Redshift lança periodicamente novas versões de cluster que são usadas para atualizar seu cluster.

**Important**

Para obter informações sobre as versões disponíveis de cluster do Amazon Redshift, bem como os respectivos recursos, melhorias e correções, consulte Versões de cluster para o Amazon Redshift.

# Trabalho com Integrações ETL zero

Este tópico inclui a documentação de pré-lançamento para Integrações ETL zero do Aurora PostgreSQL e do RDS for MySQL com Amazon Redshift, que estão na versão de visualização. A documentação e os recursos estão sujeitos a alterações. Só é recomendável usar integrações ETL zero do RDS for MySQL e do Aurora PostgreSQL em ambientes de teste, e não em ambientes de produção. Para conferir os termos e condições da pré-visualização, consulte Betas e pré-visualizações nos Termos de serviços da AWS.

A Integração ETL zero é uma solução totalmente gerenciada que disponibiliza dados transacionais ou operacionais no Amazon Redshift quase em tempo real. Com essa solução, é possível configurar uma integração da fonte com um data warehouse do Amazon Redshift. Você não precisa manter um pipeline de extração, transformação e carregamento (ETL). Cuidamos do ETL para você automatizando a criação e o gerenciamento da replicação de dados da fonte de dados para o cluster do Amazon Redshift ou o namespace do Redshift Serverless. É possível continuar atualizando e consultando os dados de origem e, ao mesmo tempo, usar o Amazon Redshift em workloads analíticos, como relatórios e painéis.

As seguintes origens são atualmente compatíveis com integrações ETL zero:

- Aurora MySQL-Compatible Edition
- Aurora PostgreSQL-Compatible Edition (visualização)
- RDS for MySQL (visualização)

Para criar uma integração ETL zero, você especifica uma origem de integração e um data warehouse do Amazon Redshift como o destino. A integração replica dados do data warehouse de origem para o data warehouse de destino. Os dados permanecem disponíveis no Amazon Redshift em questão de segundos. A integração monitora a integridade do pipeline de dados e se recupera de problemas quando possível. É possível criar integrações de fontes do mesmo tipo em um único data warehouse do Amazon Redshift para derivar insights holísticos em várias aplicações.

Com os dados no Amazon Redshift, é possível usar a análise fornecida pelo Amazon Redshift. Por exemplo, machine learning (ML) integrado, visões materializadas, compartilhamento de dados e acesso direto a vários armazenamentos de dados e data lakes. Como uma integração ETL zero mantém os recursos de computação isolados dos recursos de dados, você está usando as

ferramentas mais eficientes para processar dados. Para engenheiros de dados, a Integração ETL zero dá acesso a dados urgentes que, do contrário, podem ser atrasados por erros intermitentes em pipelines de dados complexos. É possível executar consultas analíticas e modelos ML em dados transacionais para obter insights quase em tempo real de eventos urgentes e decisões comerciais.

É possível criar uma assinatura de notificação de evento do Amazon Redshift, de maneira que você receba uma notificação quando um evento ocorre para uma determinada integração ETL zero. Para exibir a lista de notificações de eventos relacionadas à integração, consulte Notificações de evento da integração ETL zero com o Amazon EventBridge. A maneira mais simples de criar uma assinatura é com o console do Amazon SNS. Para obter informações sobre como criar um tópico do Amazon SNS e assiná-lo, consulte Getting started with Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

Ao começar a usar integrações ETL zero, considere os seguintes conceitos:

- Um banco de dados de origem é o banco de dados no qual os dados são replicados para o Amazon Redshift.
- Um data warehouse de destino é o cluster provisionado do Amazon Redshift ou o grupo de trabalho do Redshift Serverless no qual os dados são replicados.
- Um banco de dados de destino é o banco de dados criado por você a partir de uma integração ETL zero no data warehouse de destino.

Você pode monitorar as integrações ETL zero consultando exibições específicas do sistema no Amazon Redshift.

- SVV_INTEGRATION fornece informações sobre detalhes de configuração das integrações ETL zero.
- SYS_INTEGRATION_ACTIVITY fornece informações sobre integrações ETL zero concluídas.
- SVV_INTEGRATION_TABLE_STATE fornece informações sobre o estado da integração.
- SYS_INTEGRATION_TABLE_STATE_CHANGE fornece informações sobre o log de alteração do estado da tabela para integrações.

Para obter informações sobre preços de integrações ETL zero, consulte a página de preços indicada:

- Preços do Amazon Redshift
- Preço do Amazon Aurora

- Preços do Amazon RDS

Para obter mais informações sobre origens de integração ETL zero, consulte os seguintes tópicos:

- Para integrações ETL zero do Aurora, consulte Benefits, Key concepts, Limitations, Quotas e Supported Regions de integrações ETL zero no Guia do usuário do Amazon Aurora.
- Para integrações ETL zero do RDS, consulte Benefits, Key concepts, Limitations, Quotas e Supported Regions de integrações ETL zero no Guia do usuário do Amazon RDS.

Tópicos


- Considerações ao usar integrações ETL zero com o Amazon Redshift
- Conceitos básicos das integrações ETL zero
- Criar bancos de dados de destino no Amazon Redshift
- Consulta e criação de visões materializadas com dados replicados
- Gerenciamento de integrações ETL zero
- Métricas para integrações ETL zero
- Solução de problemas em integrações ETL zero


# Considerações ao usar integrações ETL zero com o Amazon Redshift

As considerações a seguir se aplicam a integrações ETL zero com o Amazon Redshift.

- O data warehouse de destino do Amazon Redshift deve atender aos seguintes pré-requisitos:
  - Execução do Amazon Redshift sem servidor ou de um tipo de nó RA3 (ra3.16xlarge, ra3.4xlarge e ra3.xlplus).
  - Ser criptografado (se estiver usando um cluster provisionado).
  - Ter a diferenciação entre maiúsculas e minúsculas habilitada.
- Não é possível habilitar o suporte avançado da VPC em data warehouses com integrações configuradas.
- Se você excluir uma origem de integração autorizada para um data warehouse do Amazon Redshift, todas as integrações associadas entrarão no estado `FAILED`.

- Não é possível excluir um data warehouse do Amazon Redshift que já tenha Integrações ETL zero. É necessário excluir todas as integrações correspondentes primeiro.
- Você deve primeiro excluir todas as integrações associadas a um banco de dados de destino antes de excluir o banco de dados de destino.
- O banco de dados de destino é somente leitura. Não é possível criar tabelas, visualizações ou visões materializadas no banco de dados de destino. No entanto, é possível usar visões materializadas em outras tabelas no data warehouse de destino.
- As visões materializadas são compatíveis quando usadas em consultas entre bancos de dados. A atualização de visões materializadas com dados replicados de integrações ETL zero leva a uma atualização completa da exibição. Atualização incremental, regravação automática de consultas, atualização automática e visões materializadas automatizadas não são compatíveis. Para obter informações sobre como criar visões materializadas com dados replicados por meio de integrações ETL zero, consulte Criação de visões materializadas com dados replicados.
- Só é possível consultar tabelas no data warehouse de destino que estejam no estado `Synced`. Para ter mais informações, consulte Métricas para integrações ETL zero.
- As integrações ETL zero não são compatíveis em data warehouses de destino configurados para implantação multi-AZ.
- O redimensionamento clássico não é compatível com clusters provisionados com integração ETL zero. A execução dessa operação fará com que a integração entre no estado `FAILED`.
- Como só aceita caracteres UTF-8, talvez o Amazon Redshift não respeite o agrupamento definido na origem. As regras de classificação e comparação podem ser diferentes, o que pode, em última análise, alterar os resultados da consulta.
- As tabelas na fonte de integração devem ter uma chave primária. Caso contrário, as tabelas não poderão ser replicadas no data warehouse de destino no Amazon Redshift.
- Para integrações ETL zero do Aurora PostgreSQL e do RDS for MySQL com o Amazon Redshift, crie o data warehouse de destino em Visualização. Para ter mais informações, consulte Criar e configurar um data warehouse do Amazon Redshift de destino.

Para considerações que também se apliquem à origem da integração, consulte um dos seguintes tópicos:

- Para origens do Aurora, consulte Limitations no Guia de usuário do Amazon Aurora.
- Para origens do Aurora, consulte Limitations no Guia de usuário do Amazon RDS.

# Conceitos básicos das integrações ETL zero

Antes de configurar a integração ETL zero no Amazon Redshift, configure a origem de integração e o configure com as permissões e os parâmetros necessários. Depois, prossiga com a configuração inicial restante na AWS CLI e no console do Amazon Redshift.

Para criar uma integração ETL zero do Aurora com o Amazon Redshift

Para criar uma integração ETL zero do Aurora com o Amazon Redshift, faça o seguinte:

1. No console do Amazon RDS, crie um grupo de parâmetros do cluster do banco de dados personalizado conforme descrito no Guia do usuário do Amazon Aurora.
2. No console do Amazon RDS, crie um cluster do banco de dados do Amazon Aurora de origem conforme descrito no Guia do usuário do Amazon Aurora.
3. No console do Amazon Redshift: Criar e configurar um data warehouse do Amazon Redshift de destino.
   - Na AWS CLI ou no console do Amazon Redshift: Ative a diferenciação entre letras maiúsculas e minúsculas no data warehouse.
   - No console do Amazon Redshift: Configurar a autorização para o data warehouse do Amazon Redshift.
4. No console do Amazon RDS, crie uma integração ETL zero, conforme descrito no Guia do usuário do Amazon Aurora.
5. No console do Amazon Redshift ou no editor de consultas v2, crie um banco de dados do Amazon Redshift a partir da integração.

   Em seguida, consulte e crie visões materializadas com dados replicados.

Para criar uma integração ETL zero do RDS com o Amazon Redshift

Para criar uma integração ETL zero do RDS com o Amazon Redshift, faça o seguinte:

1. No console do Amazon RDS, crie um grupo de parâmetros do banco de dados personalizado conforme descrito no Guia do usuário do Amazon Aurora.
2. No console do Amazon RDS, crie uma instância do Amazon RDS de origem conforme descrito no Guia do usuário do Amazon Aurora.
3. No console do Amazon Redshift: Criar e configurar um data warehouse do Amazon Redshift de destino.

- Na AWS CLI ou no console do Amazon Redshift: Ative a diferenciação entre letras maiúsculas e minúsculas no data warehouse.
- No console do Amazon Redshift: Configurar a autorização para o data warehouse do Amazon Redshift.

4. No console do Amazon RDS, crie uma integração ETL zero conforme descrito no Guia do usuário do Amazon RDS.
5. No console do Amazon Redshift ou no editor de consultas v2, crie um banco de dados do Amazon Redshift a partir da integração.

   Em seguida, consulte e crie visões materializadas com dados replicados.

O console do Amazon RDS oferece um fluxo de criação da integração passo a passo, no qual você especifica o banco de dados de origem e o data warehouse de destino do Amazon Redshift. Se ocorrerem problemas, você poderá optar por fazer o Amazon RDS corrigir os problemas, em vez de corrigi-los manualmente no console do Amazon RDS ou do Amazon Redshift.

## Criar e configurar um data warehouse do Amazon Redshift de destino

Antes dessa etapa, crie a fonte de integração e configure parâmetros exigidos pelo tipo da fonte para integrações ETL zero.

Nesta etapa, você cria e configura um data warehouse do Amazon Redshift de destino, como um grupo de trabalho do Redshift Serverless ou um cluster provisionado.

O data warehouse de destino deve ter as seguintes características:

- Executar o Amazon Redshift sem servidor ou um cluster provisionado do tipo de instância ra3.16xlarge, ra3.4xlarge ou ra3.xlplus.
- Diferenciar letras maiúsculas de minúsculas (`enable_case_sensitive_identifier`). Para ter mais informações, consulte Ative a diferenciação entre letras maiúsculas e minúsculas no data warehouse.
- Criptografado, se o data warehouse de destino for um cluster provisionado pelo Amazon Redshift. Para ter mais informações, consulte Criptografia de banco de dados do Amazon Redshift.
- Criado na mesma região da AWS da origem da integração.

> **Note**
>
> Para integrações ETL zero do Aurora PostgreSQL e do RDS for MySQL com o Amazon Redshift, considere também o seguinte para o data warehouse de destino.
>
> - Você deve criar o data warehouse na Pré-visualização na faixa `preview_2023`. Não é possível usar recursos de visualização em produção nem mover o data warehouse de visualização para uma implantação de produção.
> - Se você optar por criar um cluster provisionado pelo Amazon Redshift, esse cluster deverá ter pelo menos dois nós.
> - Para origens do Aurora PostgreSQL, você deve criar o data warehouse de destino na região Leste dos EUA (Ohio) da AWS. Você deve criar o banco de dados de origem para integrações ETL zero do Aurora PostgreSQL usando o Ambiente de Pré-visualização do Banco de Dados do Amazon RDS.
>
>   Para origens do RDS for MySQL, você deve criar o data warehouse de destino em uma região da AWS compatível. Para obter uma lista das regiões da AWS onde as integrações ETL zero do RDS for MySQL estão disponíveis, consulte Supported Regions for zero-ETL integrations with Amazon Redshift no Guia do usuário do Amazon RDS.
>
> Para criar o data warehouse de destino em Pré-visualização das integrações ETL zero do Aurora PostgreSQL e do RDS for MySQL, consulte um dos seguintes tópicos, dependendo do tipo de implantação:
>
> - Para criar um cluster provisionado pelo Amazon Redshift de visualização, consulte Criar cluster de visualização prévia. Escolha a trilha `preview_2023` para usar Integrações ETL zero.
> - Para criar um grupo de trabalho do Amazon Redshift sem servidor de visualização, consulte Criar visualização prévia de grupo de trabalho.

Para criar o data warehouse de destino para as integrações ETL zero do Aurora MySQL, consulte um dos seguintes tópicos, dependendo do tipo de implantação:

- Para criar um cluster provisionado pelo Amazon Redshift, consulte Criar um cluster.
- Para criar um grupo de trabalho do Amazon Redshift sem servidor com um namespace, consulte Criar um grupo de trabalho com um namespace.

Quando você cria um cluster provisionado, o Amazon Redshift também cria um grupo de parâmetros padrão. Não é possível editar o grupo de parâmetros padrão. No entanto, é possível criar um grupo de parâmetros personalizado antes de criar um novo cluster e depois associá-lo ao cluster. Também é possível editar o grupo de parâmetros que será associado ao cluster criado. Você também deve ativar a diferenciação entre letras maiúsculas e minúsculas ao criar o grupo de parâmetros personalizado ou ao editar um atual para usar integrações ETL zero.

É possível criar um grupo de parâmetros personalizado usando a AWS CLI ou o console do Amazon Redshift da seguinte maneira:

- Com o console do Amazon Redshift: Gerenciamento de grupos de parâmetros usando o console
- Uso da AWS CLI: Gerenciar grupos de parâmetros usando a AWS CLI e a API do Amazon Redshift

## Ative a diferenciação entre letras maiúsculas e minúsculas no data warehouse

É possível anexar um grupo de parâmetros e habilitar a diferenciação de letras maiúsculas e minúsculas para um cluster provisionado durante a criação. No entanto, só será possível atualizar um grupo de trabalho de tecnologia sem servidor por meio do AWS Command Line Interface (AWS CLI) depois que ele tiver sido criado. Isso é exigido para dar suporte à diferenciação de letras maiúsculas e minúsculas do MySQL e do PostgreSQL. `enable_case_sensitive_identifier` é um valor de configuração que determina se identificadores de nome de bancos de dados, tabelas e colunas diferenciam letras maiúsculas e minúsculas. Esse parâmetro deve ser ativado para criar Integrações ETL zero no data warehouse. Para obter mais informações, consulte enable_case_sensitive_identifier.

Para o Amazon Redshift sem servidor: Ativar a diferenciação de letras maiúsculas e minúsculas para o Amazon Redshift sem servidor usando a AWS CLI. Só é possível ativar a diferenciação de letras maiúsculas e minúsculas para o Amazon Redshift sem servidor por meio da AWS CLI.

Para clusters provisionados pelo Amazon Redshift, habilite a distinção entre maiúsculas e minúsculas para o cluster de destino usando um dos seguintes tópicos:

- Ativar a diferenciação entre letras maiúsculas e minúsculas para clusters provisionados pelo Amazon Redshift usando o console do Amazon Redshift
- Ativar a diferenciação de letras maiúsculas e minúsculas para clusters provisionados pelo Amazon Redshift usando a AWS CLI

## Ativar a diferenciação de letras maiúsculas e minúsculas para o Amazon Redshift sem servidor usando a AWS CLI

Execute o comando AWS CLI para ativar a diferenciação entre letras maiúsculas e minúsculas para o grupo de trabalho.

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

Aguarde até que o status do grupo de trabalho seja `Active` para passar à próxima etapa.

## Ativar a diferenciação entre letras maiúsculas e minúsculas para clusters provisionados pelo Amazon Redshift usando o console do Amazon Redshift

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No painel de navegação à esquerda, escolha Painel de clusters provisionados.
3. Escolha o cluster provisionado no qual você deseja replicar os dados.
4. No painel de navegação à esquerda, escolha Configurações > Gerenciamento de workloads.
5. Na página de gerenciamento de workloads, escolha o grupo de parâmetros.
6. Selecione a guia Parâmetros.
7. Escolha Editar parâmetros e altere enable_case_sensitive_identifier para verdadeiro.
8. Selecione Salvar.

## Ativar a diferenciação de letras maiúsculas e minúsculas para clusters provisionados pelo Amazon Redshift usando a AWS CLI

1. Como não é possível editar o grupo de parâmetros padrão, no programa de terminal, execute o comando AWS CLI a seguir para criar um grupo de parâmetros personalizado. Posteriormente, você vai associá-lo ao cluster provisionado.

   ```
   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. Execute o comando AWS CLI a seguir para ativar a diferenciação entre letras maiúsculas e minúsculas para o grupo de parâmetros.

```
aws redshift modify-cluster-parameter-group \
    --parameter-group-name zero-etl-params \
    --parameters ParameterName=enable_case_sensitive_identifier,ParameterValue=true
```

3. Execute o comando a seguir para associar o grupo de parâmetros ao cluster.

```
aws redshift modify-cluster \
    --cluster-identifier target-cluster \
    --cluster-parameter-group-name zero-etl-params
```

4. Aguarde até que o cluster provisionado esteja disponível. É possível verificar o status do cluster usando o comando `describe-cluster`. Depois, execute o comando a seguir para reiniciar o cluster.

```
aws redshift reboot-cluster \
    --cluster-identifier target-cluster
```

## Configurar a autorização para o data warehouse do Amazon Redshift

Para replicar dados da origem da integração para o data warehouse do Amazon Redshift, você deve adicionar estas duas entidades inicialmente:

- Entidade principal autorizada: identifica o usuário ou a função que pode criar Integrações ETL zero no data warehouse.
- Fonte de integração autorizada: identifica o banco de dados de origem capaz de atualizar o data warehouse.

É possível configurar entidades principais e fontes de integração autorizadas na guia Política de recursos no console do Amazon Redshift ou usando a operação de API `PutResourcePolicy` do Amazon Redshift.

## Adicionar entidades principais autorizadas

Para criar uma Integração ETL zero no grupo de trabalho ou cluster provisionado do Redshift sem servidor, autorize o acesso ao namespace associado ou ao cluster provisionado.

Você poderá pular essa etapa se as duas condições abaixo forem verdadeiras:

- A Conta da AWS que detém o grupo de trabalho ou o cluster provisionado do Redshift Serverless também detém o banco de dados de origem.
- Essa entidade principal está associada a uma política do IAM baseada em identidade com permissões para criar Integrações ETL zero nesse namespace ou cluster provisionado do Redshift sem servidor.

Adicionar entidades principais autorizadas a um namespace do Amazon Redshift sem servidor

1. No console do Amazon Redshift, no painel de navegação à esquerda, escolha Redshift Serverless.
2. Escolha Configuração do namespace, o namespace e vá até a guia Política de recursos.
3. Escolha Adicionar as entidades principais autorizadas.
4. Para cada entidade principal autorizada que você deseja adicionar, insira no namespace o ARN do usuário ou da função da AWS, ou o ID da conta da Conta da AWS à qual você deseja conceder acesso para criar integrações ETL zero. O ID da conta é armazenado como um ARN.
5. Escolha Salvar alterações.

Adicionar entidades principais autorizadas a um cluster provisionado do Amazon Redshift

1. No console do Amazon Redshift, no painel de navegação à esquerda, escolha Painel de clusters provisionados.
2. Escolha Clusters, o cluster e vá até a guia Política de recursos.
3. Escolha Adicionar as entidades principais autorizadas.
4. Para cada entidade principal autorizada que você deseja adicionar, insira no cluster o ARN do usuário ou da função da AWS, ou o ID da conta da Conta da AWS à qual você deseja conceder acesso para criar integrações ETL zero. O ID da conta é armazenado como um ARN.
5. Escolha Salvar alterações.

## Adicionar fontes de integração autorizadas

Para permitir que a origem atualize o data warehouse do Amazon Redshift, você deve adicioná-lo como uma fonte de integração autorizada ao namespace.

Adicionar uma fonte de integração autorizada a um namespace do Amazon Redshift sem servidor

1. No console do Amazon Redshift, acesse Painel do Serverless.
2. Escolha o nome do namespace.
3. Vá até a guia Política de recursos.
4. Selecione Adicionar a origem de integração autorizada.
5. Especifique o ARN da origem para a integração ETL zero.

> **Note**
>
> A remoção de uma fonte de integração autorizada impede que os dados se repliquem no namespace. Essa ação desativa todas as integrações ETL zero dessa origem nesse namespace.

Adicionar uma fonte de integração autorizada a um cluster provisionado do Amazon Redshift

1. No console do Amazon Redshift, acesse o Painel de clusters provisionados.
2. Escolha o nome do cluster provisionado.
3. Vá até a guia Política de recursos.
4. Selecione Adicionar a origem de integração autorizada.
5. Especifique o ARN da origem que é a fonte de dados para a integração ETL zero.

> **Note**
>
> A remoção de uma fonte de integração autorizada impede que os dados se repliquem no cluster provisionado. Essa ação desativa todas as integrações ETL zero dessa origem no cluster provisionado pelo Amazon Redshift.

## Configurar autorização usando a API do Amazon Redshift

É possível usar as operações de API do Amazon Redshift para configurar políticas de recurso que funcionem com integrações ETL zero.

Para controlar a fonte capaz de criar uma integração de entrada no namespace, crie uma política de recurso e a anexe ao namespace. Com a política de recurso, é possível especificar a fonte com acesso à integração. A política de recursos é anexada ao namespace do data warehouse de destino para permitir que a fonte crie uma integração de entrada a fim de replicar dados ativos da fonte para o Amazon Redshift.

Esta é uma política de recurso de exemplo.

```
{
  "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"
    }
  ]
}
```

Isto resume as operações de API do Amazon Redshift aplicáveis à configuração de políticas de recurso para integrações:

- Use a operação da API PutResourcePolicy para manter a política de recurso. Quando você fornece outra política de recurso, a política de recurso anterior no recurso é substituída. Use a política de recurso do exemplo anterior, que concede permissões para as seguintes ações:
  - `CreateInboundIntegration`: permite que a entidade principal de origem crie uma integração de entrada para que os dados sejam replicados da origem para o data warehouse de destino.
  - `AuthorizeInboundIntegration`: permite que o Amazon Redshift valide continuamente se o data warehouse de destino pode receber dados replicados do ARN de origem.
- Use a operação da API getResourcePolicy para exibir políticas de recursos existentes.
- Use a operação da API DeleteResourcePolicy para remover uma política do recurso.

Para atualizar uma política de recurso, também é possível usar o comando put-resource-policy da AWS CLI.

### Próximas etapas

Agora que configurou a autorização para o data warehouse de destino do Amazon Redshift, você pode criar uma Integração ETL zero e começar a replicar dados.

Dependendo da origem, faça o seguinte:

- Para criar integrações ETL zero do Aurora, consulte Creating Amazon Aurora zero-ETL integrations with Amazon Redshift no Guia o Usuário do Amazon Aurora.
- Para criar integrações ETL zero do RDS, consulte Creating Amazon RDS zero-ETL integrations with Amazon Redshift no Guia o Usuário do Amazon RDS.

## Criar bancos de dados de destino no Amazon Redshift

Para replicar dados da origem para o Amazon Redshift, você deve criar um banco de dados a partir da integração no Amazon Redshift.

Conecte-se ao grupo de trabalho ou ao cluster provisionado do Redshift Serverless de destino e crie um banco de dados com uma referência ao identificador de integração. Esse identificador é o valor retornado para `integration_id` quando você consulta a visualização SVV_INTEGRATION.

> **Important**
>
> Para criar um banco de dados a partir da integração, a integração ETL zero deve ser criada e estar no estado `Active` no console do Amazon RDS ou do Amazon Redshift.

## Criação de um banco de dados de destino no Amazon Redshift

Para começar a replicar dados da origem para o Amazon Redshift, você deve crie um banco de dados a partir da integração no Amazon Redshift. Você pode criar o banco de dados usando o console do Amazon Redshift ou o editor de consultas v2.

### Criação de um banco de dados de destino usando o console do Amazon Redshift

1. No painel de navegação à esquerda, escolha Integrações ETL zero.
2. Escolha uma integração na lista.
3. Se estiver usando um cluster provisionado, você deverá primeiramente se conectar ao banco de dados. Escolha Connect to database (Conectar ao banco de dados). É possível se conectar usando uma conexão recente ou criando uma.
4. Para criar um banco de dados com base na integração, escolha Criar banco de dados com base na integração.
5. Insira um Database name (Nome do banco de dados). O ID de integração e o nome do data warehouse são pré-preenchidos.

   Para fontes do Aurora PostgreSQL, também insira o banco de dados nomeado especificado por você ao criar a integração ETL zero.
6. Selecione Criar banco de dados.

### Criação de um banco de dados de destino usando o editor de consultas v2

1. Navegue até o console do Amazon Redshift e escolha Editor de consultas v2.
2. No painel à esquerda, escolha o grupo de trabalho do Amazon Redshift sem servidor ou o cluster provisionado do Amazon Redshift e, em seguida, conecte-se a ele.
3. Para obter o ID de integração, navegue até a lista de integrações no console do Amazon Redshift.

Ou você pode executar o seguinte comando para obter o valor de `integration_id`:

```
SELECT integration_id FROM SVV_INTEGRATION;
```

4. Depois, execute o comando a seguir para criar o banco de dados. Ao especificar o ID de integração, você estabelece uma conexão entre o banco de dados e a origem.

   Substitua `integration_id` pelo valor retornado pelo comando anterior.

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

   Para fontes do Aurora PostgreSQL, você também deve incluir uma referência ao banco de dados nomeado dentro do cluster especificado por você ao criar a integração. Por exemplo:

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

> **Note**
>
> Somente a fonte de integração pode atualizar os dados no banco de dados criado por você pela integração. Para alterar o esquema de uma tabela, execute comandos DDL ou DML nas tabelas na origem. É possível executar comandos DDL e DML em tabelas na origem, mas só executar comandos DDL e consultas somente leitura no banco de dados de destino.

Para obter informações sobre como exibir o status de um banco de dados de destino, consulte Gerenciamento de integrações ETL zero.

## Adicionar dados à origem

Depois de criar um banco de dados de destino, será possível adicionar dados à origem. Para adicionar dados à origem, consulte um dos seguintes tópicos:

- Para fontes do Aurora, consulte Add data to the source DB cluster no Guia do usuário do Amazon Aurora.
- Para origens do Amazon RDS, consulte Add data to the source DB instance no Guia do usuário do Amazon RDS.

# Consulta e criação de visões materializadas com dados replicados

## Consulta de dados replicados no Amazon Redshift

Depois que você adicionar dados à origem, eles serão replicados quase em tempo real para o data warehouse do Amazon Redshift e estarão prontos para consulta. Para obter informações sobre métricas de integração e estatísticas de tabela, consulte Métricas para integrações ETL zero.

> **Note**
>
> Como um banco de dados é igual a um esquema no MySQL, o nível do banco de dados do MySQL é mapeado para o nível do esquema do Amazon Redshift. Observe essa diferença de mapeamento ao consultar dados replicados do Aurora MySQL ou do RDS for MySQL.

Como consultar os dados replicados

1. Navegue até o console do Amazon Redshift e escolha Editor de consultas v2.
2. Conecte-se ao grupo de trabalho do Amazon Redshift sem servidor ou ao cluster provisionado pelo Amazon Redshift e escolha o banco de dados na lista suspensa.
3. Use uma instrução SELECT para selecionar todos os dados replicados do esquema e da tabela criados por você na origem. Para diferenciar letras maiúsculas de minúsculas, use aspas duplas (" ") para nomes de esquema, tabela e coluna. Por exemplo:

   ```
   SELECT * FROM "schema_name"."table_name";
   ```

   Você também pode consultar os dados usando a CLI do Amazon Redshift.

## Criação de visões materializadas com dados replicados

É possível criar visões materializadas no banco de dados do Amazon Redshift local para transformar dados replicados por meio de integrações ETL zero. Conecte-se ao banco de dados local e use consultas entre bancos de dados para acessar os bancos de dados de destino. É possível usar nomes de objeto totalmente qualificados com a notação em três partes (destination-database-name.schema-name.table-name) ou criar um esquema externo referenciando o par banco de dados/esquema de destino e usar a notação em duas partes (external-schema-name.table-name). Para

obter mais informações sobre consultas entre bancos de dados, consulte Querying data across databases.

Use o exemplo a seguir para criar e inserir dados de exemplo nas tabelas *sales_zetl* e *event_zetl* da *tickit_zetl* de origem. As tabelas são replicadas para o banco de dados do 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");
```

Você pode criar uma visão materializada para obter o total de vendas por evento usando a notação em três partes:

```
--three part notation zetl-database-name.schema-name.table-name
CREATE MATERIALIZED VIEW mv_transformed_sales_per_event_3p as
(SELECT eventname, sum(pricepaid) as total_price
FROM  zetl_int_db.tickit_zetl.sales_zetl S, zetl_int_db.tickit_zetl.event_zetl E
WHERE S.eventid = E.eventid
GROUP BY 1);
```

Você pode criar uma visão materializada para obter o total de vendas por evento usando a notação em duas partes:

```
--two part notation external-schema-name.table-name notation
CREATE EXTERNAL schema ext_tickit_zetl
FROM REDSHIFT
```

```
DATABASE zetl_int_db
SCHEMA tickit_zetl;

CREATE MATERIALIZED VIEW mv_transformed_sales_per_event_2p
AS
(
    SELECT eventname, sum(pricepaid) as total_price
    FROM  ext_tickit_zetl.sales_zetl S, ext_tickit_zetl.event_zetl E
    WHERE S.eventid = E.eventid
    GROUP BY 1
);
```

Para exibir as visões materializadas criadas por você, use o exemplo a seguir.

```
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        |
+-----------+-------------+
```

# Gerenciamento de integrações ETL zero

É possível exibir os detalhes de uma integração ETL zero para ver as informações de configuração e o status no console do Amazon Redshift.

Como visualizar os detalhes de uma integração ETL zero

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

2. No painel de navegação à esquerda, escolha o painel Serverless ou Clusters provisionados. Depois, escolha Integrações ETL zero.
3. Selecione a Integração ETL zero que você deseja visualizar. Para cada integração, as seguintes informações são fornecidas:

   - ID de integração é o identificador retornado quando a integração é criada.
   - Status pode ser um dos seguintes:
     - `Active`: a integração ETL zero está enviando dados transacionais ao data warehouse do Amazon Redshift.
     - `Syncing`: a integração ETL zero encontrou um erro recuperável e está reenviando os dados. As tabelas afetadas não estão disponíveis para consulta no Amazon Redshift até que terminem a ressincronização.
     - `Failed`: a integração ETL zero encontrou um evento ou um erro irrecuperável que não pode ser corrigido. Você precisa excluir e recriar a integração ETL zero.
     - `Creating`: a integração ETL zero está sendo criada.
     - `Deleting`: a integração ETL zero está sendo excluída.
     - `Needs attention`: a integração ETL zero encontrou um evento ou um erro que requer intervenção manual para ser resolvido. Para corrigir o problema, siga as etapas na mensagem de erro.
   - ARN de origem é o ARN dos dados de origem.
   - Destino é o ARN do namespace do data warehouse de destino.
   - Banco de dados pode ser um dos seguintes:
     - `No database`: não há banco de dados de destino para a integração.
     - `Creating`: o Amazon Redshift está criando o banco de dados de destino para a integração.
     - `Active`: os dados estão sendo replicados da origem da integração para o Amazon Redshift.
     - `Error`: há um erro na integração.
     - `Recovering`: a integração está se recuperando após a reinicialização do data warehouse.
     - `Resyncing`: o Amazon Redshift está ressincronizando as tabelas na integração.
   - Tipo de destino é o tipo de data warehouse do Amazon Redshift.
   - Data de criação é a data e a hora (UTC) quando a integração foi criada.

> **Note**
>
> Para exibir detalhes da integração de um data warehouse, escolha a página de detalhes do cluster provisionado ou do namespace sem servidor e, em seguida, escolha a guia Integrações ETL zero.

Na lista Integrações ETL zero, é possível escolher Consultar Dados para ir até o editor de consultas do Amazon Redshift v2. O banco de dados de destino do Amazon Redshift tem o parâmetro enable_case_sensitive_identifier habilitado. Ao escrever SQL, talvez você precise colocar esquemas, tabelas e nomes de coluna entre aspas duplas ("<name>"). Para obter mais informações sobre como consultar dados no data warehouse do Amazon Redshift, consulte Consultar um banco de dados usando o editor de consultas v2 do Amazon Redshift.

Na lista Integrações ETL zero, é possível escolher Compartilhar dados para criar uma unidade de compartilhamento de dados. Para criar uma unidade de compartilhamento de dados para o banco de dados do Amazon Redshift, siga as instruções na página Criar compartilhamento de dados. Para compartilhar dados no banco de dados do Amazon Redshift, você deve primeiramente criar um banco de dados de destino. Para obter mais informações sobre compartilhamento de dados, consulte Data sharing concepts for Amazon Redshift.

Para atualizar a integração, é possível usar o comando ALTER DATABASE. Isso replica todos os dados da fonte de integração para o banco de dados de destino. O exemplo a seguir atualiza todas as tabelas sincronizadas e com falha na integração ETL zero.

```
ALTER DATABASE sample_integration_db INTEGRATION REFRESH ALL tables;
```

## Compartilhamento de dados no Amazon Redshift

Depois que você adicionar dados à origem, eles serão replicados imediatamente para o Amazon Redshift e estarão prontos para serem compartilhados pela criação das unidades de compartilhamento de dados.

Para compartilhar dados, você deve criar um banco de dados de destino primeiro.

> **Important**
>
> Para compartilhar dados de um data warehouse de visualização do Amazon Redshift com um data warehouse consumidor do Amazon Redshift, o data warehouse consumidor deve

estar na faixa `preview_2023`. Para obter informações sobre unidades de compartilhamento de dados, consulte What is a datashare? no Guia do desenvolvedor do banco de dados do Amazon Redshift.
Para criar uma pré-visualização do data warehouse de destino, consulte um dos seguintes tópicos, dependendo do tipo de implantação:

- Cluster provisionado pelo Amazon Redshift – Criar cluster de visualização prévia
- Grupo de trabalho do Redshift Serverless – Criar visualização prévia de grupo de trabalho

## Compartilhamento de dados no Amazon Redshift sem servidor usando o console do Amazon Redshift

1. No console do Amazon Redshift, no painel de navegação à esquerda, escolha Amazon Redshift Serverless > Painéis da tecnologia sem servidor.
2. No painel de navegação à esquerda, escolha Integrações ETL zero.
3. Escolha Share data (Compartilhar dados).
4. Na página de criação da unidade de compartilhamento de dados, siga as etapas em Criação das unidades de compartilhamento de dados.

## Compartilhamento de dados em clusters provisionados pelo Amazon Redshift usando o console do Amazon Redshift

1. No console do Amazon Redshift, no painel de navegação à esquerda, escolha Painel de clusters provisionados.
2. No painel de navegação à esquerda, escolha Integrações ETL zero.
3. Escolha uma integração na lista.
4. Na página de detalhes da integração, escolha Conectar-se ao banco de dados.
5. Na página Conexão com banco de dados, é possível criar uma conexão ou usar uma recente. A conexão deve ser feita com o banco de dados de destino.
6. Se você criar uma conexão, insira um Nome do banco de dados para o banco de dados. Depois, clique em Conectar.
7. Na página de detalhes da integração, escolha Compartilhar dados.

8. Na página de criação da unidade de compartilhamento de dados, siga as etapas em Criação das unidades de compartilhamento de dados.

# Métricas para integrações ETL zero

É possível usar as métricas no console do Amazon Redshift e no Amazon CloudWatch para saber mais sobre a integridade e o desempenho das integrações ETL zero. É possível ajustar as métricas para exibir dados de períodos mais curtos ou mais longos ou optar por visualizar métricas no CloudWatch. Para exibir as métricas da integração no console do Amazon Redshift, escolha Integrações ETL zero no painel de navegação à esquerda e escolha o ID da integração.

Para integrações ETL zero do Aurora e do Amazon RDS, o Amazon Redshift oferece dois tipos de métricas na página de detalhes de uma integração. Os tipos de métricas são os seguintes:

- Na guia Métricas de integração, estes são os gráficos disponíveis:

| Métrica | Descrição |
| --- | --- |
| `Lag` | O atraso entre o momento em que os dados são confirmados para a origem e o momento em que os dados estão disponíveis para consulta no Amazon Redshift.<br><br>Unidades: segundo<br><br>Dimensões: `IntegrationLag` |
| `Tables replicated` | O número de tabelas que foram replicadas do banco de dados de origem para o Amazon Redshift.<br><br>Unidades: contagem<br><br>Dimensões: `IntegrationNumTablesReplicated` |
| `Tables failed` | O número de tabelas que apresentaram falha na replicação.<br><br>Unidades: contagem<br><br>Dimensões: `IntegrationNumTablesFailedReplication` |

- Na guia Estatísticas da tabela, é possível ver a lista de tabelas que estão ativas no momento ou com erros. As estatísticas nessa guia são as seguintes:
  - Nome do esquema: o nome do esquema no qual a tabela está.
  - Nome da tabela: o nome da tabela no banco de dados de origem.
  - Status: o status da tabela. Os valores possíveis incluem `Synced`, `Failed`, `Deleted`, `Resync Required` e `Resync Initiated`.
  - Banco de dados: o banco de dados do Amazon Redshift no qual a tabela está.
  - Última atualização: a data e a hora (UTC) em que a última atualização foi feita na tabela.

# Solução de problemas em integrações ETL zero

## Solução de problemas em integrações ETL zero com o Aurora MySQL

Use as informações a seguir para solucionar problemas comuns com integrações ETL zero com o Aurora MySQL.

Tópicos


- A criação da integração apresentou falha
- As tabelas não têm chaves primárias
- Tipos de dados não compatíveis em tabelas
- Falha nos comandos da linguagem de manipulação de dados
- As alterações rastreadas entre as fontes de dados não coincidem
- Falha na autorização
- O número de tabelas é superior a 100 mil ou o número de esquemas é superior a 4.950
- O Amazon Redshift não consegue carregar dados
- As configurações dos parâmetros do grupo de trabalho estão incorretas
- O banco de dados não foi criado para ativar uma Integração ETL zero
- A tabela está no estado Ressincronização necessária ou Ressincronização iniciada


### A criação da integração apresentou falha

Se a criação da Integração ETL zero apresentar falha, o status da integração será `Inactive`. Confira se o indicado abaixo está correto para seu cluster de banco de dados de origem do Aurora:

- Você criou o cluster no console do Amazon RDS.
- O cluster do banco de dados de origem do Aurora está executando o MySQL versão 3.05 ou posterior. Para confirmar, acesse a guia Configuração do cluster e verifique a Versão do mecanismo.
- Você definiu corretamente as configurações dos parâmetros de log binário para o cluster. Se os parâmetros de log binário do Aurora MySQL estiverem definidos incorretamente ou não estiverem associados ao cluster de banco de dados de origem do Aurora, a criação falhará. Consulte Configurar parâmetros do cluster de banco de dados.

Além disso, confira se o indicado abaixo está correto para seu data warehouse do Amazon Redshift:

- A diferenciação entre letras maiúsculas e minúsculas está ativada. Consulte Ative a diferenciação entre letras maiúsculas e minúsculas no data warehouse.
- Você adicionou a entidade principal autorizada e a fonte de integração corretas para seu namespace. Consulte Configurar a autorização para o data warehouse do Amazon Redshift.

As tabelas não têm chaves primárias

No banco de dados de destino, uma ou mais tabelas não têm uma chave primária e não podem ser sincronizadas.

Para resolver esse problema, acesse a guia Estatísticas da tabela na página de detalhes da integração ou use SVV_INTEGRATION_TABLE_STATE para visualizar as tabelas com falha. É possível adicionar chaves primárias às tabelas, e o Amazon Redshift vai ressincronizar as tabelas. Como alternativa, embora não seja recomendável, é possível descartar essas tabelas no Aurora e criar tabelas com uma chave primária. Para obter mais informações, consulte Práticas recomendadas do Amazon Redshift para projetar tabelas.

Tipos de dados não compatíveis em tabelas

No banco de dados criado por você pela integração no Amazon Redshift e no qual os dados são replicados do cluster do banco de dados do Aurora, uma ou mais das tabelas têm tipos de dados não compatíveis e não podem ser sincronizadas.

Para resolver esse problema, acesse a guia Estatísticas da tabela na página de detalhes da integração ou use SVV_INTEGRATION_TABLE_STATE para visualizar as tabelas com falha. Depois, remova essas tabelas e recrie outras no Amazon RDS. Para obter mais informações sobre

tipos de dados não compatíveis, consulte Data type differences between Aurora and Amazon Redshift databases no Guia do usuário do Amazon Aurora.

Falha nos comandos da linguagem de manipulação de dados

O Amazon Redshift não pôde executar comandos DML nas tabelas do Redshift. Para resolver esse problema, use SVV_INTEGRATION_TABLE_STATE para visualizar as tabelas com falha. O Amazon Redshift ressincroniza automaticamente as tabelas para resolver esse erro.

As alterações rastreadas entre as fontes de dados não coincidem

Esse erro ocorre quando as alterações entre o Amazon Aurora e o Amazon Redshift não coincidem, fazendo com que a integração entre em um estado `Failed`.

Para resolver isso, exclua a Integração ETL zero e crie-a novamente no Amazon RDS. Para obter mais informações, consulte Criar Integrações ETL zero e Excluir Integrações ETL zero.

Falha na autorização

A autorização falhou porque o cluster de banco de dados de origem do Aurora foi removido como uma fonte de integração autorizada para o data warehouse do Amazon Redshift.

Para resolver esse problema, exclua a Integração ETL zero e crie-a novamente no Amazon RDS. Para obter mais informações, consulte Criar Integrações ETL zero e Excluir Integrações ETL zero.

O número de tabelas é superior a 100 mil ou o número de esquemas é superior a 4.950

Para um data warehouse de destino, o número de tabelas é superior a 100 mil ou o número de esquemas é superior a 4.950. O Amazon Aurora não pode enviar dados para o Amazon Redshift. O número de tabelas e esquemas excede o limite definido. Para resolver esse problema, remova todos os esquemas ou tabelas desnecessários do banco de dados de origem.

O Amazon Redshift não consegue carregar dados

O Amazon Redshift não consegue carregar dados na Integração ETL zero.

Para resolver esse problema, exclua a Integração ETL zero no Amazon RDS e crie-a novamente. Para obter mais informações, consulte Criar Integrações ETL zero e Excluir Integrações ETL zero.

As configurações dos parâmetros do grupo de trabalho estão incorretas

O grupo de trabalho não diferencia letras maiúsculas de minúsculas.

Para resolver esse problema, acesse a guia Propriedades na página de detalhes da integração, escolha o grupo de parâmetros e ative o identificador que diferencia letras maiúsculas de minúsculas na guia Propriedades. Se você não tiver um grupo de parâmetros em vigor, crie um com o identificador que diferencia letras maiúsculas de minúsculas ativado. Depois, crie uma Integração ETL zero no Amazon RDS. Para obter mais informações, consulte Criar Integrações ETL zero.

O banco de dados não foi criado para ativar uma Integração ETL zero

Não há um banco de dados criado para que a Integração ETL zero o ative.

Para resolver esse problema, crie um banco de dados para a integração. Para ter mais informações, consulte Criação de um banco de dados de destino no Amazon Redshift.

A tabela está no estado Ressincronização necessária ou Ressincronização iniciada

A tabela está no estado Ressincronização necessária ou Ressincronização iniciada.

Para obter informações de erro mais detalhadas sobre o motivo pelo qual a tabela está nesse estado, use a exibição de sistema SYS_LOAD_ERROR_DETAIL.

## Solução de problemas em integrações ETL zero com o Aurora PostgreSQL

Use as informações a seguir para solucionar problemas comuns com integrações ETL zero com o Aurora PostgreSQL.

Tópicos


- A criação da integração apresentou falha
- As tabelas não têm chaves primárias
- Tipos de dados não compatíveis em tabelas
- Falha nos comandos da linguagem de manipulação de dados
- As alterações rastreadas entre as fontes de dados não coincidem
- Falha na autorização
- O número de tabelas é superior a 100 mil ou o número de esquemas é superior a 4.950
- O Amazon Redshift não consegue carregar dados
- As configurações dos parâmetros do grupo de trabalho estão incorretas
- O banco de dados não foi criado para ativar uma Integração ETL zero
- A tabela está no estado Ressincronização necessária ou Ressincronização iniciada

A criação da integração apresentou falha

Se a criação da Integração ETL zero apresentar falha, o status da integração será `Inactive`. Confira se o indicado abaixo está correto para seu cluster de banco de dados de origem do Aurora:

- Você criou o cluster no console do Amazon RDS.
- O cluster do banco de dados de origem do Aurora está executando o Aurora PostgreSQL versão 15.4.99 ou posterior. Para confirmar, acesse a guia Configuração do cluster e verifique a Versão do mecanismo.
- Você definiu corretamente as configurações dos parâmetros de log binário para o cluster. Se os parâmetros de log binário do Aurora PostgreSQL estiverem definidos incorretamente ou não estiverem associados ao cluster do banco de dados do Aurora de origem, haverá falha na criação. Consulte Configurar parâmetros do cluster de banco de dados.

Além disso, confira se o indicado abaixo está correto para seu data warehouse do Amazon Redshift:

- A diferenciação entre letras maiúsculas e minúsculas está ativada. Consulte Ative a diferenciação entre letras maiúsculas e minúsculas no data warehouse.
- Você adicionou a entidade principal autorizada e a fonte de integração corretas para seu namespace. Consulte Configurar a autorização para o data warehouse do Amazon Redshift.

As tabelas não têm chaves primárias

No banco de dados de destino, uma ou mais tabelas não têm uma chave primária e não podem ser sincronizadas.

Para resolver esse problema, acesse a guia Estatísticas da tabela na página de detalhes da integração ou use SVV_INTEGRATION_TABLE_STATE para visualizar as tabelas com falha. É possível adicionar chaves primárias às tabelas, e o Amazon Redshift vai ressincronizar as tabelas. Como alternativa, embora não seja recomendável, é possível descartar essas tabelas no Aurora e criar tabelas com uma chave primária. Para obter mais informações, consulte Práticas recomendadas do Amazon Redshift para projetar tabelas.

Tipos de dados não compatíveis em tabelas

No banco de dados criado por você pela integração no Amazon Redshift e no qual os dados são replicados do cluster do banco de dados do Aurora, uma ou mais das tabelas têm tipos de dados não compatíveis e não podem ser sincronizadas.

Para resolver esse problema, acesse a guia Estatísticas da tabela na página de detalhes da integração ou use SVV_INTEGRATION_TABLE_STATE para visualizar as tabelas com falha. Depois, remova essas tabelas e recrie outras no Amazon RDS. Para obter mais informações sobre tipos de dados não compatíveis, consulte Data type differences between Aurora and Amazon Redshift databases no Guia do usuário do Amazon Aurora.

Falha nos comandos da linguagem de manipulação de dados

O Amazon Redshift não pôde executar comandos DML nas tabelas do Redshift. Para resolver esse problema, use SVV_INTEGRATION_TABLE_STATE para visualizar as tabelas com falha. O Amazon Redshift ressincroniza automaticamente as tabelas para resolver esse erro.

As alterações rastreadas entre as fontes de dados não coincidem

Esse erro ocorre quando as alterações entre o Amazon Aurora e o Amazon Redshift não coincidem, fazendo com que a integração entre em um estado `Failed`.

Para resolver isso, exclua a Integração ETL zero e crie-a novamente no Amazon RDS. Para obter mais informações, consulte Criar Integrações ETL zero e Excluir Integrações ETL zero.

Falha na autorização

A autorização falhou porque o cluster de banco de dados de origem do Aurora foi removido como uma fonte de integração autorizada para o data warehouse do Amazon Redshift.

Para resolver esse problema, exclua a Integração ETL zero e crie-a novamente no Amazon RDS. Para obter mais informações, consulte Criar Integrações ETL zero e Excluir Integrações ETL zero.

O número de tabelas é superior a 100 mil ou o número de esquemas é superior a 4.950

Para um data warehouse de destino, o número de tabelas é superior a 100 mil ou o número de esquemas é superior a 4.950. O Amazon Aurora não pode enviar dados para o Amazon Redshift. O número de tabelas e esquemas excede o limite definido. Para resolver esse problema, remova todos os esquemas ou tabelas desnecessários do banco de dados de origem.

O Amazon Redshift não consegue carregar dados

O Amazon Redshift não consegue carregar dados na Integração ETL zero.

Para resolver esse problema, exclua a Integração ETL zero no Amazon RDS e crie-a novamente. Para obter mais informações, consulte Criar Integrações ETL zero e Excluir Integrações ETL zero.

As configurações dos parâmetros do grupo de trabalho estão incorretas

O grupo de trabalho não diferencia letras maiúsculas de minúsculas.

Para resolver esse problema, acesse a guia Propriedades na página de detalhes da integração, escolha o grupo de parâmetros e ative o identificador que diferencia letras maiúsculas de minúsculas na guia Propriedades. Se você não tiver um grupo de parâmetros em vigor, crie um com o identificador que diferencia letras maiúsculas de minúsculas ativado. Depois, crie uma Integração ETL zero no Amazon RDS. Para obter mais informações, consulte Criar Integrações ETL zero.

O banco de dados não foi criado para ativar uma Integração ETL zero

Não há um banco de dados criado para que a Integração ETL zero o ative.

Para resolver esse problema, crie um banco de dados para a integração. Para ter mais informações, consulte Criação de um banco de dados de destino no Amazon Redshift.

A tabela está no estado Ressincronização necessária ou Ressincronização iniciada

A tabela está no estado Ressincronização necessária ou Ressincronização iniciada.

Para obter informações de erro mais detalhadas sobre o motivo pelo qual a tabela está nesse estado, use a exibição de sistema SYS_LOAD_ERROR_DETAIL.

## Solução de problemas em integrações ETL zero com o RDS for MySQL

Use as informações a seguir para solucionar problemas comuns com integrações ETL zero com o RDS for MySQL.

Tópicos


- A criação da integração apresentou falha
- As tabelas não têm chaves primárias
- Tipos de dados não compatíveis em tabelas
- Falha nos comandos da linguagem de manipulação de dados
- As alterações rastreadas entre as fontes de dados não coincidem
- Falha na autorização
- O número de tabelas é superior a 100 mil ou o número de esquemas é superior a 4.950
- O Amazon Redshift não consegue carregar dados
- As configurações dos parâmetros do grupo de trabalho estão incorretas

- O banco de dados não foi criado para ativar uma Integração ETL zero
- A tabela está no estado Ressincronização necessária ou Ressincronização iniciada

A criação da integração apresentou falha

Se a criação da Integração ETL zero apresentar falha, o status da integração será `Inactive`. Verifique se as seguintes informações estão corretas para a instância do banco de dados do RDS de origem:

- Você criou a instância no console do Amazon RDS.
- A instância do banco de dados do RDS de origem está executando o RDS for MySQL versão 8.0.28 ou superior. Para validar isso, vá até a guia Configuração da instância e verifique a Versão do mecanismo.
- Você definiu corretamente as configurações do parâmetro de log binário para a instância. Se os parâmetros de log binário do RDS for MySQL estiverem definidos incorretamente ou não estiverem associados à instância do banco de dados do RDS de origem, haverá falha na criação. Consulte Configure DB instance parameters.

Além disso, confira se o indicado abaixo está correto para seu data warehouse do Amazon Redshift:

- A diferenciação entre letras maiúsculas e minúsculas está ativada. Consulte Ative a diferenciação entre letras maiúsculas e minúsculas no data warehouse.
- Você adicionou a entidade principal autorizada e a fonte de integração corretas para seu namespace. Consulte Configurar a autorização para o data warehouse do Amazon Redshift.

As tabelas não têm chaves primárias

No banco de dados de destino, uma ou mais tabelas não têm uma chave primária e não podem ser sincronizadas.

Para resolver esse problema, acesse a guia Estatísticas da tabela na página de detalhes da integração ou use SVV_INTEGRATION_TABLE_STATE para visualizar as tabelas com falha. É possível adicionar chaves primárias às tabelas, e o Amazon Redshift vai ressincronizar as tabelas. Como alternativa, embora não seja recomendável, é possível descartar essas tabelas no RDS e criar tabelas com uma chave primária. Para obter mais informações, consulte Práticas recomendadas do Amazon Redshift para projetar tabelas.

Tipos de dados não compatíveis em tabelas

No banco de dados criado por você pela integração no Amazon Redshift e no qual os dados são replicados da instância do banco de dados do RDS, uma ou mais das tabelas têm tipos de dados não compatíveis e não podem ser sincronizadas.

Para resolver esse problema, acesse a guia Estatísticas da tabela na página de detalhes da integração ou use SVV_INTEGRATION_TABLE_STATE para visualizar as tabelas com falha. Depois, remova essas tabelas e recrie outras no Amazon RDS. Para obter mais informações sobre tipos de dados não compatíveis, consulte Data type differences between RDS and Amazon Redshift databases no Guia do usuário do Amazon RDS.

Falha nos comandos da linguagem de manipulação de dados

O Amazon Redshift não pôde executar comandos DML nas tabelas do Redshift. Para resolver esse problema, use SVV_INTEGRATION_TABLE_STATE para visualizar as tabelas com falha. O Amazon Redshift ressincroniza automaticamente as tabelas para resolver esse erro.

As alterações rastreadas entre as fontes de dados não coincidem

Esse erro ocorre quando as alterações entre o Amazon Aurora e o Amazon Redshift não coincidem, fazendo com que a integração entre em um estado `Failed`.

Para resolver isso, exclua a Integração ETL zero e crie-a novamente no Amazon RDS. Para obter mais informações, consulte Criar Integrações ETL zero e Excluir Integrações ETL zero.

Falha na autorização

Houve falha na autorização porque o cluster do banco de dados do RDS de origem foi removido como uma fonte de integração autorizada para o data warehouse do Amazon Redshift.

Para resolver esse problema, exclua a Integração ETL zero e crie-a novamente no Amazon RDS. Para obter mais informações, consulte Criar Integrações ETL zero e Excluir Integrações ETL zero.

O número de tabelas é superior a 100 mil ou o número de esquemas é superior a 4.950

Para um data warehouse de destino, o número de tabelas é superior a 100 mil ou o número de esquemas é superior a 4.950. O Amazon Aurora não pode enviar dados para o Amazon Redshift. O número de tabelas e esquemas excede o limite definido. Para resolver esse problema, remova todos os esquemas ou tabelas desnecessários do banco de dados de origem.

O Amazon Redshift não consegue carregar dados

O Amazon Redshift não consegue carregar dados na Integração ETL zero.

Para resolver esse problema, exclua a Integração ETL zero no Amazon RDS e crie-a novamente. Para obter mais informações, consulte Criar Integrações ETL zero e Excluir Integrações ETL zero.

As configurações dos parâmetros do grupo de trabalho estão incorretas

O grupo de trabalho não diferencia letras maiúsculas de minúsculas.

Para resolver esse problema, acesse a guia Propriedades na página de detalhes da integração, escolha o grupo de parâmetros e ative o identificador que diferencia letras maiúsculas de minúsculas na guia Propriedades. Se você não tiver um grupo de parâmetros em vigor, crie um com o identificador que diferencia letras maiúsculas de minúsculas ativado. Depois, crie uma Integração ETL zero no Amazon RDS. Para obter mais informações, consulte Criar Integrações ETL zero.

O banco de dados não foi criado para ativar uma Integração ETL zero

Não há um banco de dados criado para que a Integração ETL zero o ative.

Para resolver esse problema, crie um banco de dados para a integração. Para ter mais informações, consulte Criação de um banco de dados de destino no Amazon Redshift.

A tabela está no estado Ressincronização necessária ou Ressincronização iniciada

A tabela está no estado Ressincronização necessária ou Ressincronização iniciada.

Para obter informações de erro mais detalhadas sobre o motivo pelo qual a tabela está nesse estado, use a exibição de sistema SYS_LOAD_ERROR_DETAIL.

# Consultar um banco de dados

Para consultar bancos de dados hospedados por seu cluster do Amazon Redshift, você tem duas opções:

- Conecte-se ao cluster e execute consultas no AWS Management Console com o Query Editor.

  Se você usa o editor de consulta no console do Amazon Redshift, não precisa baixar e configurar um aplicativo cliente SQL.
- Conecte-se ao cluster por meio de uma ferramenta de cliente SQL, como SQL Workbench/J.

  O Amazon Redshift oferece suporte a ferramentas do cliente SQL conectadas por meio de Java Database Connectivity (JDBC) e Open Database Connectivity (ODBC) O Amazon Redshift não fornece nem instala nenhuma biblioteca ou ferramenta do cliente SQL, portanto, você deve instalá-las no computador cliente ou na instância do Amazon EC2 para usá-las. Você pode usar a maioria das ferramentas do cliente SQL que oferecem suporte aos drivers do JDBC ou do ODBC.

> **Note**
>
> Quando você escreve procedimentos armazenados, recomendamos a prática de proteger valores confidenciais:
> Não codifique nenhuma informação confidencial na lógica do procedimento armazenado. Por exemplo, não atribua uma senha de usuário em uma instrução CREATE USER no corpo de um procedimento armazenado. Isso representa um risco de segurança, pois valores codificados podem ser registrados como metadados de esquema nas tabelas do catálogo. Em vez disso, transmita valores confidenciais, como senhas, como argumentos ao procedimento armazenado por meio de parâmetros.
> Para obter mais informações sobre os procedimentos armazenados, consulte CREATE PROCEDURE e “Criar procedimentos armazenados no Amazon Redshift”. Para obter mais informações sobre tabelas de catálogo, consulte “Tabelas de catálogo do sistema”.

Tópicos


- Consultar um banco de dados usando o editor de consultas v2 do Amazon Redshift
- Consultar um banco de dados usando o Query Editor
- Conectar-se a um data warehouse do Amazon Redshift usando ferramentas de cliente SQL

- Usar a API de dados Amazon Redshift

# Consultar um banco de dados usando o editor de consultas v2 do Amazon Redshift

O editor de consultas v2 é uma aplicação de cliente SQL baseada na Web separada que você usa para criar e executar consultas no data warehouse do Amazon Redshift. Você pode visualizar seus resultados em gráficos e compartilhar suas consultas com outras pessoas de sua equipe. O editor de consultas v2 é um substituto do editor de consultas anterior.

> **Note**
>
> O editor de consultas v2 está disponível em Regiões da AWS comerciais. Para obter uma lista de Regiões da AWS onde o editor de consultas v2 está disponível, consulte os endpoints listados para o Editor de consultas v2 do Redshift na Referência geral da Amazon Web Services.

Para ver uma demonstração do editor de consultas v2, assista ao vídeo a seguir. Editor de consultas v2 do Amazon Redshift.

Para ver uma demonstração da análise de dados, assista ao vídeo a seguir. Análise de dados usando o editor de consultas v2 do Amazon Redshift.

Para ver uma demonstração do uso do editor de consultas v2 executando várias consultas com uma conexão isolada ou compartilhada, assista ao vídeo a seguir. Execução de consulta simultânea usando o editor de consultas v2.

O editor de consultas v2 conta com um rico conjunto de recursos para gerenciar e executar suas instruções SQL. Os tópicos das seções a seguir apresentam os primeiros passos de muitos desses recursos. Explore o editor de consultas v2 por conta própria para se familiarizar com seus recursos.

Tópicos

- Configurar sua Conta da AWS
- Trabalhar com o editor de consultas v2
- Interação com o SQL generativo do editor de consultas v2 (visualização)
- Carregar dados em um banco de dados

- Autorizar e executar consultas
- Autorizar e executar blocos de anotações
- Consulta ao AWS Glue Data Catalog
- Consultar um data lake
- Trabalho com unidades de compartilhamento de dados
- Programar uma consulta com o editor de consultas v2
- Visualizar resultados da consulta
- Compartilhar e trabalhar em equipe

## Configurar sua Conta da AWS

Quando você seleciona o editor de consultas v2 no console do Amazon Redshift, abre-se uma nova guia no navegador com a interface do editor de consultas v2. Com as devidas permissões, é possível acessar dados em um cluster ou grupo de trabalho do Amazon Redshift de propriedade de sua Conta da AWS que esteja na Região da AWS atual.

Na primeira vez que um administrador configura o editor de consultas v2 para sua Conta da AWS, ele escolhe a AWS KMS key que será usada para criptografar recursos do editor de consultas v2. Por padrão, uma chave de propriedade da AWS é usada para criptografar recursos. Ou um administrador pode usar uma chave gerenciada pelo cliente escolhendo o nome do recurso da Amazon (ARN) da chave na página de configuração. Depois de configurar uma conta, as configurações de criptografia do AWS KMS não poderão ser alteradas. Para obter mais informações sobre como criar e usar uma chave gerenciada pelo cliente com o editor de consultas v2, consulte Criar uma chave AWS KMS gerenciada pelo cliente para usar com o editor de consultas v2. O administrador também pode selecionar um S3 bucket (Bucket do S3) e um caminho que é usado para alguns recursos, como carregar dados de um arquivo. Para ter mais informações, consulte Carregar dados de uma configuração e fluxo de trabalho de arquivo local.

O editor de consultas v2 do Amazon Redshift é compatível com autenticação, criptografia, isolamento e conformidade para manter seus dados em repouso e em trânsito seguros. Para obter mais informações sobre segurança de dados e o editor de consultas v2, consulte:

- Criptografia inativa
- Criptografia em trânsito
- Análise de configuração e vulnerabilidade no Amazon Redshift

O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por sua conta da Conta da AWS ou em nome dela e entrega os arquivos de log a um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. Para saber mais sobre como o editor de consultas v2 é executado no AWS CloudTrail, consulte Registrar em log com o CloudTrail. Para obter mais informações sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

O editor de consultas v2 conta com cotas ajustáveis para alguns de seus recursos. Para obter mais informações, consulte Cotas para objetos do Amazon Redshift.

## Recursos criados com o editor de consultas v2

No editor de consultas v2, é possível criar recursos como consultas e gráficos salvos. Todos os recursos no editor de consultas v2 estão associados a um usuário ou perfil do IAM. Recomendamos anexar políticas a um perfil do IAM e atribuir o perfil a um usuário.

No editor de consultas v2, é possível adicionar e remover etiquetas para consultas e gráficos salvos. Você pode usar essas etiquetas ao configurar políticas personalizadas do IAM ou para pesquisar recursos. Também é possível gerenciar as etiquetas coletivamente usando o Tag Editor no AWS Resource Groups.

É possível configurar perfis do IAM com políticas do IAM para compartilhar consultas com outras pessoas na mesma Conta da AWS na Região da AWS.

## Criar uma chave AWS KMS gerenciada pelo cliente para usar com o editor de consultas v2

Para criar uma chave gerenciada pelo cliente de criptografia simétrica:

Você pode criar uma chave de criptografia simétrica gerenciada pelo cliente para criptografar recursos do editor de consultas v2 usando o console do AWS KMS ou operações de API do AWS KMS. Para obter instruções sobre como criar uma chave, consulte “Criar chaves do AWS KMS de criptografia simétrica” no Guia do desenvolvedor do AWS Key Management Service.

Política de chaves

As políticas de chaves controlam o acesso à chave gerenciada pelo seu cliente. Cada chave gerenciada pelo cliente deve ter exatamente uma política de chaves, que contém declarações que determinam quem pode usar a chave e como pode usá-la. Ao criar a chave gerenciada pelo cliente,

você pode especificar uma política de chaves. Para obter mais informações, consulte Gerenciar do acesso às chaves do AWS KMS) no Guia do desenvolvedor do AWS Key Management Service.

Para usar a chave gerenciada pelo cliente com o editor de consultas do Amazon Redshift v2, as seguintes operações de API deverão ser permitidas na política de chaves:

- `kms:GenerateDataKey`: gera uma chave de dados simétrica exclusiva para criptografar seus dados.
- `kms:Decrypt`: descriptografa dados que foram criptografados com a chave gerenciada pelo cliente.
- `kms:DescribeKey`: fornece os principais detalhes gerenciados pelo cliente para permitir que o serviço valide a chave.

Veja a seguir um exemplo de política do AWS KMS para Conta da AWS `111122223333`. Na primeira seção, o `kms:ViaService` limita o uso da chave para o serviço do editor de consultas v2 (que é chamado `sqlworkbench.`*`region`*`.amazonaws.com` na política). A Conta da AWS que usará a chave deve ser `111122223333`. Na segunda seção, o usuário raiz e os principais administradores da Conta da AWS `111122223333` podem acessar a chave.

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os recursos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do 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"
        }
    ]
}
```

Os recursos a seguir fornecem mais informações sobre chaves do AWS KMS:

- Para obter mais informações sobre políticas do AWS KMS, consulte Especificar permissões em uma política no Guia do desenvolvedor do AWS Key Management Service.
- Para obter informações sobre solução de problemas em políticas do AWS KMS, consulte Solucionar problemas de acesso à chave no Guia do desenvolvedor AWS Key Management Service.
- Para obter mais informações sobre chaves, consulte Chaves do AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

## Acessar o editor de consultas v2

Para acessar o editor de consultas v2, é necessário ter permissão. Um administrador pode anexar uma das seguintes políticas gerenciadas pela AWS ao perfil para conceder permissão. (Recomendamos anexar políticas a um perfil do IAM e atribuir o perfil a um usuário.) Essas políticas

gerenciadas pela AWS são redigidas com diferentes opções que controlam como os recursos de marcação permitem o compartilhamento de consultas. Você pode usar o console do IAM (https://console.aws.amazon.com/iam/) para anexar políticas do IAM.

- AmazonRedshiftQueryEditorV2FullAccess: concede acesso total às operações e recursos do editor de consultas v2 do Amazon Redshift. Essa política também concede acesso a outros serviços necessários.
- AmazonRedshiftQueryEditorV2NoSharing: concede a capacidade de trabalhar com o editor de consultas v2 do Amazon Redshift sem compartilhar recursos. Essa política também concede acesso a outros serviços necessários.
- AmazonRedshiftQueryEditorV2ReadSharing: concede a capacidade de trabalhar com o editor de consultas v2 do Amazon Redshift com compartilhamento limitado de recursos. A entidade principal concedida pode ler os recursos compartilhados com sua equipe, mas não pode atualizá-los. Essa política também concede acesso a outros serviços necessários.
- AmazonRedshiftQueryEditorV2ReadWriteSharing: concede a capacidade de trabalhar com o editor de consultas v2 do Amazon Redshift com compartilhamento de recursos. A entidade principal concedida pode ler e atualizar os recursos compartilhados com sua equipe. Essa política também concede acesso a outros serviços necessários.

Você também pode criar sua própria política com base nas permissões concedidas e negadas nas políticas gerenciadas fornecidas. Se usar o editor de políticas de console do IAM para criar sua própria política, escolha SQL Workbench como o serviço para o qual você está criando a política no editor visual. O editor de consultas v2 usa o nome do serviço AWS SQL Workbench no editor visual e no IAM Policy Simulator.

Para que uma entidade principal (um usuário ou perfil do IAM atribuído) se conecte a um cluster do Amazon Redshift, ela precisa das permissões em uma das políticas gerenciadas do editor de consultas v2. Também necessita da permissão `redshift:GetClusterCredentials` para o cluster. Para obter essa permissão, alguém com permissão administrativa pode anexar uma política aos perfis do IAM usados para se conectar ao cluster usando credenciais temporárias. Você pode definir o escopo da política para clusters específicos ou ser mais genérico. Para obter mais informações sobre permissão para usar credenciais temporárias, consulte Criar uma função do IAM ou um usuário com permissões para chamar GetClusterCredentials.

Para uma entidade principal (geralmente, um usuário com um perfil do IAM atribuído) ativar a capacidade na página Configurações da conta para outras pessoas na conta para Exportar o conjunto de resultados, ela precisa da permissão

`sqlworkbench:UpdateAcountExportSettings` anexada ao perfil. Essa permissão está incluída na política gerenciada `AmazonRedshiftQueryEditorV2FullAccess` da AWS.

À medida que novos recursos são adicionados ao editor de consultas v2, as políticas gerenciadas da AWS são atualizadas conforme a necessidade. Se você criar sua própria política com base nas permissões concedidas e negadas nas políticas gerenciadas fornecidas, edite suas políticas para mantê-las atualizadas com as alterações nas políticas gerenciadas. Para obter mais informações sobre políticas gerenciadas no Amazon Redshift, consulte Políticas gerenciadas pela AWS para o Amazon Redshift.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

> **Note**
>
> Se um administrador do AWS IAM Identity Center remover todas as associações do conjunto de permissões de um determinado conjunto de permissões em toda a conta, o acesso a qualquer recurso do editor de consultas originalmente associado ao conjunto de permissões removido deixará de estar acessível. Se, posteriormente, as mesmas permissões forem recriadas, um novo identificador interno será criado. Como o identificador interno foi alterado, o acesso aos recursos do editor de consultas anteriormente de propriedade de um usuário não pode ser acessado. Recomendamos que, antes de administradores excluírem um

conjunto de permissões, os usuários desse conjunto de permissões exportem recursos do editor de consultas, como notebooks e consultas, como backup.

## Configuração de etiquetas de entidade principal para se conectar a um cluster ou a um grupo de trabalho pelo editor de consultas v2

Para se conectar ao cluster ou ao grupo de trabalho usando a opção de usuário federado, configure o perfil do IAM ou o usuário com etiquetas de entidade principal. Como alternativa, configure o provedor de identidades (IdP) para transmitir `RedshiftDbUser` e (opcionalmente) `RedshiftDbGroups`. Para obter mais informações sobre como usar o IAM para gerenciar etiquetas, consulte Transmitir etiquetas de sessão no AWS Security Token Service no Guia do usuário do IAM. Para configurar o acesso usando o AWS Identity and Access Management, um administrador pode adicionar etiquetas usando o console do IAM (https://console.aws.amazon.com/iam/).

Como adicionar etiquetas de entidades principais a um perfil do IAM

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. Selecione Roles (Funções) no painel de navegação.
3. Selecione a função que precisa de acesso ao editor de consultas v2 usando um usuário federado.
4. Escolha a guia Tags.
5. Selecione Manage tags (Gerenciar tags).
6. Selecione Add tag (Adicionar etiqueta), insira a Key (Chave) como `RedshiftDbUser` e insira um Value (Valor) do nome do usuário federado.
7. Se preferir, escolha Add tag (Adicionar etiqueta), insira a Key (Chave) como `RedshiftDbGroups` e insira um Value (Valor) do nome do grupo a ser associado ao usuário.
8. Selecione Save changes (Salvar alterações) para visualizar a lista de etiquetas associadas ao perfil do IAM escolhido. A propagação das alterações pode levar vários segundos.
9. Para usar o usuário federado, atualize a página do editor de consultas v2 após a propagação das alterações.

Configurar o provedor de identidades (IdP) para transmitir etiquetas de entidades principais

O procedimento para configurar etiquetas usando um provedor de identidades (IdP) varia de acordo com o IdP. Consulte a documentação do IdP para obter instruções sobre como transmitir informações de usuário e grupo para atributos SAML. Quando configurado corretamente, os seguintes atributos aparecem em sua resposta SAML que é usada pelo AWS Security Token Service para preencher nas tags de entidades principais para `RedshiftDbUser` e `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>
```

O *db_groups* opcional deve ser uma lista separada por dois pontos, como `group1:group2:group3`.

Além disso, você pode definir o atributo `TransitiveTagKeys` para persistir as etiquetas durante o encadeamento de funções.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
  <AttributeValue>RedshiftDbUser</AttributeValue>
  <AttributeValue>RedshiftDbGroups</AttributeValue>
</Attribute>
```

Para obter mais informações sobre como configurar o editor de consultas v2, consulte Permissões necessárias para usar o editor de consultas v2 .

> **Note**
>
> Quando você se conecta ao cluster ou ao grupo de trabalho usando a opção de conexão de Usuário federado do editor de consultas v2, o provedor de identidades (IdP) pode fornecer etiquetas de entidade principal personalizadas para `RedshiftDbUser` e `RedshiftDbGroups`. Atualmente, o AWS IAM Identity Center não dá suporte para a passagem direta de etiquetas de entidade principal personalizadas para o editor de consultas v2.

# Trabalhar com o editor de consultas v2

O editor de consultas v2 é usado principalmente para editar e executar consultas, visualizar resultados e compartilhar seu trabalho com sua equipe. Com o editor de consultas v2, é possível criar bancos de dados, esquemas, tabelas e funções definidas pelo usuário (UDFs). Em um painel de exibição em árvore, é possível visualizar os esquemas de cada um de seus bancos de dados. É possível visualizar tabelas, exibições, UDFs e procedimentos armazenados de cada esquema.

Tópicos


- Abrir o editor de consultas v2
- Conectar-se a um banco de dados do Amazon Redshift
- Navegar por um banco de dados do Amazon Redshift
- Criar objetos de banco de dados
- Visualizar o histórico de consultas e guias
- Considerações ao trabalhar com o editor de consultas v2
- Alterar as configurações da conta


## Abrir o editor de consultas v2

Para abrir o editor de consultas v2

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu do navegador, selecione Editor e Query editor V2 (Editor de consultas V2). O editor de consultas v2 é aberto em uma nova guia do navegador.

A página do editor de consultas tem um menu do navegador no qual você escolhe uma exibição da seguinte maneira:

Editor

Você gerencia e consulta os dados organizados como tabelas e contidos em um banco de dados. O banco de dados pode conter dados armazenados ou uma referência a dados armazenados em

outro lugar, como o Amazon S3. Você se conecta a um banco de dados contido em um cluster ou em um grupo de trabalho com tecnologia sem servidor.

Ao trabalhar na visualização Editor, você tem os seguintes controles:

- O campo Cluster ou Workgroup (Grupo de trabalho) exibe o nome ao qual você está conectado no momento. O campo Database (Banco de dados) exibe os bancos de dados dentro do cluster ou grupo de trabalho. As ações que você executa na visualização Database (Banco de dados) padrão para atuar no banco de dados selecionado.
- Uma visualização hierárquica de exibição em árvore de seus clusters ou grupos de trabalho, bancos de dados e esquemas. Em esquemas, é possível trabalhar com suas tabelas, exibições, funções e procedimentos armazenados. Cada objeto na exibição em árvore oferece suporte a um menu de contexto para executar ações associadas, como Refresh(Atualizar) ou Drop (Descartar), para o objeto.
- Uma ação Create (Criar)

  para criar bancos de dados, esquemas, tabelas e funções.
- Uma ação

  Carreg

  dados para carregar dados do Amazon S3 ou de um arquivo local para o banco de dados.
- Um ícone Save (Salvar)

  para salvar sua consulta.
- Um ícone Shortcuts (Atalhos)

  para exibir atalhos de teclado para o editor.
- Um ícone

  Mais

  para exibir mais ações no editor. Como:
  - Compartilhar com minha equipe: para compartilhar um caderno com sua equipe. Para ter mais informações, consulte Compartilhar e trabalhar em equipe.
  - Atalhos: para exibir atalhos de teclado para o editor.
  - Histórico de guias: para exibir o histórico de guias de uma guia no editor.

    - Atualizar preenchimento automático: para atualizar as sugestões exibidas ao criar SQL.
- Uma área

  Editor na qual você pode digitar e executar uma consulta.

  Depois de executar uma consulta, é exibida a guia Result (Resultado) com os resultados. Aqui é onde você pode ativar Chart (Gráfico) para visualizar seus resultados. Você também pode Export (Exportar) os resultados.
- Uma área

  Notebook (Caderno) na qual você pode adicionar seções para inserir e executar SQL ou adicionar Markdown.

  Depois de executar uma consulta, é exibida a guia Result (Resultado) com os resultados. Aqui é lugar em que você pode Export (Exportar) os resultados.

Consultas

Uma consulta contém os comandos SQL para gerenciar e consultar dados em um banco de dados. Ao usar o editor de consultas v2 para carregar dados de exemplo, ele também cria e salva consultas de exemplo para você.

Ao escolher uma consulta salva, é possível abri-la, renomeá-la e excluí-la usando o menu de contexto (clique com o botão direito do mouse). Você pode visualizar atributos, como o ARN da consulta, de uma consulta salva escolhendo Detalhes da consulta. Você também pode ver o histórico de versões, editar as etiquetas anexadas à consulta e compartilhá-la com sua equipe.

Cadernos

Um caderno SQL contém células SQL e Markdown. Use cadernos SQL para organizar, anotar e compartilhar vários comandos SQL em um único documento.

Ao escolher um caderno salvo, é possível abri-lo, renomeá-lo, duplicá-lo e excluí-lo usando o menu de contexto (clique com o botão direito do mouse). Você pode visualizar atributos, como o ARN do caderno, de um caderno salvo escolhendo Detalhes do caderno. Você também pode ver

o histórico de versões, editar as etiquetas anexadas ao caderno, exportá-lo e compartilhá-lo com sua equipe. Para ter mais informações, consulte Autorizar e executar blocos de anotações.

Gráficos

Gráfico é uma representação visual dos dados. O editor de consultas v2 fornece ferramentas para criar vários tipos de gráfico e salvá-los.

Ao escolher um gráfico salvo, é possível abri-lo, renomeá-lo e excluí-lo usando o menu de contexto (clique com o botão direito do mouse). Você pode visualizar atributos, como o ARN do gráfico, de um gráfico salvo escolhendo Detalhes do gráfico. Você também pode editar as etiquetas anexadas ao gráfico e exportá-lo. Para ter mais informações, consulte Visualizar resultados da consulta.

Histórico

O histórico de consultas é uma lista das consultas que você executou usando o editor de consultas v2 do Amazon Redshift. Essas consultas foram executadas como consultas individuais ou como parte de um caderno SQL. Para ter mais informações, consulte Visualizar o histórico de consultas e guias.

Consultas

programadas

Uma consulta programada é uma consulta configurada para iniciar em horários específicos.

Todas as visualizações do editor de consultas v2 têm os seguintes ícones:

- Um ícone

  Visual mode (Modo visual) para alternar entre o modo claro e o modo escuro.
- Um ícone

  Settings (Configurações) para mostrar um menu das diferentes telas de configurações.

- Um ícone

  Editor preferences (Preferências do editor) para editar suas preferências ao usar o editor de consultas v2. Aqui você pode Editar configurações do espaço de trabalho para alterar o tamanho da fonte, o tamanho da guia e outras configurações de exibição. Você também pode ativar (ou desativar) o Preenchimento automático para mostrar sugestões ao inserir SQL.

- Um ícone

  Connections (Conexões) para visualizar as conexões usadas pelas guias do editor.

  A conexão é usada para recuperar dados de um banco de dados. Ela é criada para um banco de dados específico. Com uma conexão isolada, os resultados de um comando SQL que altera o banco de dados, como a criação de uma tabela temporária em uma guia do editor, não são visíveis em outra guia. Quando você abre uma guia no editor de consultas v2, o padrão é uma conexão isolada. Quando você cria uma conexão compartilhada, ou seja, desativa o botão Isolated session (Sessão isolada), os resultados em outras conexões compartilhadas com o mesmo banco de dados são visíveis entre si. No entanto, as guias do editor que usam uma conexão compartilhada com um banco de dados não são executadas em paralelo. As consultas que usam a mesma conexão devem aguardar até que a conexão esteja disponível. Uma conexão com um banco de dados não pode ser compartilhada com outro banco de dados e, portanto, os resultados SQL não são visíveis em diferentes conexões de banco de dados.

  O número de conexões ativas que qualquer usuário na conta pode ter é controlado por um administrador do editor de consultas v2.

- Um ícone

  Account settings (Configurações da conta) usado por um administrador para alterar determinadas configurações de todos os usuários na conta. Para obter mais informações, consulte Alterar as configurações da conta.

## Conectar-se a um banco de dados do Amazon Redshift

Para se conectar a um banco de dados, escolha o nome do cluster ou grupo de trabalho no painel de exibição em árvore. Caso seja solicitado, insira os parâmetros de conexão.

Ao se conectar a um cluster ou grupo de trabalho e a seus bancos de dados, você geralmente fornece um nome ao Database (Banco de dados). Você também fornece parâmetros necessários para um destes métodos de autenticação:

IAM Identity Center

Com esse método, conecte-se ao data warehouse do Amazon Redshift usando as credenciais de logon único do provedor de identidades (IdP). O cluster ou o grupo de trabalho deve estar habilitado para o IAM Identity Center no console do Amazon Redshift.

Usuário federado

Com esse método, as tags de entidades principais do usuário ou perfil do IAM devem fornecer os detalhes da conexão. Você configura essas etiquetas no AWS Identity and Access Management ou no provedor de identidades (IdP). O editor de consultas v2 se baseia nas etiquetas a seguir.

- `RedshiftDbUser`: essa etiqueta define o usuário do banco de dados usado pelo editor de consultas v2. Essa etiqueta é obrigatória.
- `RedshiftDbGroups`: essa etiqueta define os grupos de banco de dados que são unidos ao se conectar ao editor de consultas v2. Essa etiqueta é opcional e seu valor deve ser uma lista separada por dois pontos, como `group1:group2:group3`. Valores vazios são ignorados, ou seja, `group1::::group2` é interpretado como `group1:group2`.

Essas etiquetas são encaminhadas à API do `redshift:GetClusterCredentials` a fim de obter credenciais para o cluster. Para ter mais informações, consulte Configuração de etiquetas de entidade principal para se conectar a um cluster ou a um grupo de trabalho pelo editor de consultas v2.

Credenciais temporárias usando um nome de usuário do banco de dados

Essa opção só está disponível ao se conectar a um cluster. Com esse método, o editor de consultas v2 fornece um User name (Nome de usuário) para o banco de dados. O editor de consultas v2 gera uma senha temporária para se conectar ao banco de dados como o nome de usuário do banco de dados. Um usuário que usa esse método para se conectar deve ter permissão do IAM para `redshift:GetClusterCredentials`. Para impedir que os usuários usem esse método, modifique o perfil ou usuário do IAM para negar essa permissão.

Credenciais temporárias usando sua identidade do IAM

Essa opção só está disponível ao se conectar a um cluster. Com esse método, o editor de consultas v2 mapeia um nome de usuário para a identidade do IAM e gera

uma senha temporária para se conectar ao banco de dados como a identidade do IAM. Um usuário que usa esse método para se conectar deve ter permissão do IAM para `redshift:GetClusterCredentialsWithIAM`. Para impedir que os usuários usem esse método, modifique o perfil ou usuário do IAM para negar essa permissão.

Nome de usuário e senha do banco de dados

Com esse método, forneça também um User name (Nome de usuário) e uma Password (Senha) para o banco de dados ao qual você está se conectando. O editor de consultas v2 cria um segredo em seu nome armazenado em AWS Secrets Manager. Este segredo contém credenciais para se conectar ao seu banco de dados.

AWS Secrets Manager

Com esse método, em vez de um nome de banco de dados, forneça um Secret (Segredo) armazenado no Secrets Manager que contém seu banco de dados e credenciais de login. Para obter informações sobre como criar um segredo, consulte Criar um segredo para credenciais de conexão de banco de dados.

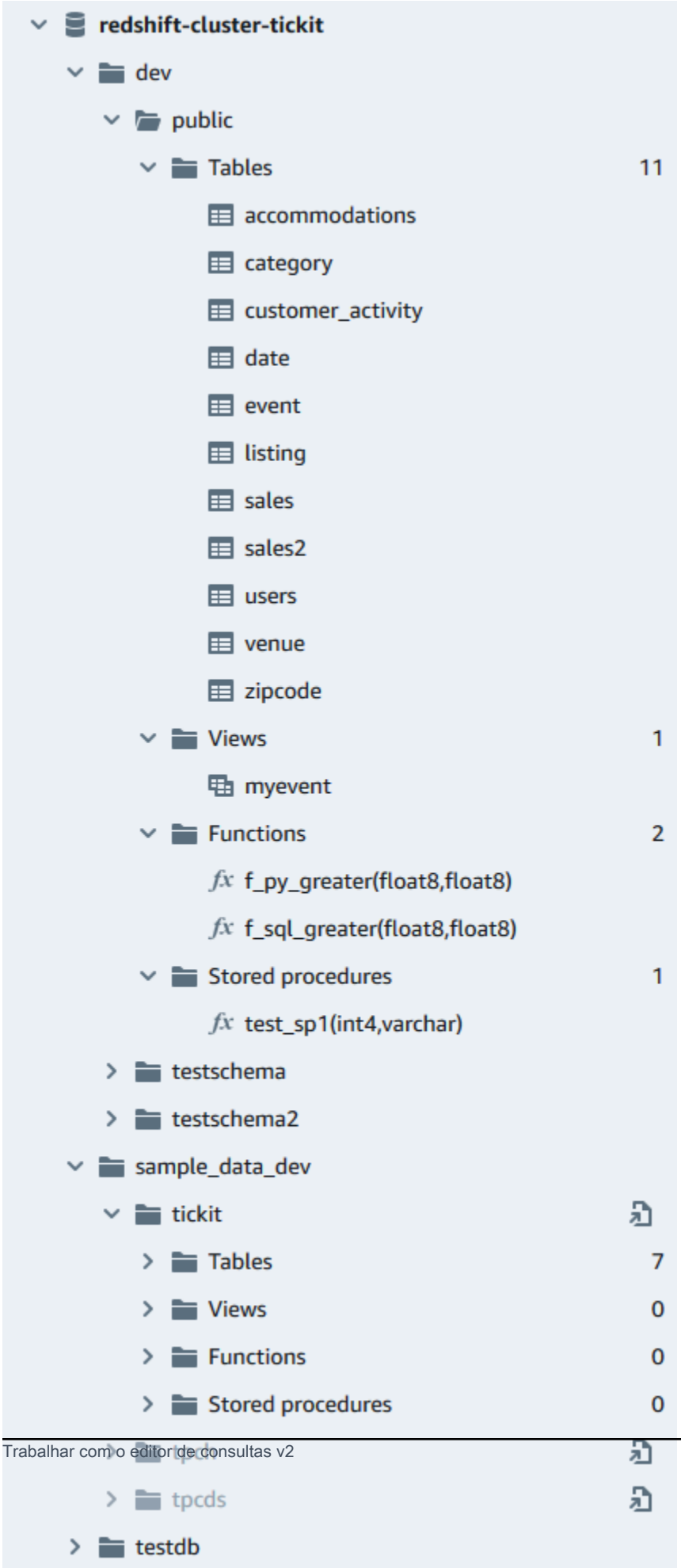
Ao selecionar um cluster ou grupo de trabalho com o editor de consultas v2, dependendo do contexto, é possível criar, editar e excluir conexões usando o menu de contexto (clique com o botão direito do mouse). Você pode visualizar atributos, como o ARN da conexão, escolhendo Detalhes da conexão. Você também pode editar as etiquetas anexadas à conexão.

## Navegar por um banco de dados do Amazon Redshift

Em um banco de dados, você pode gerenciar esquemas, tabelas, visualizações, funções e procedimentos armazenados no painel de exibição em árvore. Cada objeto da exibição tem ações associadas a ele em um menu de contexto (clique com o botão direito do mouse).

O painel de exibição em árvore hierárquica exibe objetos do banco de dados. Para atualizar o painel de visualização em árvore a fim de exibir objetos do banco de dados que possam ter sido criados após a última exibição da visualização em árvore, selecione o ícone
.

Abra o menu de contexto (clique com o botão direito do mouse) de um objeto para ver quais ações você pode executar.


redshift-cluster-tickit
dev
public
Tables 11
accommodations
category
customer_activity
date
event
listing
sales
sales2
users
venue
zipcode
Views 1
myevent
Functions 2
f_py_greater(float8,float8)
f_sql_greater(float8,float8)
Stored procedures 1
test_sp1(int4,varchar)
testschema
testschema2
sample_data_dev
tickit
Tables 7
Views 0
Functions 0
Stored procedures 0
tpcds
tpcds
testdb

Depois de escolher uma tabela, você pode fazer o seguinte:

- Para iniciar uma consulta no editor com uma instrução SELECT que consulta todas as colunas da tabela, use Select table (Selecionar tabela).
- Para ver os atributos ou uma tabela, use Show table definition (Exibir definição de tabela). Use isso para ver nomes de colunas, tipos de coluna, codificação, chaves de distribuição, chaves de classificação e verificar se uma coluna pode conter valores nulos. Para obter mais informações sobre atributos de tabela, consulte CREATE TABLE no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- Para excluir uma tabela, use Delete (Excluir). Você também pode usar Truncate table (Truncar tabela) para excluir todas as linhas da tabela ou Drop table (Descartar tabela) para remover a tabela do banco de dados. Para obter mais informações, consulte TRUNCATE e DROP TABLE no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Escolha um esquema para Refresh (Atualizar) ou Drop schema (Descartar esquema).

Escolha uma visualização para Show view definition (Exibir definição de visualização) ou Drop view (Descartar visualização).

Escolha uma função para Show function definition (Exibir definição de função) ou Drop function (Descartar função).

Escolha um procedimento armazenado para Show procedure definition (Exibir definição de procedimento) ou Drop procedure (Descartar procedimento).

## Criar objetos de banco de dados

É possível criar objetos de banco de dados, inclusive bancos de dados, esquemas, tabelas e funções definidas pelo usuário (UDFs). Você deve estar conectado a um cluster ou grupo de trabalho e a um banco de dados para criar objetos de banco de dados.

### Criar bancos de dados

É possível usar o editor de consultas v2 para criar bancos de dados no cluster ou grupo de trabalho.

#### Para criar um banco de dados

Para obter informações sobre bancos de dados, consulte CREATE DATABASE no Guia do desenvolvedor de banco de dados do Amazon Redshift.

1. Selecione

   Create (Criar) e escolha Database (Banco de dados).
2. Insira um Database name (Nome do banco de dados).
3. (Opcional) Selecione Users and groups (Usuários e grupos) e escolha um Database user (Usuário do banco de dados).
4. (Opcional) Você pode criar o banco de dados por meio da unidade de compartilhamento de dados ou do AWS Glue Data Catalog. Para obter mais informações sobre o AWS Glue, consulte O que é o AWS Glue? no Guia do desenvolvedor do AWS Glue.
   - (Opcional) Selecione Criar usando uma unidade de compartilhamento de dados e escolha Selecione uma unidade de compartilhamento de dados. A lista inclui unidades de compartilhamento de dados do produtor que podem ser usadas para criar uma unidade de compartilhamento de dados do consumidor no cluster ou grupo de trabalho atual.
   - (Opcional) Selecione Criar usando o AWS Glue Data Catalog e Selecione um banco de dados do AWS Glue. Em Esquema do catálogo de dados, insira o nome que será usado para o esquema ao se referir aos dados em um nome de três partes (database.schema.table).
5. Selecione Criar banco de dados.

   O novo banco de dados é exibido no painel de exibição em árvore.

   Ao passar pela etapa opcional de consultar um banco de dados criado por uma unidade de compartilhamento de dados, conecte-se a um banco de dados do Amazon Redshift no cluster ou grupo de trabalho (por exemplo, o banco de dados padrão `dev`) e use a notação de três partes (database.schema.table) que faça referência ao nome do banco de dados que você criou quando selecionou Criar usando uma unidade de compartilhamento de dados. O banco de dados da unidade de compartilhamento de dados está listado na guia “Editor” do editor de consultas v2 mas não está habilitado para conexão direta.

   Ao passar pela etapa opcional de consultar um banco de dados criado por meio de um AWS Glue Data Catalog, conecte-se ao banco de dados do Amazon Redshift no cluster ou grupo de trabalho (por exemplo, o banco de dados padrão `dev`) e use a notação de três partes (database.schema.table) que faça referência ao nome do banco de dados que você criou quando selecionou Criar usando o AWS Glue Data Catalog, o esquema que você nomeou em Esquema do catálogo de dados e a tabela no AWS Glue Data Catalog. Similar a:

```
SELECT * FROM glue-database.glue-schema.glue-table
```

> **Note**
>
> Confirme se conexão com o banco de dados padrão está utilizando o método de conexão Credenciais temporárias usando sua identidade do IAM e se as credenciais do IAM receberam privilégios de uso para o banco de dados do AWS Glue.
>
> ```
> GRANT USAGE ON DATABASE glue-database to "IAM:MyIAMUser"
> ```

O banco de dados do AWS Glue está listado na guia “Editor” do editor de consultas v2 mas não está habilitado para conexão direta.

Para obter mais informações sobre como consultar um AWS Glue Data Catalog, consulte Trabalhar com unidades de compartilhamento de dados gerenciadas pelo Lake Formation como consumidor e Trabalhar com unidades de compartilhamento de dados gerenciadas pelo Lake Formation como produtor no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Exemplo de criação de um banco de dados como consumidor da unidade de compartilhamento de dados

O exemplo a seguir descreve um cenário específico que foi usado para criar um banco de dados com base em uma unidade de compartilhamento de dados usando o editor de consultas v2. Analise esse cenário para saber como você pode criar um banco de dados com base em uma unidade de compartilhamento de dados em seu ambiente. Esse cenário usa dois clusters: `cluster-base` (o cluster do produtor) e `cluster-view` (o cluster do consumidor).

1. Use o console do Amazon Redshift para criar uma unidade de compartilhamento de dados para a tabela `category2` no cluster `cluster-base`. A unidade de compartilhamento de dados do produtor é chamada `datashare_base`.

   Para obter informações sobre como criar unidades de compartilhamento de dados, consulte Compartilhar dados entre clusters no Amazon Redshift no Guia do desenvolvedor de banco de dados do Amazon Redshift.

2. Use o console do Amazon Redshift para aceitar a unidade de compartilhamento de dados `datashare_base` como consumidor para a tabela `category2` no cluster `cluster-view`.
3. Exiba o painel de visualização em árvore no editor de consultas v2, que mostra a hierarquia de `cluster-base` como:

   - Cluster: `cluster-base`
     - Banco de dados: `dev`
       - Esquema: `public`
         - Tabelas: `category2`
4. Selecione Create (Criar) e escolha Database (Banco de dados).
5. Insira `see_datashare_base` em Nome do banco de dados.
6. Selecione Criar usando uma unidade de compartilhamento de dados e escolha Selecione uma unidade de compartilhamento de dados. Escolha `datashare_base` para usar como fonte do banco de dados que você está criando.

   O painel de visualização em árvore no editor de consultas v2 mostra a hierarquia de `cluster-view` como:

   - Cluster: `cluster-view`
     - Banco de dados: `see_datashare_base`
       - Esquema: `public`
         - Tabelas: `category2`
7. Ao consultar os dados, conecte-se ao banco de dados padrão do cluster `cluster-view` (normalmente chamado `dev`), mas faça referência ao banco de dados da unidade de compartilhamento de dados `see_datashare_base` no SQL.

   > **Note**
   >
   > Na visualização do editor de consultas v2, o cluster selecionado é `cluster-view`. O banco de dados selecionado é `dev`. O banco de dados `see_datashare_base` está

listado mas não está habilitado para conexão direta. Você escolhe o banco de dados dev e faz referência a see_datashare_base no SQL que executa.

```
SELECT * FROM "see_datashare_base"."public"."category2";
```

A consulta recupera dados da unidade de compartilhamento de dados datashare_base no cluster cluster_base.

Exemplo de criação de um banco de dados por meio de um AWS Glue Data Catalog

O exemplo a seguir descreve um cenário específico que foi usado para criar um banco de dados por meio de um AWS Glue Data Catalog usando o editor de consultas v2. Analise esse cenário para saber como você pode criar um banco de dados por meio de um AWS Glue Data Catalog em seu ambiente. Esse cenário usa um cluster, cluster-view, para conter o banco de dados que você cria.

1. Selecione Create (Criar) e escolha Database (Banco de dados).
2. Insira data_catalog_database em Nome do banco de dados.
3. Selecione Criar usando um AWS Glue Data Catalog e escolha Selecione um banco de dados do AWS Glue. Escolha glue_db para usar como fonte do banco de dados que você está criando.

   Escolha Esquema do catálogo de dados e insira myschema como o nome do esquema a ser usado na notação de três partes.

   O painel de visualização em árvore no editor de consultas v2 mostra a hierarquia de cluster-view como:

   - Cluster: cluster-view
     - Banco de dados: data_catalog_database
       - Esquema: myschema
         - Tabelas: category3

4. Ao consultar os dados, conecte-se ao banco de dados padrão do cluster `cluster-view` (normalmente chamado `dev`), mas faça referência ao banco de dadosdata_catalog_database no SQL.

   > **Note**
   >
   > Na visualização do editor de consultas v2, o cluster selecionado é `cluster-view`. O banco de dados selecionado é `dev`. O banco de dados `data_catalog_database` está listado mas não está habilitado para conexão direta. Você escolhe o banco de dados `dev` e faz referência a `data_catalog_database` no SQL que executa.

   ```
   SELECT * FROM "data_catalog_database"."myschema"."category3";
   ```

   A consulta recupera dados catalogados pelo AWS Glue Data Catalog.

Criar esquemas

É possível usar o editor de consultas v2 para criar esquemas no cluster ou grupo de trabalho.

Para criar um esquema

Para obter informações sobre esquemas, consulte Esquemas no Guia do desenvolvedor de banco de dados do Amazon Redshift.

1. Selecione (Criar) e escolha Schema (Esquema). Create
2. Digite um Schema name (Nome do esquema).
3. Escolha Local ou External (Externo) como Schema type (Tipo de esquema).

   Para obter mais informações sobre esquemas, consulte CREATE SCHEMA no Guia do desenvolvedor de banco de dados do Amazon Redshift. Para obter mais informações sobre esquemas, consulte EXTERNAL SCHEMA no Guia do desenvolvedor de banco de dados do Amazon Redshift.
4. Se escolher External (Externo), você terá as opções de um esquema externo a seguir.

- Glue Data Catalog: para criar um esquema externo no Amazon Redshift que se refira a tabelas no AWS Glue. Além de escolher o banco de dados do AWS Glue, selecione o perfil do IAM associado ao cluster e o perfil do IAM associado ao catálogo de dados.
- PostgreSQL: para criar um esquema externo no Amazon Redshift que se refira a um banco de dados do Amazon RDS para PostgreSQL ou do Amazon Aurora compatível com PostgreSQL. Forneça também as informações de conexão com o banco de dados. Para obter mais informações sobre consultas federadas, consulte Querying data with federated queries (Consultar dados com consultas federadas) no Guia do .de banco de dados do Amazon Redshift.
- MySQL: para criar um esquema externo no Amazon Redshift que se refira a um banco de dados do Amazon RDS para MySQL ou do Amazon Aurora compatível com MySQL. Forneça também as informações de conexão com o banco de dados. Para obter mais informações sobre consultas federadas, consulte Querying data with federated queries (Consultar dados com consultas federadas) no Guia do .de banco de dados do Amazon Redshift.

5. Selecione Create schema (Criar esquema).

   O novo esquema aparece no painel de exibição em árvore.

## Criar tabelas

Você pode usar o editor de consultas v2 para criar tabelas no cluster ou grupo de trabalho.

### Para criar uma tabela do

É possível criar uma tabela com base em um arquivo de valores separados por vírgulas (CSV) especificado ou define cada coluna da tabela. Para obter mais informações, consulte Design de tabelas e CREATE TABLE no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Selecione Open query in editor (Abrir consulta no editor) para visualizar e editar a instrução CREATE TABLE antes de executar a consulta para criar a tabela.

1. Escolha

   Create (Criar) Table (Tabela).
2. Escolha um esquema.
3. Escolha um nome da tabela.

4. Selecione

   Add field (Adicionar campo) para adicionar uma coluna.
5. Use um arquivo CSV como modelo para a definição da tabela:

   a. Selecione Load from CSV (Carregar do CSV).
   b. Navegue até o local do arquivo.

      Se você usar um arquivo CSV, certifique-se de que a primeira linha do arquivo contém os cabeçalhos da coluna.
   c. Escolha o arquivo selecione Open (Abrir). Confirme que os nomes das colunas e os tipos de dados são os que você deseja.
6. Para cada coluna, escolha a coluna e as opções que deseja:

   - Escolha um valor para Encoding (Codificação).
   - Escolha um Default value (Valor padrão).
   - Ative Automatically increment (Incrementar automaticamente), se quiser que os valores da coluna sejam incrementados. Em seguida, especifique um valor para o Auto increment seed (Incrementar seed automaticamente) e Auto increment step (Etapa de incremento automático).
   - Ative Not NULL (Não NULL), se a coluna deve sempre conter um valor.
   - Digite o valor de Size (Tamanho) para a coluna.
   - Ative Primary key (Chave primária), se quiser que a coluna seja uma chave primária.
   - Ative Unique key (Chave exclusiva), se quiser que a coluna seja uma chave exclusiva.
7. (Opcional) Escolha Table details (Detalhes da tabela) e selecione uma das opções a seguir:

   - Coluna e estilo da chave de distribuição.
   - Coluna de chave de classificação e tipo de classificação.
   - Ative Backup para incluir a tabela em snapshots.
   - Ative Temporary table (Tabela temporária) para criar a tabela como uma tabela temporária.
8. Selecione Open query in editor (Abrir consulta no editor) para continuar especificando opções para definir a tabela ou escolha Create table (Criar tabela) para criar a tabela.

### Criar funções

É possível usar o editor de consultas v2 para criar funções no cluster ou grupo de trabalho.

Como criar uma função do

1. Selecione

   Create
   (Criar) e escolha Function (Função).
2. Em Type (Tipo), escolha SQL ou Python.
3. Escolha um valor para Schema (Esquema).
4. Insira um valor para Name (Nome) da função.
5. Insira um valor para Volatility (Volatilidade) da função.
6. Selecione Parameters (Parâmetros) por tipos de dados na ordem dos parâmetros de entrada.
7. Em Returns (Retornos), escolha um tipo de dados.
8. Insira o código do programa SQL ou programa Python da função.
9. Escolha Criar.

Para obter mais informações sobre funções definidas pelo usuário (UDFs), consulte Criar funções definidas pelo usuário no Guia do desenvolvedor de banco de dados do Amazon Redshift.

## Visualizar o histórico de consultas e guias

É possível ver seu histórico de consultas com o editor de consultas v2. Somente as consultas que você executou usando o editor de consultas v2 aparecem no histórico de consultas. Tanto as consultas executadas usando uma guia Editor ou uma guia Notebook (Caderno) são exibidas. É possível filtrar a lista exibida por um período, como `This week`, em que uma semana é definida como de segunda a domingo. A lista de consultas retorna 25 linhas de consultas por vez que correspondem ao seu filtro. Selecione Load more (Carregar mais) para ver o próximo conjunto. Selecione uma consulta. No menu Actions (Ações), As ações disponíveis dependem de a consulta escolhida ter sido salva. É possível selecionar as seguintes operações:

- View query details (Visualizar detalhes da consulta): exibe uma página de detalhes da consulta com mais informações sobre a consulta executada.
- Open query in a new tab (Abrir consulta em uma nova guia): abre uma nova guia do editor e a prepara com a consulta escolhida. Se ainda estiver conectado, o cluster ou o grupo de trabalho e o banco de dados serão selecionados automaticamente. Para executar a consulta, primeiro confirme se o cluster ou grupo de trabalho e o banco de dados corretos foram escolhidos.

- Open source tab (Aba de código aberto): se ainda estiver aberta, acessa a guia do editor ou do caderno que continha a consulta quando ela foi executada. O conteúdo do editor ou do caderno pode ter mudado após a execução da consulta.
- Open saved query (Abrir consulta salva): acessa a guia do editor ou do caderno e abre a consulta.

Também é possível visualizar o histórico das consultas executadas em uma guia Editor ou o histórico das consultas executadas em uma guia Notebook (Caderno). Para ver um histórico de consultas em uma guia, selecione Tab history (Histórico da guia). No histórico da guia, é possível executar as seguintes operações:

- Copy query (Copiar consulta): copia o conteúdo SQL da versão da consulta para a área de transferência.
- Open query in a new tab (Abrir consulta em uma nova guia): abre uma nova guia do editor e a prepara com a consulta escolhida. Para executar a consulta, você deve escolher o cluster ou o grupo de trabalho e o banco de dados.
- View query details (Visualizar detalhes da consulta): exibe uma página de detalhes da consulta com mais informações sobre a consulta executada.

## Considerações ao trabalhar com o editor de consultas v2

Considere o seguinte ao trabalhar com o editor de consultas v2:

- O tamanho máximo do resultado da consulta é 5 MB ou 100 mil linhas, o que for menor.
- É possível salvar uma consulta de até 300 mil caracteres.
- É possível salvar uma consulta de até 30 mil caracteres.
- Por padrão, o editor de consultas v2 confirma automaticamente cada comando SQL individual executado. Quando uma instrução BEGIN é fornecida, as instruções no bloco BEGIN-COMMIT ou BEGIN-ROLLBACK são executadas como uma única transação. Para obter mais informações sobre transações, consulte BEGIN no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- O número máximo de avisos que o editor de consultas v2 exibe ao executar uma instrução SQL é `10`. Por exemplo, quando um procedimento armazenado é executado, não mais de dez instruções RAISE são exibidas.
- O editor de consultas v2 não é compatível com um `RoleSessionName` do IAM que contenha vírgula (,). Você pode ver um erro semelhante ao seguinte: Mensagem de erro:

"'AROA123456789EXAMPLE:mytext,yourtext' is not a valid value for TagValue - it contains illegal characters". Esse problema surge quando você define um `RoleSessionName` do IAM que inclui uma vírgula e usa o editor de consultas v2 com esse perfil do IAM.

Para obter mais informações sobre um `RoleSessionName` do IAM, consulte Atributo SAML RoleSessionName no Guia do usuário do IAM.

### Alterar as configurações da conta

Um usuário com as permissões corretas do IAM pode visualizar e alterar Account settings (Configurações da conta) para outros usuários na mesma Conta da AWS. Esse administrador pode exibir ou definir o seguinte:

- O máximo de conexões simultâneas de banco de dados por usuário na conta. Isso inclui conexões para Isolated sessions (Sessão isoladas). Quando você altera esse valor, pode levar 10 minutos para que a mudança tenha efeito.
- Permita que os usuários da conta exportem um conjunto inteiro de resultados de um comando SQL para um arquivo.
- Carregue e exiba bancos de dados de exemplo com algumas consultas salvas correspondentes.
- Especifique um caminho do Amazon S3 usado pelos usuários da conta para carregar dados de um arquivo local.
- Visualize o ARN da chave do KMS a ser usada para criptografar os recursos do editor de consultas v2.

## Interação com o SQL generativo do editor de consultas v2 (visualização)

Esta é uma documentação de pré-lançamento SQL generativo do editor de consultas v2, que está em lançamento de visualização. A documentação e o atributo estão sujeitos a alteraçõe s. Recomendamos o uso desse recurso somente em ambientes de teste, e não em ambientes de produção. Para previsualizar termos e condições, consulte Participação no serviço beta nos Termos de Serviço da AWS.

> **Note**
>
> Atualmente, o suporte ao SQL generativo só está disponível nas seguintes Regiões da AWS:

- Região Leste dos EUA (Norte da Virgínia) (us-east-1)
- Região Oeste dos EUA (Oregon) (us-west-2)

É possível interagir com o recurso SQL generativo do Amazon Q no editor de consultas do Amazon Redshift v2. Trata-se de um assistente de codificação que gera instruções SQL com base nos prompts e no esquema do banco de dados. Esse assistente de codificação está disponível enquanto você cria um notebook no editor de consultas v2.

Ao interagir com o SQL generativo, faça perguntas específicas, itere quando tiver solicitações complexas e verifique se as respostas estão corretas.

Ao fornecer solicitações de análise em linguagem natural, tente usar o máximo de especificidade para ajudar o assistente de codificação a compreender exatamente aquilo de que você precisa. Em vez de perguntar "encontre os espaços que mais venderam ingressos", dê mais detalhes como "encontre nomes/IDs dos três espaços que mais venderam ingressos em 2008". Use nomes consistentes de objetos no banco de dados, como nomes de esquema, tabela e coluna, conforme definido no banco de dados, em vez de se referir ao mesmo objeto de maneiras diferentes, o que pode confundir o assistente.

Divida solicitações complexas em várias declarações simples que sejam mais fáceis do assistente interpretar. Faça perguntas de acompanhamento de maneira iterativa para obter uma análise mais detalhada do assistente. Por exemplo, pergunte primeiro "qual estado tem mais espaços?" Em seguida, com base na resposta, pergunte "qual é o espaço mais conhecido desse estado?".

Revise o SQL gerado antes de executá-lo para garantir a precisão. Se a consulta SQL gerada tiver erros ou não corresponder à intenção, dê instruções ao assistente sobre como corrigi-la, em vez de reformular a solicitação inteira. Por exemplo, se a consulta não tiver uma cláusula de predicado no ano, peça "Dê locais do ano de 2008".

## Considerações ao interagir com SQL generativo

Considere o seguinte ao trabalhar no painel de chat:

- O administrador do editor de consultas v2 da conta deve ter ativado o recurso de chat na página Configurações do SQL generativo.
- Para usar o SQL generativo do editor de consultas v2, você precisa da permissão `sqlworkbench:GetQSqlRecommendations` na política do IAM, além de outras permissões

especificadas na política gerenciada pela AWS do editor de consultas v2. Para obter mais informações sobre políticas gerenciadas pela AWS, consulte Acessar o editor de consultas v2.

- As perguntas devem ser escritas em inglês.
- As perguntas devem fazer referência ao banco de dados conectado no cluster ou no grupo de trabalho. Para evitar erros de estado vazio, deve haver pelo menos uma tabela e alguns dados no banco de dados.
- As perguntas devem fazer referência aos dados armazenados no banco de dados conectado. Eles não podem fazer referência a um esquema externo. Para obter mais informações sobre os esquemas compatíveis, consulte Create schema no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- Qualquer dúvida que resulte em um SQL que altere o banco de dados conectado pode resultar em um aviso.
- A tecnologia de IA generativa é nova e pode haver erros, às vezes chamados de alucinações, nas respostas. Teste e analise todo o código em busca de erros e vulnerabilidades antes de usá-lo no ambiente ou no workload.
- Você pode melhorar as recomendações compartilhando as consultas SQL executadas por outros usuários na conta. O administrador da conta pode executar os seguintes comandos SQL para permitir o acesso ao histórico de consultas da conta.

```
GRANT ROLE SYS:MONITOR to "IAMR:role-name";
GRANT ROLE SYS:MONITOR to "IAM:user-name";
GRANT ROLE SYS:MONITOR to "database-username";
```

  Para obter mais informações sobre `SYS:MONITOR`, consulte Amazon Redshift system-defined roles no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- Os dados são seguros e privados. Os dados não são compartilhados entre contas. As consultas, os dados e os esquemas de banco de dados não são usados para treinar um modelo de base (FM) de IA generativa. A entrada é usada como solicitações contextuais para o FM responder apenas às consultas.

## Uso do SQL generativo

Depois que as permissões corretas forem configuradas, ao trabalhar com um notebook no editor de consultas v2, você poderá escolher um ícone para iniciar uma conversa.

Para interagir com o chat SQL generativo do editor de consultas v2 para gerar SQL

1. Na guia Editor do editor de consultas v2, abra um noteook.
2. Escolha o ícone de SQL generativo

   e siga as instruções para fazer as perguntas ao SQL generativo do editor de consultas do Amazon Redshift v2 no painel de chat.

   Você faz perguntas em um campo de prompt, e o editor de consultas v2 responde com o SQL sugerido. Todos os erros encontrados são retornados para você no painel de chat.
3. Escolha Adicionar ao notebook para adicionar uma célula Markdown com o prompt e uma célula SQL com o SQL sugerido ao notebook.
4. (Opcional) Escolha Regenerar SQL para gerar outra resposta para o mesmo prompt. É possível optar por Regenerar SQL uma vez para o prompt atual.
5. (Opcional) No painel de chat do SQL generativo, escolha o ícone

   Mais e Atualizar banco de dados para atualizar os metadados que descrevem o banco de dados conectado. Esses metadados incluem as definições de esquemas, tabelas e colunas no banco de dados.

## Atualização de configurações do SQL generativo como administrador

Um usuário com as permissões do IAM corretas pode exibir e alterar Configurações do SQL generativo de outros usuários na mesma Conta da AWS. Esse administrador deve ter permissão `sqlworkbench:UpdateAccountQSqlSettings` na política do IAM, além de outras permissões especificadas na política gerenciada pelo AWS para o editor de consultas v2. Para obter mais informações sobre políticas gerenciadas, consulte Permissões necessárias para usar o editor de consultas v2 .

Para um administrador ativar o chat SQL generativo para todos os usuários da conta

1. Um ícone

   Configurações para mostrar um menu das telas de configurações diferentes.

2. Em seguida, escolha o ícone

de configurações do SQL generativo para mostrar a página Configurações do SQL generativo.

3. Selecione SQL generativo a fim de ativar o recurso de SQL generativo para usuários na conta.

## Exemplo de uso do recurso SQL generativo do Amazon Q com os dados TICKIT

Para criar solicitações eficientes a fim de gerar SQL, você deve aprender mais sobre o esquema do banco de dados e os dados. Os dados TICKIT consistem em sete tabelas: duas de fatos e cinco de dimensões. Os dados de exemplo contêm registros sobre vendas a participantes de eventos do entretenimento ocorridos em 2008. Para obter informações sobre o esquema de dados TICKIT, consulte Sample database no Guia de desenvolvedor de banco de dados do Amazon Redshift. É possível carregar os dados do TICKIT em um banco de dados por vários métodos no console do Amazon Redshift e no editor de consultas v2. O editor de consultas v2 oferece um método para carregar dados TICKIT no banco de dados `sample_data_dev`. Para obter mais informações, consulte Carregar dados de exemplo. O editor de consultas v2 também oferece solicitações de exemplo para os dados do TICKIT. O cenário a seguir descreve uma conversa com SQL generativo para gerar SQL sobre os dados de exemplo do TICKIT. Nesse cenário, os dados de exemplo do TICKIT já foram criados em um banco de dados `dev` em um cluster do Amazon Redshift.

> **Note**
>
> Este exemplo serve para ilustrar uma conversa. As respostas do SQL generativo talvez não correspondam aos resultados usando as mesmas solicitações.

Conversa de exemplo com o SQL generativo do editor de consultas v2

1. No Editor, conecte-se a um cluster ou a um grupo de trabalho que contenha os dados de exemplo do TICKIT.
2. Crie um notebook vazio e escolha o ícone

de SQL generativo para abrir o painel de chat.

3. Insira a seguinte solicitação a fim de gerar SQL para verificar o número de registros na tabela `VENUE`:

```
How many venues are there?
```

```
SELECT
  COUNT(*) AS num_venues
FROM
  tickit.venue
```

Escolha Adicionar ao notebook para adicionar duas células ao notebook aberto. Uma célula Markdown "Existem quantos espaços?" e uma contendo o SQL gerado.

Na célula SQL, escolha Executar para receber o resultado:

```
count
------
202
```

4. Para solicitar outra versão do SQL, escolha Regenerar SQL e receba a seguinte resposta:

```
SELECT
  venuestate,
  COUNT(*) AS num_venues
FROM
  tickit.venue
GROUP BY
  venuestate
```

Escolha Adicionar ao notebook para adicionar mais duas células ao notebook aberto. Uma célula Markdown "Existem quantos espaços?" e uma contendo o SQL gerado.

Na célula SQL, escolha Executar para receber o resultado listando os estados do espaço por número:

```
venuestate num_venues
----------------------
MA         4
OH         8
MI         5
```

```
...
```

5. O assistente de SQL generativo pode fazer suposições sobre o que você está perguntando. Embora não haja widgets no banco de dados, você ainda pode perguntar. Nesse caso, ele exibe uma mensagem de que não foi possível gerar SQL.

```
How many widgets are there?
```

```


I was not able to generate any SQL
```

6. À medida que aprende mais sobre o banco de dados, você pode fazer perguntas mais específicas para gerar SQL. Por exemplo, você sabe que o banco de dados contém dados de vendas referentes a diversos meses em 2008. Insira a seguinte solicitação a fim de gerar SQL para encontrar o número de vendas em novembro de 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
```

Escolha Adicionar ao notebook para adicionar duas células ao notebook aberto. Uma célula Markdown "Quantas vendas houve em novembro de 2008?" e uma contendo o SQL gerado.

Na célula SQL, escolha Executar para receber o resultado:

```
num_sales
-----
0
```

Você percebe que não se trata do resultado que estava esperando.

7. Você percebe que o predicado `date.month='November'` espera que o mês na tabela DATE seja representado por uma abreviação do nome do mês. Você altera o predicado para `d.month='NOV'` e reexecuta o SQL.

```
SELECT
  COUNT(*)
FROM
  sales
  JOIN date ON sales.dateid = date.dateid
WHERE
  date.month = 'NOV'
  AND date.year = 2008
```

   Na célula SQL, escolha Executar para obter novos resultados.

```
count
-----
14261
```

8. Se você fizer uma pergunta que tente alterar o banco de dados conectado, uma mensagem de aviso será retornada com qualquer SQL recomendado. Insira a seguinte solicitação a fim de gerar SQL para inserir dados em uma tabela:

```
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.
```

Se você escolher Adicionar ao notebook para adicionar duas células ao notebook aberto e executar o SQL, haverá falha no SQL.

```
ERROR: syntax error at or near "," Position: 132 [ErrorId:
 1-6546764a-011df2691778846219ce6ec2]
```

Esse cenário só ilustrou algumas maneiras básicas de interagir com o SQL generativo do editor de consultas v2. É possível experimentar ainda mais usando essa tecnologia de IA generativa a fim de ajudar você a começar a criar SQL para consultar o banco de dados.

## Carregar dados em um banco de dados

É possível usar o editor de consultas v2 para carregar dados em um banco de dados em um cluster ou um grupo de trabalho do Amazon Redshift.

### Carregar dados de exemplo

O editor de consultas v2 vem com dados e blocos de anotações de exemplo disponíveis para serem carregados em um banco de dados de exemplo e esquema correspondente.

Para carregar dados de exemplo, escolha o ícone

associado aos dados de exemplo que você deseja carregar. Depois, o editor de consultas v2 carrega os dados em um esquema no banco de dados `sample_data_dev` e cria uma pasta de blocos de anotações salvos em sua pasta Notebooks (Blocos de anotações).

Os conjuntos de dados de exemplo a seguir estão disponíveis.

tickit

A maioria dos exemplos na documentação do Amazon Redshift usa um exemplo de dados chamado `tickit`. Esses dados consistem em sete tabelas: duas de fatos e cinco de dimensões. Quando você carrega esses dados, o esquema `tickit` é atualizado com dados de exemplo. Para obter informações sobre dados `tickit`, consulte Banco de dados de exemplo no Guia do desenvolvedor de banco de dados do Amazon Redshift.

tpch

Esses dados são usados para um parâmetro de comparação de apoio a decisões. Quando você carrega esses dados, o esquema `tpch` é atualizado com dados de exemplo. Para obter mais informações sobre os tipos de dados `tpch`, consulte TPC-H.

tpcds

Esses dados são usados para um parâmetro de comparação de apoio a decisões. Quando você carrega esses dados, o esquema `tpcds` é atualizado com dados de exemplo. Para obter mais informações sobre os tipos de dados `tpcds`, consulte TPC-DC.

## Carregar dados do Amazon S3

É possível carregar dados do Amazon S3 em uma tabela nova ou existente.

Para carregar dados para uma tabela existente

O editor de consulta v2 utiliza o comando COPY para carregar dados do Amazon S3. O comando COPY gerado e usado no assistente de carregamento de dados do editor de consultas v2 é compatível com muitos parâmetros disponíveis para a sintaxe do comando COPY para copiar do Amazon S3. Para obter informações sobre o comando COPY e suas opções usadas para carregar dados do Amazon S3, consulte COPY do Amazon Simple Storage Service no Guia do desenvolvedor de banco de dados do Amazon Redshift.

1. Confirme se já foi criada a tabela no banco de dados onde você deseja carregar dados.
2. Confirme se você está conectado ao banco de dados de destino no painel de visualização em árvore do editor de consultas v2 antes de continuar. É possível criar uma conexão usando o menu de contexto (clique com o botão direito do mouse) para o cluster ou o grupo de trabalho no qual os dados serão carregados.

   Selecione

   Load data (Carregar dados).
3. Em Fonte de dados, selecione Carregar de um bucket do S3.
4. Em S3 URIs (URIs do S3), escolha Browse S3 (Navegar pelo S3) para procurar o bucket do Amazon S3 que contém os dados a serem carregados.

5. Se o bucket do Amazon S3 especificado não estiver na mesma Região da AWS que a tabela de destino, selecione a S3 file location (Localização do arquivo do S3) para a Região da AWS onde os dados estão localizados.
6. Selecione This file is a manifest file (Este arquivo é um arquivo manifesto) se o arquivo do Amazon S3 for um manifesto contendo vários URIs de bucket do Amazon S3.
7. Selecione o File format (Formato do arquivo) para o arquivo a ser carregado. Os formatos de dados compatíveis são CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET e ORC. Dependendo do formato de arquivo especificado, é possível escolher a respectivas File options (Opções de arquivos). Você também pode selecionar Data is encrypted (Os dados são criptografados), se os dados estiverem criptografados, e inserir o nome do recurso da Amazon (ARN) da chave KMS usada para criptografar os dados.

   Se você escolher CSV ou DELIMITADOR, também poderá escolher o Caractere delimitador e decidir se deseja Ignorar linhas de cabeçalho se o número especificado de linhas for nomes de colunas em vez de dados a serem carregados.
8. Escolha um método de compactação para compactar o arquivo. O padrão é sem compactação.
9. (Opcional) Advanced settings (Configurações avançadas) oferece suporte a vários parâmetros da conversão de dados e operações de carregamento. Insira essas informações conforme necessário para o arquivo.

   Para obter mais informações sobre conversão de dados e parâmetros de carregamento de dados, consulte Parâmetros de conversão de dados e Operações de carregamento de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift.
10. Escolha Next (Próximo).
11. Escolha Carregar tabela existente.
12. Confirme ou selecione a localização da Target table (Tabela de destino), incluindo Cluster or workgroup (Cluster ou grupo de trabalho), Database (Banco de dados), Schema (Esquema) e Table (Tabela) em que os dados serão carregados.
13. Escolha uma função do IAM que tenha as permissões necessários para carregar dados do Amazon S3.
14. (Opcional) Selecione os nomes das colunas para inseri-las em Column mapping (Mapeamento de colunas) para mapear colunas na ordem do arquivo de dados de entrada.
15. Selecione Load data (Carregar dados) para iniciar o carregamento de dados.

Quando o carregamento for concluído, exibe-se o editor de consultas o comando COPY gerado que foi usado para carregar seus dados. Exibe-se Result (Resultado) do COPY. Se for concluído corretamente, agora você poderá usar o SQL para selecionar dados da tabela carregada. Quando houver um erro, consulte a visualização do sistema STL_LOAD_ERRORS para obter mais detalhes. Para obter informações sobre erros do comando COPY, consulte STL_LOAD_ERRORS no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Quando você carrega dados em uma nova tabela, o editor de consultas v2 cria a tabela no banco de dados, depois carrega os dados como ações separadas no mesmo fluxo de trabalho.

Como carregar dados em uma nova tabela

O editor de consulta v2 utiliza o comando COPY para carregar dados do Amazon S3. O comando COPY gerado e usado no assistente de carregamento de dados do editor de consultas v2 é compatível com muitos parâmetros disponíveis para a sintaxe do comando COPY para copiar do Amazon S3. Para obter informações sobre o comando COPY e suas opções usadas para carregar dados do Amazon S3, consulte COPY do Amazon Simple Storage Service no Guia do desenvolvedor de banco de dados do Amazon Redshift.

1. Confirme se você está conectado ao banco de dados de destino no painel de visualização em árvore do editor de consultas v2 antes de continuar. É possível criar uma conexão usando o menu de contexto (clique com o botão direito do mouse) para o cluster ou o grupo de trabalho no qual os dados serão carregados.

   Selecione Load data (Carregar dados).
2. Em Fonte de dados, selecione Carregar de um bucket do S3.
3. Em S3 URIs (URIs do S3), escolha Browse S3 (Navegar pelo S3) para procurar o bucket do Amazon S3 que contém os dados a serem carregados.
4. Se o bucket do Amazon S3 especificado não estiver na mesma Região da AWS que a tabela de destino, selecione a S3 file location (Localização do arquivo do S3) para a Região da AWS onde os dados estão localizados.
5. Selecione This file is a manifest file (Este arquivo é um arquivo manifesto) se o arquivo do Amazon S3 for um manifesto contendo vários URIs de bucket do Amazon S3.

6. Selecione o File format (Formato do arquivo) para o arquivo a ser carregado. Os formatos de dados compatíveis são CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET e ORC. Dependendo do formato de arquivo especificado, é possível escolher a respectivas File options (Opções de arquivos). Você também pode selecionar Data is encrypted (Os dados são criptografados), se os dados estiverem criptografados, e inserir o nome do recurso da Amazon (ARN) da chave KMS usada para criptografar os dados.

   Se você escolher CSV ou DELIMITADOR, também poderá escolher o Caractere delimitador e decidir se deseja Ignorar linhas de cabeçalho se o número especificado de linhas for nomes de colunas em vez de dados a serem carregados.
7. Escolha um método de compactação para compactar o arquivo. O padrão é sem compactação.
8. (Opcional) Advanced settings (Configurações avançadas) oferece suporte a vários parâmetros da conversão de dados e operações de carregamento. Insira essas informações conforme necessário para o arquivo.

   Para obter mais informações sobre conversão de dados e parâmetros de carregamento de dados, consulte Parâmetros de conversão de dados e Operações de carregamento de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift.
9. Escolha Next (Próximo).
10. Escolha Carregar nova tabela.

    As colunas da tabela são inferidas dos dados de entrada. Você pode modificar a definição do esquema da tabela adicionando colunas e detalhes da tabela. Para reverter para o esquema de tabela inferida do editor de consultas v2, escolha Restaurar os padrões.
11. Confirme ou selecione a localização da Tabela de destino, incluindo o Cluster ou grupo de trabalho, o Banco de dados e o Esquema em que os dados são carregados. Insira um nome para a Tabela que será criada.
12. Escolha uma função do IAM que tenha as permissões necessários para carregar dados do Amazon S3.
13. Escolha Criar tabela para criar a tabela usando a definição mostrada.

    Um resumo é exibido para revisão da definição da tabela. A tabela é criada no banco de dados. Para excluir a tabela posteriormente, execute um comando SQL DROP TABLE. Para obter mais informações, consulte DROP TABLE no Guia do desenvolvedor de banco de dados do Amazon Redshift.
14. Selecione Load data (Carregar dados) para iniciar o carregamento de dados.

Quando o carregamento for concluído, exibe-se o editor de consultas o comando COPY gerado que foi usado para carregar seus dados. Exibe-se Result (Resultado) do COPY. Se for concluído corretamente, agora você poderá usar o SQL para selecionar dados da tabela carregada. Quando houver um erro, consulte a visualização do sistema STL_LOAD_ERRORS para obter mais detalhes. Para obter informações sobre erros do comando COPY, consulte STL_LOAD_ERRORS no Guia do desenvolvedor de banco de dados do Amazon Redshift.

## Carregar dados de uma configuração e fluxo de trabalho de arquivo local

É possível carregar dados de um arquivo local em uma tabela nova ou existente.

Configuração do administrador para carregar dados de um arquivo local

Seu administrador do editor de consultas v2 deve especificar o bucket comum do Amazon S3 na janela Account settings (Configurações da conta). Os usuários da conta devem ser configurados com as permissões adequadas.

- Permissões necessárias do IAM: os usuários que carregam do arquivo local devem ter as permissões `s3:ListBucket`, `s3:GetBucketLocation`, `s3:putObject`, `s3:getObject` e `s3:deleteObject`. O *`prefixo opcional`* pode ser especificado para limitar o uso desse bucket relacionado ao editor de consultas v2 a objetos com esse prefixo. Você pode usar essa opção ao usar esse mesmo bucket do Amazon S3 para outros usos além do editor de consultas v2. Para obter mais informações sobre buckets e prefixos, consulte Managing user access to specific folders (Gerenciar o acesso do usuário a pastas específicas) no Guia do usuário do Amazon Simple Storage Service. Para garantir que não seja permitido o acesso aos dados entre usuários, recomendamos que o administrador do editor de consultas v2 use uma política de bucket do Amazon S3 para restringir o acesso a objetos com base em `aws:userid`. O exemplo a seguir trata de permissões do Amazon S3 para um *`<staging-bucket-name>`* com acesso de leitura/gravação somente a objetos do Amazon S3 com `aws:userid` como um prefixo.

```
{
    "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}/*"
            ]
        }
    ]
}
```

- Separação de dados: recomendamos que os usuários não tenham acesso aos dados uns dos outros (mesmo que brevemente). O carregamento de um arquivo local usa o bucket de preparação do Amazon S3 configurado pelo administrador do editor de consultas v2. Configure a política para o bucket de preparação a fim de fornecer separação de dados entre usuários. O exemplo a seguir mostra uma política de bucket que separa os dados entre os usuários do *<staging-bucket-name>*.

```
{
 "Version": "2012-10-17",
    "Statement": [
        {"Sid": "userIdPolicy",
            "Effect": "Deny",
            "Principal": "*",
            "Action": ["s3:PutObject",
                       "s3:GetObject",
                       "s3:DeleteObject"],
            "NotResource": [
                "arn:aws:s3:::<staging-bucket-name>[/<optional-prefix>]/
${aws:userid}/*"
            ]
         }
    ]
```

```
}
```

### Carregar dados de um arquivo local

#### Como carregar dados de um arquivo local em uma tabela existente

O administrador do editor de consultas v2 deve especificar o bucket comum do Amazon S3 na janela Configurações da conta. O editor de consultas v2 carrega automaticamente o arquivo local em um bucket comum do Amazon S3 utilizado por sua conta, depois usa o comando COPY para carregar dados. O comando COPY gerado e executado pela janela Load local file (Carregar arquivo local) do editor de consultas v2 é compatível com muitos parâmetros disponíveis para a sintaxe do comando COPY para copiar do Amazon S3. Para obter informações sobre o comando COPY e suas opções usadas para carregar dados do Amazon S3, consulte COPY from Amazon S3 (COPY do Amazon S3) no Guia do desenvolvedor de banco de dados do Amazon Redshift.

1. Confirme se já foi criada a tabela no banco de dados onde você deseja carregar dados.
2. Confirme se você está conectado ao banco de dados de destino no painel de visualização em árvore do editor de consultas v2. É possível criar uma conexão usando o menu de contexto (clique com o botão direito do mouse) para o cluster ou o grupo de trabalho no qual os dados serão carregados.
3. Selecione Load data (Carregar dados).
4. Em Data source (Fonte de dados), selecione Load from local file (Carregar do arquivo local).
5. Selecione Procurar para procurar o arquivo que contém os dados e Carregar arquivo. Por padrão, são exibidos arquivos com extensão `.csv`, `.avro`, `.parquet` e `.orc`, mas você pode escolher outros tipos de arquivo. O tamanho máximo do arquivo é de 5 MB.
6. Selecione o File format (Formato do arquivo) para o arquivo a ser carregado. Os formatos de dados compatíveis são CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET e ORC. Dependendo do formato de arquivo especificado, é possível escolher a respectivas File options (Opções de arquivos). Você também pode selecionar Data is encrypted (Os dados são criptografados), se os dados estiverem criptografados, e inserir o nome do recurso da Amazon (ARN) da chave KMS usada para criptografar os dados.

Se você escolher CSV ou DELIMITADOR, também poderá escolher o Caractere delimitador e decidir se deseja Ignorar linhas de cabeçalho se o número especificado de linhas for nomes de colunas em vez de dados a serem carregados.

7. (Opcional) Advanced settings (Configurações avançadas) oferece suporte a vários parâmetros da conversão de dados e operações de carregamento. Insira essas informações conforme necessário para o arquivo.

   Para obter mais informações sobre conversão de dados e parâmetros de carregamento de dados, consulte Parâmetros de conversão de dados e Operações de carregamento de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift.

8. Escolha Next (Próximo).
9. Escolha Carregar tabela existente.
10. Confirme ou selecione a localização da Target table (Tabela de destino), incluindo Cluster or workgroup (Cluster ou grupo de trabalho), Database (Banco de dados), Schema (Esquema) e Table (Tabela) em que os dados serão carregados.
11. (Opcional) É possível selecionar os nomes das colunas para inseri-las em Column mapping (Mapeamento de colunas) para mapear colunas na ordem do arquivo de dados de entrada.
12. Selecione Load data (Carregar dados) para iniciar o carregamento de dados.

    Quando o carregamento for concluído, uma mensagem será exibida informando se o carregamento foi bem-sucedido ou não. Se for concluído corretamente, agora você poderá usar o SQL para selecionar dados da tabela carregada. Quando houver um erro, consulte a visualização do sistema STL_LOAD_ERRORS para obter mais detalhes. Para obter informações sobre erros do comando COPY, consulte STL_LOAD_ERRORS no Guia do desenvolvedor de banco de dados do Amazon Redshift.

    O modelo de comando COPY usado para carregar dados aparece no seu Query history (Histórico de consultas). Esse modelo de comando COPY mostra alguns dos parâmetros usados, mas não pode ser executado diretamente em uma guia do editor. Para obter mais informações sobre histórico de consultas, consulte Visualizar o histórico de consultas e guias.

Quando você carrega dados em uma nova tabela, o editor de consultas v2 cria a tabela no banco de dados, depois carrega os dados como ações separadas no mesmo fluxo de trabalho.

### Como carregar dados de um arquivo local em uma tabela nova

Seu administrador do editor de consultas v2 deve especificar o bucket comum do Amazon S3 na janela Account settings (Configurações da conta). O arquivo local é automaticamente carregado para um bucket comum do Amazon S3 utilizado por sua conta e, depois, o comando COPY é utilizado pelo editor de consultas v2 para carregar dados. O comando COPY gerado e executado pela janela Load local file (Carregar arquivo local) do editor de consultas v2 é compatível com muitos parâmetros disponíveis para a sintaxe do comando COPY para copiar do Amazon S3. Para obter informações sobre o comando COPY e suas opções usadas para carregar dados do Amazon S3, consulte COPY from Amazon S3 (COPY do Amazon S3) no Guia do desenvolvedor de banco de dados do Amazon Redshift.

1. Confirme se você está conectado ao banco de dados de destino no painel de visualização em árvore do editor de consultas v2. É possível criar uma conexão usando o menu de contexto (clique com o botão direito do mouse) para o cluster ou o grupo de trabalho no qual os dados serão carregados.
2. Selecione Load data (Carregar dados).
3. Em Data source (Fonte de dados), selecione Load from local file (Carregar do arquivo local).
4. Selecione Procurar para procurar o arquivo que contém os dados e Carregar arquivo. Por padrão, são exibidos arquivos com extensão `.csv`, `.avro`, `.parquet` e `.orc`, mas você pode escolher outros tipos de arquivo. O tamanho máximo do arquivo é de 5 MB.
5. Selecione o File format (Formato do arquivo) para o arquivo a ser carregado. Os formatos de dados compatíveis são CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET e ORC. Dependendo do formato de arquivo especificado, é possível escolher a respectivas File options (Opções de arquivos). Você também pode selecionar Data is encrypted (Os dados são criptografados), se os dados estiverem criptografados, e inserir o nome do recurso da Amazon (ARN) da chave KMS usada para criptografar os dados.

   Se você escolher CSV ou DELIMITADOR, também poderá escolher o Caractere delimitador e decidir se deseja Ignorar linhas de cabeçalho se o número especificado de linhas for nomes de colunas em vez de dados a serem carregados.
6. (Opcional) Advanced settings (Configurações avançadas) oferece suporte a vários parâmetros da conversão de dados e operações de carregamento. Insira essas informações conforme necessário para o arquivo.

Para obter mais informações sobre conversão de dados e parâmetros de carregamento de dados, consulte Parâmetros de conversão de dados e Operações de carregamento de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift.

7. Escolha Next (Próximo).
8. Escolha Carregar nova tabela.
9. Confirme ou selecione a localização da Tabela de destino, incluindo o Cluster ou grupo de trabalho, o Banco de dados e o Esquema em que os dados são carregados. Insira um nome para a Tabela que será criada.
10. Escolha Criar tabela para criar a tabela usando a definição mostrada.

    Um resumo é exibido para revisão da definição da tabela. A tabela é criada no banco de dados. Para excluir a tabela posteriormente, execute um comando SQL DROP TABLE. Para obter mais informações, consulte DROP TABLE no Guia do desenvolvedor de banco de dados do Amazon Redshift.
11. Selecione Load data (Carregar dados) para iniciar o carregamento de dados.

    Quando o carregamento for concluído, uma mensagem será exibida informando se o carregamento foi bem-sucedido ou não. Se for concluído corretamente, agora você poderá usar o SQL para selecionar dados da tabela carregada. Quando houver um erro, consulte a visualização do sistema STL_LOAD_ERRORS para obter mais detalhes. Para obter informações sobre erros do comando COPY, consulte STL_LOAD_ERRORS no Guia do desenvolvedor de banco de dados do Amazon Redshift.

    O modelo de comando COPY usado para carregar dados aparece no seu Query history (Histórico de consultas). Esse modelo de comando COPY mostra alguns dos parâmetros usados, mas não pode ser executado diretamente em uma guia do editor. Para obter mais informações sobre histórico de consultas, consulte Visualizar o histórico de consultas e guias.

## Autorizar e executar consultas

Você pode inserir uma consulta no editor ou selecionar uma consulta salva na lista Queries (Consultas) e escolha Run (Executar).

Por padrão, é definido Limit 100 para limitar os resultados a 100 linhas. É possível desativar essa opção para retornar um conjunto de resultados maior. Se você desativar essa opção, poderá incluir a opção LIMIT na instrução SQL para evitar conjuntos de resultados muito grandes. Para obter

mais informações, consulte cláusula ORDER BY no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Para exibir um plano de consulta na área de resultados, ative Explain (Explicar). Ative Explain graph (Explicar grafo) para que os resultados também exibam uma representação gráfica do plano de explicação.

Para salvar uma consulta na pasta Queries (Consultas), escolha Save (Salvar).

Se a consulta for bem-sucedida, será exibida uma mensagem de sucesso. Se a consulta retornar informações, os resultados serão exibidos na seção Results (Resultados). Se o número de resultados exceder a área de exibição, os números serão visualizados na parte superior da área de resultados. É possível escolher os números para exibir sucessivas páginas de resultados.

Você pode filtrar e classificar Result (Resultado) para cada coluna. Para inserir critérios de filtro no cabeçalho da coluna de resultados, passe o mouse sobre a coluna para ver um menu ( ) onde é possível inserir critérios para filtrar a coluna.

Se a consulta contiver um erro, o editor de consultas v2 exibirá uma mensagem de erro na área de resultados. A mensagem fornece informações sobre como corrigir a consulta.

Você pode exportar ou copiar os resultados da consulta usando o menu de contexto (clique com o botão direito do mouse) na área de resultados da seguinte forma:

- Selecione Export result set (Exportar conjunto de resultados) e opte por JSON ou CSV para baixar todo o conjunto de resultados da linha em um arquivo. O número de linhas no conjunto de resultados pode ser limitado pela opção Limit (Limitar) ou pela cláusula `limit` do SQL na consulta. O tamanho máximo do conjunto de resultados baixado é de 5 MB.
- Se nenhuma linha estiver selecionada, escolha Export current page (Exportar página atual) e opte por JSON ou CSV para baixar as linhas da página atual em um arquivo.
- Se as linhas estiverem selecionadas, escolha Export selected rows (Exportar linhas selecionadas) e opte por JSON ou CSV para baixar as linhas selecionadas em um arquivo.
- Se as linhas estiverem selecionadas, escolha Copy rows (Copiar linhas) a fim de copiar as linhas selecionadas para a área de transferência.
- Se as linhas estiverem selecionadas, escolha Copy rows with headers (Copiar linhas com cabeçalho) a fim de copiar as linhas selecionadas com os cabeçalhos de coluna para a área de transferência.

Você também pode usar o atalho Ctrl+C no Windows ou Cmd+C no macOS para copiar os dados da página de resultados atual para a área de transferência. Se nenhuma linha for selecionada, a célula com foco será copiada para a área de transferência. Se as linhas estiverem selecionadas, elas serão copiadas para a área de transferência.

Para adicionar uma nova guia de consulta, escolha o ícone

e Editor, que aparece na linha com as guias de consulta. A guia de consulta pode ou não estar usando uma `Isolated session`. Com uma sessão isolada, os resultados de um comando SQL que altera o banco de dados, como a criação de uma tabela temporária em uma guia do editor, não são visíveis em outra guia. Quando você abre uma guia no editor de consultas v2, o padrão é uma sessão isolada.

Para executar uma consulta

1. Na área de consulta, siga um destes procedimentos:

   - Insira uma consulta.
   - Cole uma consulta que você copiou.
   - Selecione a pasta Queries (Consultas) abra o menu de contexto (clique com o botão direito do mouse) em uma consulta salva e escolha Open query (Abrir consulta).

2. Confirme se escolheu o valor correto de Cluster ou Workgroup (Grupo de trabalho) e de Database (Banco de dados) para o SQL que você pretende executar.

   Inicialmente, é possível escolher seu Cluster ou WorkGroup (Grupo de trabalho) na exibição de árvore. Selecione Database (Banco de dados) na exibição de árvore também.

   Você pode alterar Cluster ou Workgroup (Grupo de trabalho) e Database (Banco de dados) dentro de cada guia do editor com o controle suspenso localizado próximo ao cabeçalho Isolated session (Sessão isolada) de cada guia do editor.

   Em cada guia do editor, você escolhe se deseja executar SQL em uma sessão isolada. A sessão isolada tem sua própria conexão com um banco de dados. Use-a para executar SQL isolado de outras sessões do editor de consultas. Para obter mais informações sobre conexões, consulte Abrir o editor de consultas v2.

3. Escolha Executar.

   A área Result (Resultado) é aberta e exibe os resultados da consulta.

Para exibir o plano de explicação de uma consulta

1. Selecione a consulta.
2. Ative Explain (Explicar).

   Por padrão, Explain graph (Explicar gráfico) também está ativado.
3. Escolha Executar.

   A consulta é executada, e o plano de explicação é exibido na área Result (Resultado) da consulta.

O editor de consultas v2 oferece suporte aos seguintes recursos:

- É possível criar consultas com várias instruções SQL em uma guia de consulta. As consultas são executadas em série, e várias guias de resultados são abertas para cada consulta.
- É possível criar consultas com variáveis de sessão e tabelas temporárias.
- Você pode criar consultas com parâmetros substituíveis designados por `${parameter}`. Crie sua consulta SQL com vários parâmetros substituíveis e usar o mesmo parâmetro em vários lugares na instrução SQL.

  Quando a consulta é executada, uma janela para inserção do valor do parâmetro é apresentada. Toda vez que você executa a consulta, a janela é exibida para a inserção dos valores dos parâmetros.

  Para ver um exemplo, consulte Exemplo: vendas maiores que um parâmetro específico.
- As consultas são versionadas automaticamente. É possível escolher uma versão anterior de uma consulta a ser executada.
- Para continuar com seu fluxo de trabalho, não é necessário esperar que uma consulta seja concluída. Suas consultas continuam sendo executadas, mesmo se você fechar o editor de consultas.
- Ao criar consultas, é possível usar o recurso de preenchimento automático de nomes de esquema, tabela e coluna.

O editor SQL é compatível com os seguintes recursos:

- Os colchetes inicial e final usados no SQL têm cores correspondentes. Linhas verticais são mostradas no editor para ajudar a combinar os colchetes.

- É possível recolher e expandir seções do SQL.
- É possível pesquisar e substituir texto no SQL.
- É possível usar teclas de atalho para várias tarefas comuns de edição.
- Os erros de SQL são realçados no editor para localização conveniente das áreas problemáticas.

Para ver uma demonstração dos recursos de edição, assista ao seguinte vídeo: “New and Enhanced Editing Experience in Amazon Redshift query editor v2” (Experiência de edição nova e aprimorada no editor de consultas v2 do Amazon Redshift).

## Exemplos de consulta

A seguir, você encontra descrições dos vários tipos de consultas que é possível executar.

Os dados usados em várias dessas consultas são do esquema de exemplo `tickit`. Para obter mais informações sobre como carregar os dados de amostra de `tickit`, consulte Carregar dados de exemplo. Para obter informações sobre dados de amostra de `tickit`, consulte Banco de dados de exemplo no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Ao executar essas consultas de exemplo, confirme se escolheu o banco de dados correto no editor, como `sample_data_dev`.

Tópicos

- Exemplo: definir variáveis de sessão
- Exemplo: principal evento por total de vendas
- Exemplo: vendas maiores que um parâmetro específico
- Exemplo: criar uma tabela temporária
- Exemplo: selecionar de uma tabela temporária

### Exemplo: definir variáveis de sessão

O comando a seguir define o parâmetro de configuração do servidor `search_path` para público para a sessão. Para obter mais informações, consulte SET e search_path no Guia do desenvolvedor de banco de dados do Amazon Redshift.

```
set search_path to public;
```

Exemplo: principal evento por total de vendas

A consulta a seguir localiza o evento com mais vendas.

```
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname
order by 3;
```

Veja a seguir uma lista parcial dos resultados.

```
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
...
```

Exemplo: vendas maiores que um parâmetro específico

A consulta a seguir localiza vendas em que a quantidade vendida é maior que o parâmetro especificado por `${numberoforders}`. Quando o valor do parâmetro é 7, o resultado é de 60 linhas. Quando você executa a consulta, o editor de consultas v2 exibe uma janela Run query form (Executar um formulário de consulta) para reunir o valor dos parâmetros na instrução SQL.

```
select salesid, qtysold
from sales
where qtysold > ${numberoforders}
order by 2;
```

Veja a seguir uma lista parcial dos resultados.

```
salesid qtysold
20005 8
21279 8
130232 8
42737 8
```

```
74681 8
67103 8
105533 8
91620 8
121552 8
...
```

Exemplo: criar uma tabela temporária

A instrução a seguir cria a tabela temporária eventsalestemp selecionando informações das tabelas sales e event.

```
create temporary table eventsalestemp as
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname;
```

Exemplo: selecionar de uma tabela temporária

A declaração a seguir seleciona eventos, total de pedidos e total de vendas da tabela temporária eventsalestemp, ordenada pelo total de pedidos.

```
select eventname,  totalorders,  totalsales
from eventsalestemp
order by 2;
```

Veja a seguir uma lista parcial de resultados.

```
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
...
```

## Autorizar e executar blocos de anotações

É possível usar blocos de anotações para organizar, anotar e compartilhar várias consultas SQL em um único documento. É possível adicionar várias células de consulta SQL e Markdown a um

bloco de anotações. Os blocos de anotações fornecem um modo de agrupar consultas e explicações associadas a uma análise de dados em um único documento usando várias células de consulta e Markdown. É possível adicionar texto e formatar a aparência usando a sintaxe Markdown para fornecer contexto e informações adicionais para suas tarefas de análise de dados. Você pode compartilhar os blocos de anotações com os membros da equipe.

Para usar blocos de anotações, você deve adicionar permissão para blocos de anotações à entidade principal do IAM (um usuário do IAM ou um perfil do IAM). Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift. Você pode adicionar a permissão a uma das políticas gerenciadas do editor de consultas v2. Para obter mais informações, consulte Acessar o editor de consultas v2.

Você pode escolher a opção Run all (Executar tudo) para as células de um blocos de anotações. A célula de consulta SQL de um bloco de anotações tem a maioria dos mesmos recursos de uma guia do editor de consultas. Para obter mais informações, consulte Autorizar e executar consultas. A seguir estão as diferenças entre uma guia do editor de consultas e uma célula SQL de um bloco de anotações.

- Não há um controle para executar `Explain` em uma instrução SQL em um bloco de anotações.
- Você só pode criar um gráfico por célula SQL em um bloco de anotações.

Você pode exportar e importar blocos de anotações para arquivos criados com o editor de consultas v2. A extensão do arquivo é `.ipynb` e o tamanho do arquivo pode ser até 5 MB. As células SQL e Markdown são armazenadas no arquivo. Um cluster ou grupo de trabalho e um banco de dados não são armazenados no bloco de anotações exportado. Ao abrir um bloco de anotações importado, escolha o cluster ou grupo de trabalho e o banco de dados onde será executado. Depois de executar as células SQL, você pode escolher na guia de resultados se deseja exibir a página atual de resultados como um gráfico. O conjunto de resultados de uma consulta não é armazenado no bloco de anotações.

Quando você executa um notebook, com Executar tudo ou Executar, um painel de Status de execução permanece disponível. Escolha o ícone

para abrir o painel. Esse painel contém um resumo do status de Executar tudo ou Executar mais recente das células SQL no notebook. Se executar várias células SQL, você poderá exibir rapidamente o status, o tempo decorrido e alguns detalhes sobre a execução. É possível filtrar

as células exibidas com base no status: `All`, `Succeeded`, `Error`, `In progress` ou `Canceled`. Também é possível usar esse painel para navegar até uma célula SQL no editor.

Para criar um caderno

1. No menu do navegador, selecione

   Editor.
2. Selecione

   e escolha Notebook.

   Por padrão, uma célula de consulta SQL é exibida no bloco de anotações.
3. Na célula de consulta SQL, siga um destes procedimentos:

   - Insira uma consulta.
   - Cole uma consulta que você copiou.
4. (Opcional) Escolha o ícone

   , depois selecione Markdown para adicionar uma célula Markdown na qual você poderá fornecer texto descritivo ou explicativo usando a sintaxe Markdown padrão.
5. (Opcionalmente) Escolha o ícone

   , depois selecione SQL para inserir uma célula SQL.

Você pode renomear blocos de anotações usando o ícone

(lápis).

No menu



(mais), você também pode realizar as seguintes operações em um bloco de anotações:

-

  Share with my team (Compartilhar com minha equipe): para compartilhar o bloco de anotações com sua equipe, conforme definido pelas tags. Para obter mais informações, consulte Compartilhar uma consulta.

-

  Export (Exportar): para exportar o bloco de anotações para um arquivo local com a extensão `.ipynb`.

-

  Save version (Salvar versão): para criar uma versão do bloco de anotações. Para ver as versões de um bloco de anotações, navegue até seus blocos de anotações salvos e abra Version history (Histórico de versões).

-

  Duplicate (Duplicar): para criar uma cópia do bloco de anotações e abrir essa cópia em uma nova guia de bloco de anotações.

-

  Shortcuts (Atalhos): para exibir os atalhos disponíveis ao criar um bloco de anotações.

Como abrir um bloco de anotações salvo

1. No menu do navegador, escolha

   Notebooks (Blocos de anotações). Seus blocos de anotações e pastas de blocos de anotações salvos são exibidos.
2. Escolha o bloco de anotações SQL que deseja abrir e clique nele duas vezes.

Você pode mostrar My notebooks (Meus blocos de anotações), blocos de anotações Shared by me (Compartilhados por mim) e blocos de anotações Shared to my team (Compartilhados com minha equipe) na guia de blocos de anotações.

Para importar um bloco de anotações de um arquivo local para My notebooks (Meus blocos de anotações), escolha

Import (Importar) e navegue até o arquivo `.ipynb` que contém seu bloco de anotações. O bloco de anotações é importado para a pasta de blocos de anotações aberta no momento. Você pode abrir o bloco de anotações pelo editor de blocos de anotações.

No menu de contexto (clique com o botão direito) de um bloco de anotações, você pode executar as seguintes operações:

- Open notebook (Abrir bloco de anotações): para abrir o bloco de anotações no editor.
- Save version (Salvar versão): para salvar uma versão do bloco de anotações.
- Version history (Histórico de versões): para exibir as versões de um bloco de anotações. Na janela Version history (Histórico de versões), você pode excluir e reverter versões. Você também pode criar um bloco de anotações usando a versão selecionada no momento.
- Edit tags (Editar etiquetas): para criar e editar etiquetas em um bloco de anotações.
- Share with my team (Compartilhar com minha equipe): para compartilhar um bloco de anotações com com sua equipe.

  Para compartilhar um bloco de anotações com sua equipe, verifique se tem a etiqueta da entidade principal `sqlworkbench-team` definida com o mesmo valor que o restante dos membros de sua equipe em sua conta. Por exemplo, um administrador pode definir o valor como `accounting-team` para todos os membros do departamento de contabilidade. Para ver um exemplo, consulte Permissões necessárias para usar o editor de consultas v2 .
- Export (Exportar): para exportar um bloco de anotações para um arquivo local.
- Rename (Renomear): para renomear um caderno.
- Duplicate (Duplicar): para fazer uma cópia de um bloco de anotações.
- Delete (Excluir): para excluir um bloco de anotações.

Para conferir uma demonstração sobre blocos de anotações, assista ao vídeo a seguir: Amazon Redshift SQL Notebooks in query editor v2.

## Consulta ao AWS Glue Data Catalog

É possível usar o editor de consultas v2 para consultar dados catalogados no AWS Glue Data Catalog. Por padrão, o AWS Glue Data Catalog está listado como um banco de dados do editor de consultas v2 chamado `awsdatacatalog`. A consulta ao AWS Glue Data Catalog não está disponível em todas as Regiões da AWS do Amazon Redshift. Use o comando SHOW para

determinar se esse recurso está disponível. Para obter mais informações sobre o AWS Glue, consulte O que é o AWS Glue? no Guia do desenvolvedor do AWS Glue.

> **Note**
>
> A consulta ao AWS Glue Data Catalog só é permitida nos clusters do tipo de nó RA3 do Amazon Redshift e no Amazon Redshift sem servidor.

É possível configurar o data warehouse e visualizar os objetos do banco de dados do AWS Glue catalogados usando os seguintes comandos SQL:

- SHOW: para mostrar se `awsdatacatalog` está montado para o data warehouse conectado no momento. Por exemplo, para mostrar o valor do parâmetro `data_catalog_auto_mount`, execute:

  ```
  SHOW data_catalog_auto_mount;
  ```

  Para obter mais informações, consulte SHOW no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- ALTER SYSTEM: para alterar a configuração no nível de sistema de `data_catalog_auto_mount`. Por exemplo, para alterar o valor do parâmetro `data_catalog_auto_mount` para on, execute:

  ```
  ALTER SYSTEM SET data_catalog_auto_mount = on;
  ```

  A alteração entra em vigor quando um cluster provisionado é reinicializado ou um grupo de trabalho sem servidor é automaticamente pausado e retomado. Para obter mais informações, consulte ALTER SYSTEM no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- SHOW SCHEMAS: mostra uma lista de esquemas. Os esquemas no banco de dados chamado `awsdatacatalog` representam os bancos de dados do AWS Glue catalogados no AWS Glue Data Catalog. Por exemplo, para mostrar esses esquemas, execute:

  ```
  SHOW SCHEMAS FROM DATABASE awsdatacatalog;
  ```

  Para obter mais informações, consulte SHOW SCHEMAS no Guia do desenvolvedor de banco de dados do Amazon Redshift.

- SHOW TABLES: mostra uma lista de tabelas em um esquema. Por exemplo, para mostrar as tabelas no banco de dados do AWS Glue Data Catalog chamado `awsdatacatalog` que estão no esquema `myglue`, execute:

  ```
  SHOW TABLES FROM SCHEMA awsdatacatalog.myschema;
  ```

  Para obter mais informações, consulte SHOW TABLES no Guia do desenvolvedor de banco de dados do Amazon Redshift.

- SHOW COLUMNS: mostra uma lista de colunas em uma tabela. Por exemplo, para mostrar as colunas no banco de dados do AWS Glue Data Catalog chamado `awsdatacatalog` que estão no esquema `myglue` e na tabela `mytable`, execute:

  ```
  SHOW COLUMNS FROM TABLE awsdatacatalog.myglue.mytable;
  ```

  Para obter mais informações, consulte SHOW COLUMNS no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Para conceder ao seu usuário ou perfil do IAM permissão para consultar o AWS Glue Data Catalog, siga estas etapas

1. No painel de visualização em árvore, conecte-se ao banco de dados inicial no cluster provisionado ou grupo de trabalho sem servidor usando o método de autenticação Nome de usuário e senha do banco de dados. Por exemplo, conecte-se ao banco de dados `dev` usando o usuário administrador e a senha que você usou ao criar o cluster ou o grupo de trabalho.
2. Em um guia do editor, execute a seguinte instrução de SQL para conceder ao usuário do IAM acesso ao AWS Glue Data Catalog.

   ```
   GRANT USAGE ON DATABASE awsdatacatalog to "IAM:myIAMUser"
   ```

   Em que *`IAM:myIAMUser`* é um usuário do IAM ao qual você deseja conceder privilégio de uso ao AWS Glue Data Catalog. Como alternativa, você pode conceder privilégio de uso a *`IAMR:myIAMRole`* para um perfil do IAM.
3. No painel de exibição em árvore, edite ou exclua a conexão com o cluster ou o grupo de trabalho que você criou anteriormente. Conecte-se ao cluster ou ao grupo de trabalho de uma das seguintes maneiras:

- Para acessar o banco de dados `awsdatacatalog` por meio de um cluster, você deve usar o método de autenticação Credenciais temporárias usando sua identidade do IAM. Para obter mais informações sobre esse método de autenticação, consulte Conectar-se a um banco de dados do Amazon Redshift. Talvez o administrador do editor de consultas v2 precise definir as Configurações de conta para que a conta exiba esse método de autenticação na janela de conexão.
- Para acessar o banco de dados `awsdatacatalog` por meio de um grupo de trabalho, você deve usar o método de autenticação Usuário federado. Para obter mais informações sobre esse método de autenticação, consulte Conectar-se a um banco de dados do Amazon Redshift.

4. Com o privilégio concedido, você pode usar sua identidade do IAM para executar o SQL em seu AWS Glue Data Catalog.

Depois de se conectar, você pode usar o editor de consultas v2 para consultar dados catalogados em AWS Glue Data Catalog. No painel de exibição em árvore do editor de consultas v2, selecione o cluster ou o grupo de trabalho e o banco de dados `awsdatacatalog`. No painel do editor ou do notebook, confirme se o cluster ou o grupo de trabalho correto foi escolhido. O banco de dados escolhido deve ser o banco de dados inicial do Amazon Redshift, como `dev`. Para obter informações sobre a criação de consultas, consulte Autorizar e executar consultas e Autorizar e executar blocos de anotações. O banco de dados denominado `awsdatacatalog` é reservado para fazer referência ao banco de dados externo do catálogo de dados em sua conta. As consultas no banco de dados `awsdatacatalog` só podem ser somente leitura. Use a notação de três partes para fazer referência à tabela em sua instrução SELECT. Em que a primeira parte é o nome do banco de dados, a segunda parte é o nome do banco de dados AWS Glue e a terceira parte é o nome da tabela AWS Glue.

```
SELECT * FROM awsdatacatalog.<aws-glue-db-name>.<aws-glue-table-name>;
```

Você pode realizar vários cenários que leem os dados de AWS Glue Data Catalog e preenchem as tabelas do Amazon Redshift.

O exemplo de SQL a seguir une duas tabelas definidas em 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;
```

O exemplo de SQL a seguir cria uma tabela do Amazon Redshift e a preenche com dados de uma união de duas tabelas 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;
```

## Consultar um data lake

Você pode consultar dados em um data lake do Amazon S3. Primeiro, você cria um esquema externo para referenciar o banco de dados externo no AWS Glue Data Catalog. Depois, você pode consultar dados em um data lake do Amazon S3.

### Demonstração: consultar um data lake

Para ver uma demonstração de como consultar um data lake, assista ao vídeo a seguir. Consulte o data lake no editor de consultas v2 do Amazon Redshift.

### Pré-requisitos

Antes de trabalhar com seu data lake no editor de consultas v2, confirme se os itens a seguir foram configurados em seu ambiente do Amazon Redshift:

- Rastreie seus dados do Amazon S3 usando o AWS Glue e habilite o Catálogo de Dados para o AWS Lake Formation.
- Crie um perfil do IAM para o Amazon Redshift usando o Catálogo de Dados do AWS Glue habilitado para o AWS Lake Formation. Para obter detalhes sobre esse procedimento, consulte Como criar um perfil do IAM para o Amazon Redshift usando um AWS Glue Data Catalog habilitado para o AWS Lake Formation. Para obter mais informações sobre como usar o Redshift Spectrum e o Lake Formation, consulte Usar o Redshift Spectrum com o AWS Lake Formation.
- Conceda permissões SELECT na tabela a ser consultada no banco de dados do Lake Formation. Para obter detalhes sobre esse procedimento, consulte Como conceder permissões SELECT na tabela a ser consultada no banco de dados do Lake Formation.

  Você pode verificar no console do Lake Formation (https://console.aws.amazon.com/lakeformation/), na seção Permissões, página Permissões do data lake, se o perfil do IAM, o banco de dados do AWS Glue e as tabelas têm as permissões adequadas.

- Confirme se seu usuário conectado tem permissão para criar esquemas no banco de dados do Amazon Redshift e acessar dados em seu data lake. Ao se conectar a um banco de dados no editor de consultas v2, você escolhe um método de autenticação que inclui credenciais, que podem ser um usuário do banco de dados ou um usuário do IAM. O usuário conectado deve ter as permissões e os privilégios de banco de dados adequados, como um `superuser`. O usuário `admin` do Amazon Redshift que criou o cluster ou grupo de trabalho tem privilégios de `superuser` e pode criar esquemas e gerenciar o banco de dados do Redshift. Para obter mais informações sobre como se conectar a um banco de dados com o editor de consultas v2, consulte Conectar-se a um banco de dados do Amazon Redshift.

## Criar um esquema externo

Para consultar dados em um data lake do Amazon S3, comece criando um esquema externo. Um esquema externo referencia o banco de dados no AWS Glue Data Catalog.

1. Na visualização Editor do editor de consultas v2, escolha Criar e Esquema.
2. Digite um Schema name (Nome do esquema).
3. Em Tipo de esquema, escolha Externo.
4. Nos detalhes do Catálogo de Dados, a opção Região assume por padrão a Região da AWS em que o banco de dados do Redshift está localizado.
5. Escolha o Banco de dados do AWS Glue para o qual o esquema externo será mapeado e que contém referências às tabelas do AWS Glue.
6. Escolha um Perfil do IAM para o Amazon Redshift que tenha as permissões necessárias para consultar dados no Amazon S3.
7. Opcionalmente, escolha um Perfil do IAM que tenha permissão para acessar o Catálogo de Dados.
8. Selecione Create schema (Criar esquema).

   O esquema aparece sob o banco de dados no painel de exibição em árvore.

Ao criar o esquema, se você receber um erro de permissão negada para o banco de dados, verifique se o usuário conectado tem o privilégio de banco de dados para criar um esquema.

### Consultar dados no data lake do Amazon S3

Você usa o esquema criado no procedimento anterior.

1. No painel de exibição em árvore, escolha o esquema.
2. Para visualizar uma definição de tabela, escolha uma tabela. As colunas da tabela e os tipos de dados são exibidos.
3. Para consultar uma tabela, escolha a tabela e, no menu de contexto (clique com o botão direito do mouse), selecione Selecionar tabela para gerar uma consulta.
4. Execute a consulta no Editor.

   O exemplo de SQL a seguir foi gerado pelo editor de consultas v2 para consultar todas as linhas na tabela do AWS Glue chamada `flightscsv`. As colunas e linhas mostradas na saída são truncadas para simplicidade.

```
SELECT * FROM "dev"."mydatalake_schema"."flightscsv";

year    quarter   month   dom  day_of_week   fl_date    unique_carrier  airline_id
  carrier   tail_num   fl_num
2016    4         10      19   3             10/19/16   OO              20304
  OO         N753SK    3086
2016    4         10      19   3             10/19/16   OO              20304
  OO         N753SK    3086
2016    4         10      19   3             10/19/16   OO              20304
  OO         N778SK    3087
2016 4         10      19   3            10/19/16   OO              20304
 OO         N778SK    3087
...
```

## Trabalho com unidades de compartilhamento de dados

Você pode criar um banco de dados para que os usuários em outro cluster possam consultar os dados. O cluster que contém os dados que você deseja compartilhar é chamado de cluster produtor. Você cria uma unidade de compartilhamento de dados no cluster produtor para os objetos de banco de dados que deseja compartilhar. Você pode compartilhar esquemas, tabelas, exibições e funções do SQL definidas pelo usuário (UDFs). O cluster com o qual você deseja compartilhar os dados é chamado de cluster consumidor. No cluster consumidor, você cria um banco de dados a partir da unidade de compartilhamento de dados. Em seguida, os usuários no cluster consumidor

podem consultar os dados. Para obter mais informações, consulte Conceitos básicos sobre compartilhamento de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift.

## Criar datashares

Você cria uma unidade de compartilhamento de dados no cluster que você deseja usar como cluster produtor. Para saber mais sobre considerações de unidades de compartilhamento de dados, consulte Considerações sobre o compartilhamento de dados no Amazon Redshift no Guia do desenvolvedor de banco de dados da Amazon.

1. Escolha o banco de dados no cluster produtor que você deseja usar.
2. Crie a unidade de compartilhamento de dados. Por exemplo:

```
create datashare mysource;
```

3. Defina permissões na unidade de compartilhamento de dados. Por exemplo:

```
grant alter, share on datashare mysource to admin;
```

4. Defina permissões nos objetos do banco de dados que você deseja compartilhar. Por exemplo:

```
alter datashare mysource add schema public;
```

```
alter datashare mysource add table public.event;
```

5. Defina permissões no namespace do cluster consumidor para acessar a unidade de compartilhamento de dados. Por exemplo:

```
grant usage on datashare mysource to namespace '2b12345-1234-5678-9012-
bb1234567890';
```

## Exibição de unidades de compartilhamento de dados

Você pode exibir as unidades de compartilhamento de dados criados no cluster produtor.

1. Escolha o cluster produtor.
2. Exiba as unidades de compartilhamento de dados. Por exemplo:

```
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
```

## Criação do banco de dados do consumidor

No cluster consumidor, você cria um banco de dados a partir da unidade de compartilhamento de dados. Essas etapas descrevem como compartilhar dados entre dois clusters na mesma conta. Para obter informações sobre o compartilhamento de dados entre contas da AWS, consulte Compartilhamento de dados entre contas da AWS no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Você pode usar comandos de SQL ou o painel de exibição em árvore do editor de consultas v2 para criar o banco de dados.

Para usar o SQL

1. Crie um banco de dados a partir da unidade de compartilhamento de dados da sua conta e do namespace do cluster produtor. Por exemplo:

   ```
   create database share_db from datashare mysource of account '123456789012'
    namespace 'p1234567-8765-4321-p10987654321';
   ```

2. Defina permissões para que os usuários possam acessar o banco de dados e o esquema. Por exemplo:

   ```
   grant usage on database share_db to usernames;
   ```

   ```
   grant usage on schema public to usernames;
   ```

Para usar o painel de exibição em árvore do editor de consultas v2

1. Selecione Create (Criar) e escolha Database (Banco de dados).
2. Insira um Database name (Nome do banco de dados).
3. (Opcional) Selecione Users and groups (Usuários e grupos) e escolha um Database user (Usuário do banco de dados).
4. Escolha Create using a datashare (Criar usando uma unidade de compartilhamento de dados).
5. Escolha a unidade de compartilhamento de dados.
6. Selecione Criar banco de dados.

   O novo banco de dados do datash (unidade de compartilhamento de dados) será exibido no painel de exibição em árvore do editor de consultas v2.
7. Defina permissões para que os usuários possam acessar o banco de dados e o esquema. Por exemplo:

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

## Consulta de objetos da unidade de compartilhamento de dados

No cluster do consumidor, é possível consultar objetos da unidade de compartilhamento de dados usando nomes de objeto totalmente qualificados expressos com a notação de três partes: banco de dados, esquema e nome do objeto.

1. No painel de exibição em árvore do editor de consultas v2, escolha o esquema.
2. Para visualizar uma definição de tabela, escolha uma tabela.

   As colunas da tabela e os tipos de dados são exibidos.
3. Para consultar uma tabela, escolha a tabela e use o menu de contexto (clique com o botão direito do mouse) para escolher Select table (Selecionar tabela).

4. Consulte tabelas usando comandos SELECT. Por exemplo:

```
select top 10 * from test_db.public.event;
```

## Programar uma consulta com o editor de consultas v2

É possível criar uma programação para executar uma instrução SQL com o Editor de Consultas v2 do Amazon Redshift. Crie uma programação para executar sua instrução SQL nos intervalos de tempo que correspondam às suas necessidades de negócios. Na hora da execução da consulta programada, a consulta é iniciada pelo Amazon EventBridge e usa a API de dados do Amazon Redshift.

Como criar uma programação a fim de executar uma instrução SQL

1. Na visualização selecione Programar criar uma programação para executar uma instrução SQL.
2. Quando você define a programação, fornece as informações a seguir.
   - Um perfil do IAM que assume as permissões necessárias para executar a consulta. Esse perfil do IAM também está associado ao cluster ou grupo de trabalho.
   - Os valores de autenticação para AWS Secrets Manager ou credenciais temporárias para autorizar o acesso ao cluster ou grupo de trabalho. Esses métodos de autenticação são compatíveis com a API de dados. Para ter mais informações, consulte Autenticar uma consulta programada.
   - O cluster ou grupo de trabalho em que o banco de dados reside.
   - O nome do banco de dados que contém os dados a serem consultados.
   - O nome da consulta programada e sua descrição. O editor de consultas v2 usa “QS2-” como prefixo do nome da consulta programada que você fornece. O editor de consultas v1 prefixa os nomes das consultas programadas com “QS-”.
   - A instrução SQL a ser executada de acordo com a programação.

- A frequência de programação e opções de repetição ou um valor formatado cron que define a programação. Para obter mais informações, consulte Expressões Cron, no Guia do usuário do Amazon CloudWatch Events.
- Opcionalmente, você pode ativar as notificações comuns do Amazon SNS para monitorar a consulta programada. Talvez seja necessário confirmar o endereço de e-mail fornecido para a notificação do Amazon SNS. Verifique se recebeu um e-mail com um link para confirmar o endereço de e-mail da notificação do Amazon SNS. Para obter mais informações, consulte Notificações de e-mail no Guia do desenvolvedor do Amazon Simple Notification Service. Se a consulta estiver sendo executada, mas você não vir mensagens publicadas no tópico do SNS, consulte Minha regra é executada, mas eu não vejo nenhuma mensagem publicada no meu tópico do Amazon SNS no Guia do usuário do Amazon EventBridge.

3. Escolha Programar consulta para salvar e ativar a programação e adicionar a programação à lista de consultas na visualização Consultas programadas.

As visualização de de Consultas programadas lista todas as consultas programadas para os clusters e grupos de trabalho. Com essa visualização, é possível exibir detalhes da consulta de programação, ativar ou desativar a programação, editar a programação e excluir a consulta programada. Ao visualizar os detalhes da consulta, você também pode ver o histórico de execução da consulta com a programação.

> **Note**
>
> A execução de uma consulta programada só está disponível na lista Histórico de programação por 24 horas. As consultas executadas de acordo com uma programação não aparecem na visualização Histórico de consultas do editor de consultas v2.

## Configurar permissões para programar uma consulta

Para programar consultas, o usuário do AWS Identity and Access Management (IAM) que define a programação e o perfil do IAM associado à programação devem ser configurados com as permissões do IAM para usar o Amazon EventBridge e a API de dados do Amazon Redshift. Para receber e-mails de consultas programadas, a notificação do Amazon SNS que você especificar opcionalmente também deverá ser configurada.

A seguir, descrevemos as tarefas para usar políticas gerenciadas da AWS para fornecer permissão, mas, dependendo do ambiente, talvez você queira reduzir as permissões concedidas.

Para o usuário do IAM conectado ao editor de consultas v2, edite o usuário do IAM que usa o console do IAM (https://console.aws.amazon.com/iam/).

- Além das permissões para executar as operações do Amazon Redshift e do editor de consultas v2, anexe as políticas gerenciadas `AmazonEventBridgeFullAccess` e `AmazonRedshiftDataFullAccess` da AWS a um usuário do IAM.
- Uma alternativa é atribuir as permissões a um perfil e designá-lo ao usuário.

  Anexe uma política com a permissão `sts:AssumeRole` ao ARN do recurso do perfil do IAM que você especificou ao definir a consulta agendada. Para obter mais informações sobre como assumir perfis, consulte Concessão de permissões a um usuário para alternar funções no Guia do usuário do IAM.

  O exemplo a seguir mostra uma política de permissão que assume o perfil do IAM `myRedshiftRole` na conta `123456789012`. O perfil do IAM `myRedshiftRole` também é o perfil anexado ao cluster ou grupo de trabalho em que a consulta programada é executada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AssumeIAMRole",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::123456789012:role/myRedshiftRole"
            ]
        }
    ]
}
```

  Atualize a política de confiança do perfil do IAM usado para programar a consulta a fim de permitir que o usuário do IAM a assuma.

```
{
            "Sid": "AssumeRole",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/myIAMusername"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Para o perfil do IAM que você especifica para permitir a execução da consulta programada, edite o perfil do IAM usando o console do IAM (https://console.aws.amazon.com/iam/).

- Anexe as políticas gerenciadas `AmazonRedshiftDataFullAccess` e `AmazonEventBridgeFullAccess` da AWS ao perfil do IAM. A política gerenciada `AmazonRedshiftDataFullAccess` só concede a permissão `redshift-serverless:GetCredentials` para grupos de trabalho do Redshift sem servidor marcados com a chave `RedshiftDataFullAccess`.

## Autenticar uma consulta programada

Ao programar uma consulta, você usa um dos métodos de autenticação a seguir quando o SQL é executado. Cada método requer uma combinação diferente de entrada no editor de consultas v2. Esses métodos de autenticação são compatíveis com a API de dados, que é usada para executar as instruções SQL.

O usuário ou perfil do banco de dados usado para executar a consulta deve ter os privilégios de banco de dados necessários. Por exemplo, para conceder privilégios `IAMR:MyRedshiftQEv2Scheduler` à tabela `mytable`, execute o comando SQL a seguir.

```
GRANT all ON TABLE mytable TO "IAMR:MyRedshiftQEv2Scheduler";
```

Para ver a lista de usuários do banco de dados no cluster ou grupo de trabalho, consulte a visualização do sistema `PG_USER_INFO`.

> **Note**
>
> Todos os grupos de trabalho do Redshift sem servidor para o qual você programa consultas devem ser marcados com a chave `RedshiftDataFullAccess`. Para ter mais informações, consulte Autorizar acesso à API de dados do Amazon Redshift.
> Como alternativa à marcação do grupo de trabalho, você pode adicionar uma política em linha ao perfil do IAM (especificado com a programação) que permite `redshift-serverless:GetCredentials`. Por exemplo:
>
> ```
> {
>     "Version": "2012-10-17",
>     "Statement": [
>         {
>             "Sid": "UseTemporaryCredentialsForAllServerlessWorkgroups",
>             "Effect": "Allow",
>             "Action": "redshift-serverless:GetCredentials",
>             "Resource": [
>                 "arn:aws:redshift-serverless:*:*:workgroup/*"
>             ]
>         }
>     ]
> }
> ```

AWS Secrets Manager

Com este método, forneça um valor secreto para secret-arn que é armazenado no AWS Secrets Manager. Este segredo contém credenciais para se conectar ao seu banco de dados. Talvez você tenha criado um segredo com as credenciais adequadas quando criou o cluster ou o grupo de trabalho. O segredo deve ser marcado com a chave `RedshiftDataFullAccess`. Se a chave da tag ainda não estiver presente, use o console AWS Secrets Manager para adicioná-la. Para obter informações sobre como criar um segredo, consulte Criar um segredo para credenciais de conexão de banco de dados.

Para obter mais informações sobre as permissões mínimas, consulte Criação e gerenciamento de segredos com o AWS Secrets Manager no Manual do usuário do AWS Secrets Manager.

Credenciais temporárias

Com esse método, forneça o Nome do banco de dados e os valores do Usuário do banco de dados ao se conectar a um banco de dados em um cluster. Você só precisa fornecer o Nome do banco de dados ao se conectar a um banco de dados em um grupo de trabalho.

Ao se conectar a um cluster, a política `AmazonRedshiftDataFullAccess` concede ao usuário do banco de dados chamado `redshift_data_api_user` permissão para `redshift:GetClusterCredentials`. Se você quiser usar um usuário de banco de dados diferente para executar a instrução SQL, adicione uma política ao perfil do IAM anexado ao cluster para permitir `redshift:GetClusterCredentials`. O exemplo a seguir permite usuários do banco de dados `awsuser` e `myuser`.

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

## Configurar permissões para consultar o histórico de consultas programadas

Para permitir que os usuários visualizem o histórico de consultas programadas, edite o perfil do IAM Relações de confiança (especificado com a programação) para adicionar permissões.

Veja a seguir um exemplo de política de confiança em um perfil do IAM que permite ao usuário do IAM *myIAMusername* ver o histórico de consultas programadas. Em vez de conceder a um usuário do IAM a permissão `sts:AssumeRole`, é possível optar por atribuir essa permissão a um perfil do IAM.

```
{
```

```
    "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"
        }
    ]
}
```

## Monitoramento da consulta programada

Para o tópico do Amazon SNS que você especifica para enviar notificações por e-mail, crie o tópico do Amazon SNS usando o editor de consultas v2. Para isso, você deve acessar a seção Notificações do SNS, Ativar o monitoramento e criar o tópico com Criar tópico do SNS. O editor de consultas v2 cria o tópico do Amazon SNS e adiciona uma entidade principal de serviço à política de acesso do Amazon EventBridge. Veja a seguir uma Política de acesso de exemplo que é criada no tópico do Amazon SNS. No exemplo, são usados a Região da AWS *us-west-2*, a Conta da AWS *123456789012* e o tópico do Amazon SNS *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"
    }
  ]
}
```

Quando a consulta programada é executada, o Amazon SNS envia e-mails de notificação da AWS. O exemplo a seguir mostra um e-mail enviado para *myemail@example.com* referente à consulta programada *QS2-may25a* executada na Região da AWS *eu-north-1* na Conta da AWS *123.456.789.012* usando o tópico de notificação do 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
```

## Solução de problemas da configuração de programação de uma consulta

Considere o seguinte se você tiver problemas ao programar uma consulta:

As consultas não são executadas

Verifique se o perfil do IAM usado na programação tem permissão para obter as credenciais temporárias do cluster. A permissão para clusters provisionados

é `redshift:GetClusterCredentialsWithIAM`. A permissão para grupos de trabalho do Redshift sem servidor é `redshift-serverless:GetCredentials`.

O histórico de programação não é exibido

O usuário do IAM ou o perfil do IAM usado para fazer login no console da AWS não foi adicionado à política de confiança do perfil do IAM usado para programar a consulta.

Ao usar o AWS Secrets Manager para a consulta agendada para se conectar, confirme se o segredo está marcado com a chave `RedshiftDataFullAccess`.

Se a consulta agendada estiver usando uma conexão do AWS Secrets Manager, o perfil do IAM usado para agendar a consulta deverá ter o valor equivalente à política gerenciada `SecretsManagerReadWrite` anexada ao perfil.

O status do histórico de consultas é **`Failed`**

Exiba a visualização do sistema SYS_QUERY_HISTORY para obter detalhes sobre por que a consulta falhou. Um problema comum é que o usuário ou o perfil do banco de dados que foi usado para executar a consulta pode não ter o privilégio necessário para executar o SQL. Para ter mais informações, consulte Autenticar uma consulta programada.

O SQL a seguir consulta a visualização SYS_QUERY_HISTORY para retornar consultas com falha.

```
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';
```

Para descobrir detalhes de uma consulta programada com falha específica, consulte Encontrar detalhes sobre consultas programadas com o AWS CloudShell.

## Encontrar detalhes sobre consultas programadas com o AWS CloudShell

É possível usar o AWS CloudShell para descobrir detalhes sobre uma consulta programada. Você deve ter as permissões adequadas para executar os comandos da AWS CLI mostrados no procedimento a seguir.

Para visualizar os resultados de uma consulta programada

1. No console do AWS, abra o prompt de comando do AWS CloudShell. Para obter mais informações sobre o AWS CloudShell, consulte O que é o AWS CloudShell no Guia do usuário do AWS CloudShell.
2. Assuma o perfil do IAM da consulta programada. Para assumir o perfil, encontre o perfil do IAM associado à consulta programada no editor de consultas v2 e use-o no comando da AWS CLI no AWS CloudShell. Por exemplo, para o perfil `scheduler`, insira um comando AWS STS para assumir o perfil usado pela consulta programada.

   ```
   aws sts assume-role –role-arn "arn:aws:iam::123456789012:role/scheduler" –role-
   session-name "scheduler-test"
   ```

   As credenciais retornadas são semelhantes às seguintes:

   ```
   "Credentials": {
   "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
   "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
   "SessionToken": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...",
   "Expiration": "2023-08-18T18:19:44+00:00"
   },
   "AssumedRoleUser": {
   "AssumedRoleId": "AROA35B2NH6WBTP7ONL4E:scheduler-test",
   "Arn": "arn:aws:sts::123456789012:assumed-role/scheduler/scheduler-test"
   }
   }
   ```
3. Crie variáveis de ambiente na AWS CLI usando as credenciais exibidas ao assumir o perfil do IAM. É necessário usar esses tokens antes do respectivo prazo de validade. Por exemplo, insira o seguinte no AWS CloudShell.

   ```
   export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
   export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
   export AWS_SESSION_TOKEN=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...
   ```
4. Para ver o erro de uma consulta com falha, execute o comando da AWS CLI para descrever uma instrução. O ID da instrução SQL é do ID mostrado na seção Histórico de programação de uma consulta programada no editor de consultas v2.

```
aws redshift-data describe-statement –id 130d2620-05d2-439c-b7cf-815d9767f513
```

Neste exemplo, o SQL programado `select * from users limit 100` resulta em um erro de SQL segundo o qual a tabela `users` não existe.


```
{
"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"
}
```


### Demonstração do agendamento de uma consulta

Para ver uma demonstração de como agendar uma consulta, assista ao vídeo a seguir.Demonstração em vídeo de como agendar uma consulta.

## Visualizar resultados da consulta

Depois de executar uma consulta e os resultados serem exibidos, você pode ativar Chart (Gráfico) para exibir uma visualização gráfica dos resultados da página atual. Você pode usar os seguintes controles para definir o conteúdo, a estrutura e a aparência do gráfico:

+

Traçado

Representa um conjunto de marcas gráficas relacionadas em um gráfico. Você pode definir vários traçados em um gráfico.

Tipo

Você pode definir o tipo de traçado para representar dados como um dos seguintes:

- Gráfico de dispersão para um diagrama de dispersão ou gráfico de bolhas.
- Gráfico de barras para representar categorias de dados com barras verticais ou horizontais.
- Gráfico de áreas para definir áreas preenchidas.
- Histograma que usa barras para representar distribuição de frequência.
- Gráfico de pizza para uma representação circular de dados, em que cada fatia representa uma porcentagem do todo.
- Gráfico de funil ou de área de funil para representar dados ao longo dos vários estágios de um processo.
- Gráfico OHLC (open-high-low-close) frequentemente usado para dados financeiros para representar valores abertos, altos, baixos e fechados ao longo do eixo x, que geralmente representa intervalos de tempo.
- Gráfico de candelabro para representar um intervalo de valores para uma categoria ao longo de uma linha do tempo.
- Gráfico em cascata para representar como um valor inicial aumenta ou diminui ao longo de uma série de valores intermediários. Os valores podem representar intervalos de tempo ou categorias.
- Gráfico de linhas para representar alterações de valor ao longo do tempo.

Eixo X

Você especifica uma coluna de tabela que contém os valores a serem plotados ao longo do eixo X. As colunas que contêm valores descritivos geralmente representam dados dimensionais. As colunas que contêm valores quantitativos geralmente representam dados factuais.

Eixo Y

Você especifica uma coluna de tabela que contém os valores a serem plotados ao longo do eixo Y. As colunas que contêm valores descritivos geralmente representam dados dimensionais. As colunas que contêm valores quantitativos geralmente representam dados factuais.

Subgráficos

Você pode definir apresentações adicionais dos dados do gráfico.

Transformações

Você pode definir transformações para filtrar os dados dos traçados. Você usa uma transformação dividida para exibir vários traçados saindo de um único traçado-fonte. Você usa uma transformação agregada para apresentar um traçado como uma média ou mínima. Você usa uma transformação de classificação para classificar um traçado.

Aparência geral

Você pode definir padrões para cor de fundo, cor de margem, escalas de cores para paletas de design, estilo e tamanhos de texto, estilo e tamanho de título e barra de modos. Você pode definir interações para arrastar, clicar e passar o mouse. Você pode definir metatextos. Você pode definir as aparências padrão para traçados, eixos, legendas e anotações.

Selecione Traces (Rastreamentos) para exibir os resultados como um gráfico. Em Type (Tipo), escolha o estilo do gráfico comoBar (Barra), Line (Linha) etc. Em Orientation (Orientação), escolha Vertical ou Horizontal. Em X, escolha a coluna da tabela que deseja usar para o eixo horizontal. Em Y, escolha a coluna da tabela que deseja usar para o eixo vertical.

Para atualizar a exibição em gráfico, escolha Refresh (Atualizar). Selecione Full screen (Tela cheia) para expandir a exibição do gráfico.

Criar um gráfico

1. Execute uma consulta e obtenha resultados.
2. Ativar o Charts (Gráficos).
3. Selecione Trace (Rastreamento) comece a visualizar seus dados.
4. Escolha um destes estilos de gráfico:

   - De dispersão
   - Barra
   - Área
   - Histograma
   - Pizza
   - Funil
   - Área do funil
   - OHLC (abertura-alta-baixa-fechamento)

- Vela
- Cascata
- Linha

5. Selecione Style (Estilo) para personalizar a aparência, inclusive cores, eixos, legenda e anotações. É possível adicionar texto, formas e imagens.
6. Selecione Annotations (Anotações) para adicionar texto, formas e imagens.

Para salvar um gráfico

1. Selecione Save Chart (Salvar gráfico).
2. Insira um nome para seu gráfico.
3. Escolha Salvar.

Para exportar um gráfico

1. Escolha Exportar.
2. SelecionePNG ou JPEG.
3. Defina a largura e a altura do gráfico.
4. Escolha Exportar.
5. Selecione para abrir o arquivo em sua aplicação gráfica padrão ou salve o arquivo com o nome padrão.

Para procurar e abrir um gráfico salvo

1. Selecione a guia Charts (Gráficos).
2. Abra o gráfico que você deseja.

Para organizar seus gráficos em pastas

1. Escolha Charts (Gráficos) no painel de navegação.
2. Selecione New folder (Nova pasta) e nomeie a pasta.
3. Selecione Create (Criar) para criar a pasta na guia Charts (Gráficos).

   É possível mover gráficos para dentro e para fora da pasta usando o método arrastar e soltar.

## Exemplo: criar um gráfico de pizza para visualizar os resultados da consulta

O exemplo a seguir usa a tabela Sales do banco de dados de exemplo. Para obter informações, consulte Banco de dados de exemplo no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Veja a seguir a consulta que você executa para fornecer os dados para o gráfico de pizza.

```
select top 5 eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid group by eventname
order by 3;
```

Para criar um gráfico de pizza para o evento principal por total de vendas

1. Executar a consulta.
2. Na área de resultados da consulta, ative Chart (Gráfico).
3. Escolha Traces (Rastreamentos).
4. Em Type (Tipo), escolha Pie (Pizza).
5. Em Values (Valores), escolha totalsales.
6. Em Labels (Etiquetas), escolha eventname.
7. Selecione Style (Estilo) e depois General (Geral).
8. Em Colorscales (Escalas de cores), escolha Categorical (Por categoria) e Pastel2.

## Exemplo: criar um gráfico combinado para comparar receita e vendas

Realize as etapas neste exemplo para criar um gráfico que combina um gráfico de barras para dados de receita e um gráfico de linhas para dados de vendas. O exemplo a seguir usa a tabela Sales (Vendas) do exemplo de banco de dados tickit. Para obter informações, consulte Banco de dados de exemplo no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Veja a seguir a consulta que você executa para fornecer os dados para o gráfico.

```
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;
```

Para criar um gráfico combinado para comparar receita e vendas

1. Executar a consulta.
2. Na área de resultados da consulta, ative Chart (Gráfico).
3. Em trace o (traçado o), para Type (Tipo), escolha Bar (Barra).
4. Para X, escolha eventname (nome do evento).
5. Para Y, escolha total_price (preço_total).

   O gráfico de barras é exibido com os nomes de eventos ao longo do eixo X.
6. Em Style (Estilo), escolha Traces (Traçados).
7. Para Name (Nome), insira Revenue (Receita).
8. Em Style (Estilo), escolha Axes (Eixos).
9. Para Titles (Títulos), escolha Y e insira Revenue (Receita).

   O rótulo Revenue (Receita) é exibido no eixo Y esquerdo.
10. Em Structure (Estrutura), escolha Traces (Traçados).

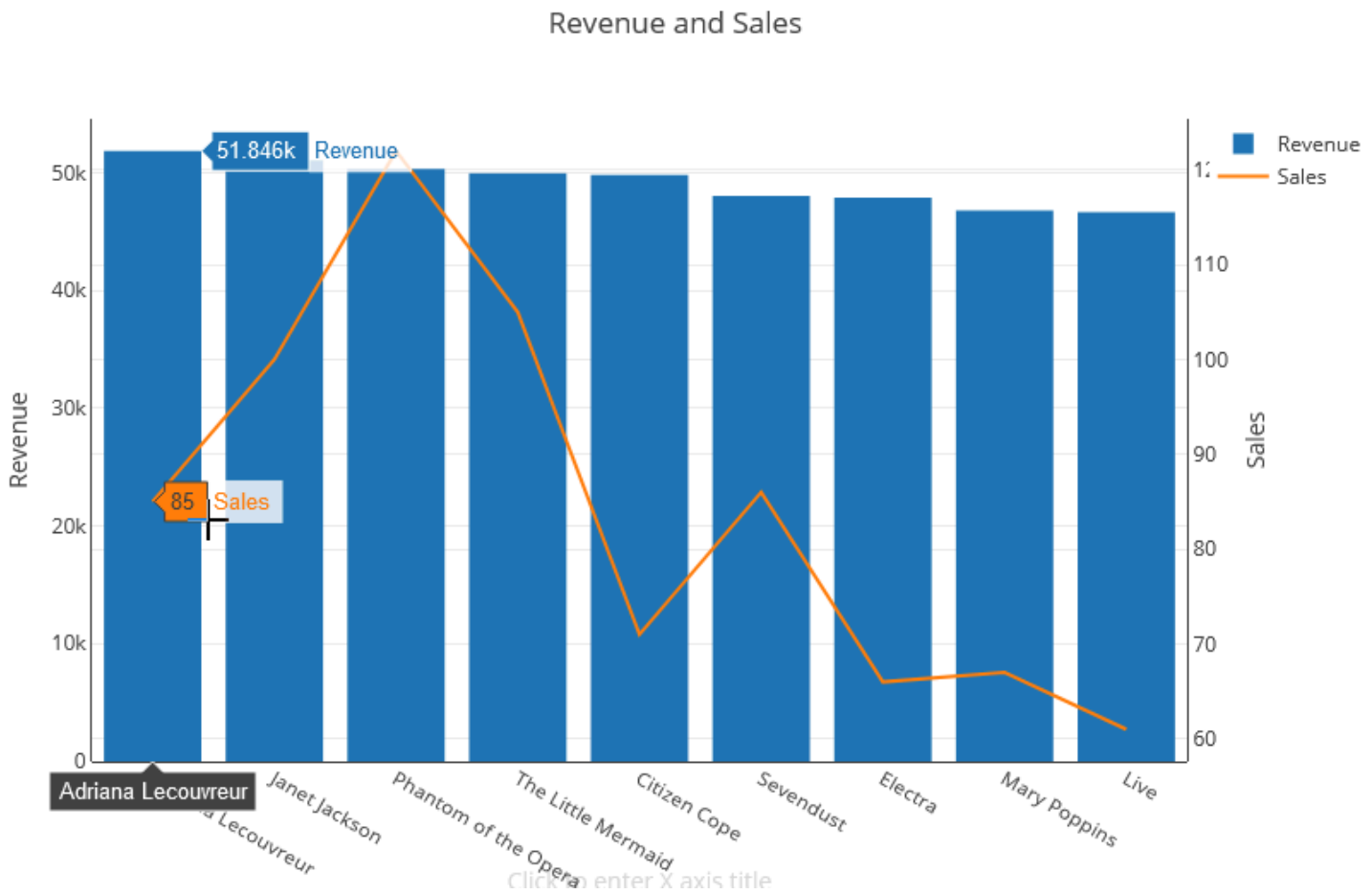
11. Escolha

    Trace (Traçado).

    As opções de trace 1 (traçado 1) são exibidas.
12. Para Type (Tipo), escolha Line (Linha).
13. Para X, escolha eventname (nome do evento).
14. Para Y, escolha total_qty_sold (qtd_total_vendida).
15. Em Axes To Use (Eixos a serem usados), para Y Axis(Eixo Y), escolha

    .

    O Y Axis (eixo Y) exibe Y2.
16. Em Style (Estilo), escolha Axes (Eixos).
17. Em Titles (Títulos), escolha Y2.
18. Para Name (Nome) insira Sales (Vendas).
19. Em Lines (Linhas), escolha Y:Sales (Y:Vendas).
20. Em Axis Line (Linha de eixo), escolha Show (Mostrar) e para Position (Posição), escolha Right (Direita).




## Demonstração: criar visualizações usando o editor de consultas v2 do Amazon Redshift

Para ver uma demonstração de como criar visualizações, assista ao vídeo a seguir. Criar visualizações usando o editor de consultas do Amazon Redshift v2.

# Compartilhar e trabalhar em equipe

Você pode compartilhar consultas com sua equipe.

Uma equipe é definida para um conjunto de usuários que colaboram e compartilham recursos do editor de consultas v2. Um administrador pode criar uma equipe adicionando uma etiqueta a um perfil do IAM. Para obter mais informações, consulte Permissões necessárias para usar o editor de consultas v2 .

## Salvar, procurar e excluir consultas

Antes de compartilhar com a equipe, salve sua consulta. Você pode visualizar e excluir consultas salvas.

Como salvar uma consulta

1. Prepare sua consulta e escolha Save (Salvar).
2. Insira um título para sua consulta.
3. Escolha Salvar.

Para procurar consultas salvas

1. No painel de navegação, escolha Queries (Consultas).
2. Você pode ver consultas que são My queries (Minhas consultas), Shared by me (Compartilhadas por mim) ou Shared to my team (Compartilhadas com minha equipe). Essas consultas podem aparecer como consultas individuais ou em pastas que você criou.

Como excluir uma consulta salva

1. Abra o menu de contexto (clique com o botão direito) para obter uma consulta salva.
2. Selecione Delete (Excluir) e confirme a ação.

Para organizar suas consultas salvas em pastas

1. No painel de navegação, escolha Queries (Consultas).
2. Selecione New folder (Nova pasta) e nomeie a pasta.
3. Selecione Create (Criar) para criar a pasta na guia Queries (Consultas).

   Agora é possível mover consultas para dentro e para fora da pasta usando o método arrastar e soltar.

## Compartilhar uma consulta

Você pode compartilhar consultas com sua equipe. Também é possível visualizar o histórico de consultas salvas e gerenciar versões de consulta.

Para compartilhar uma consulta com a equipe, verifique se tem a etiqueta da entidade principal `sqlworkbench-team` definida com o mesmo valor que o restante dos membros de sua equipe em sua conta. Por exemplo, um administrador pode definir o valor como `accounting-team` para todos os membros do departamento de contabilidade. Para ver um exemplo, consulte Permissões necessárias para usar o editor de consultas v2 .

Para compartilhar uma consulta com uma equipe

1. No painel de navegação, escolha Queries (Consultas).
2. Abra o menu de contexto (clique com o botão direito do mouse) da consulta que você deseja compartilhar e escolha Share with my team (Compartilhar com minha equipe).
3. Escolha as equipes com as quais você deseja compartilhar a consulta e escolha Save sharing options (Salvar opções de compartilhamento).

Toda vez em que você salva uma consulta SQL, o editor de consultas v2 a salva como uma nova versão. É possível procurar versões de consulta anteriores, salvar uma cópia de uma consulta ou restaurar uma consulta.

Para gerenciar versões de consulta

1. No painel de navegação, escolha Queries (Consultas).
2. Abra o menu de contexto (clique com o botão direito do mouse) da consulta com a qual você deseja trabalhar.
3. Selecione Version history (Histórico de versões) para abrir uma lista de versões da consulta.
4. Na página Version history (Histórico de versões), você pode fazer o seguinte:
   - Revert to selected (Reverter para a selecionada): reverta para a versão selecionada e continue seu trabalho com esta versão.
   - Save selected as (Salvar selecionada como): crie uma nova consulta no editor.

# Consultar um banco de dados usando o Query Editor

Usar o editor de consulta é uma maneira fácil de executar consultas em bancos de dados hospedados por seu cluster do Amazon Redshift. Depois de criar seu cluster, você pode executar consultas imediatamente usando o editor de consultas no console do Amazon Redshift.

> **Note**
>
> Você não pode consultar dados no Amazon Redshift Serverless usando esse editor de consultas original. Use o editor de consultas v2 do Amazon Redshift.

Em fevereiro de 2021, um editor de consultas atualizado foi implantado e as permissões de autorização para usar o editor de consultas foram alteradas. O novo editor de consultas usa a API de dados do Amazon Redshift para executar consultas. A política `AmazonRedshiftQueryEditor`, que é uma política do AWS Identity and Access Management (IAM) gerenciada pela AWS, foi atualizada para incluir as permissões necessárias. Se você tiver uma política do IAM personalizada, certifique-se de atualizá-la. Use o `AmazonRedshiftQueryEditor` como um guia. Essas alterações no `AmazonRedshiftQueryEditor` incluem o seguinte:

- A permissão para gerenciar os resultados da instrução do editor de consulta requer o usuário proprietário da instrução.
- A permissão para usar o Secrets Manager para se conectar a um banco de dados foi adicionada.

Para ter mais informações, consulte Permissões necessárias para usar o editor de consulta do console do Amazon Redshift.

Quando você se conecta ao cluster a partir do novo editor de consultas, você pode usar um dos dois métodos de autenticação, conforme descrito em Conectando-se com o editor de consultas.

Usando o Query Editor, você pode fazer o seguinte:

- Execute consultas únicas de comando SQL.
- Faça download de conjuntos de resultados de até 100 MB para um arquivo de valores separados por vírgula (CSV).
- Salve consultas para reutilização. Você não pode salvar consultas em na região da Europa (Paris), Ásia-Pacífico (Osaka), Ásia-Pacífico (Hong Kong) ou do Oriente Médio (Bahrein).
- Visualizar os detalhes do tempo de execução da consulta para tabelas definidas pelo usuário.
- Agendar consultas para serem executadas em um momento futuro.
- Exibir um histórico de consultas que você criou no editor de consultas.
- Executar consultas em clusters usando o roteamento aprimorado da VPC.

## Considerações do Query Editor

Considere o seguinte sobre como trabalhar com consultas ao usar o editor de consultas:

- A duração máxima de uma consulta é de 24 horas.
- O tamanho máximo do resultado da consulta é 100 MB. Se uma chamada retornar mais de 100 MB de dados de resposta, a chamada será encerrada.
- O tempo máximo de retenção para resultados da consulta é de 24 horas.
- O tamanho máximo da instrução de consulta é de 100 KB.
- O cluster deve estar em uma Virtual Private Cloud (VPC) baseada no serviço Amazon VPC.
- Você não pode usar transações no Query Editor. Para obter mais informações sobre transações, consulte BEGIN no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- Você pode salvar uma consulta de até 3.000 caracteres.

## Habilitar o acesso ao Query Editor

Para acessar o Query Editor, você precisa de permissão. Para habilitar o acesso, recomendamos que você anexe as políticas `AmazonRedshiftQueryEditor` e `AmazonRedshiftReadOnlyAccess` gerenciadas pela AWS para obter permissões do IAM para o perfil do IAM que você usa para acessar o cluster. Então, é possível atribuir o perfil a um usuário. Você pode usar o console do IAM (https://console.aws.amazon.com/iam/) para anexar políticas do IAM. Para obter mais informações, consulte Usar políticas baseadas em identidade (políticas do IAM) para o Amazon Redshift.

Se você já criou um usuário para acessar o Amazon Redshift, é possível anexar as políticas `AmazonRedshiftQueryEditor` e `AmazonRedshiftReadOnlyAccess` gerenciadas pela AWS a esse usuário por meio de um perfil atribuído. Se você ainda não criou um usuário, crie-o, anexe a política ao perfil do IAM e atribua-o ao usuário.

A política `AmazonRedshiftQueryEditor` gerenciada pela AWS permite a ação `redshift:GetClusterCredentials` que, por padrão, concede ao superusuário acesso ao banco de dados. Para restringir o acesso, você pode fazer o seguinte:

- Criar uma política personalizada que permite chamar `redshift:GetClusterCredentials` e restringir o recurso a um determinado valor para `DbUser`.

- Adicione uma política que negue permissão a `redshift:GetClusterCredentials`. Todo usuário atribuído a um perfil com essa permissão anexada deve fazer login no editor de consultas com credenciais temporárias. Essa política de negação ilustra o exemplo.

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

Para obter mais informações sobre como criar um perfil com as permissões necessárias, consulte Para criar um perfil do IAM com permissões para chamar GetClusterCredentials.

Todo usuário com acesso ao Editor de Consultas do Amazon Redshift por meio da política `AmazonRedshiftQueryEditor` gerenciada pela AWS pode listar todos os segredos. No entanto, essa política permite a criação e a recuperação somente de segredos marcados com a chave `RedshiftQueryOwner` e o valor `${aws:userid}`. Se você criar a chave a partir do Editor de Consultas do Amazon Redshift, a chave será automaticamente marcada. Para usar um segredo que não foi criado com o editor de consultas do Amazon Redshift, confirme se o segredo está marcado com a chave `RedshiftQueryOwner` e um valor de seu identificador de usuário exclusivo do IAM, por exemplo `AIDACKCEVSQ6C2EXAMPLE`.

As permissões necessárias para usar o Editor de Consultas do Amazon Redshift são AmazonRedshiftQueryEditor e AmazonRedshiftReadOnlyAccess.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:

- Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
- (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

## Conectando-se com o editor de consultas

Quando você se conecta a um cluster com o editor de consultas, será necessário usar um dos métodos de autenticação a seguir. Cada método requer uma combinação diferente de entrada do console do Amazon Redshift.

AWS Secrets Manager

Com este método, forneça um valor secreto para secret-arn que é armazenado no AWS Secrets Manager. Este segredo contém credenciais para se conectar ao seu banco de dados.

Credenciais temporárias

Com este método, forneça os valoers do banco de dados e db-user.

### Armazenar credenciais de banco de dados no AWS Secrets Manager

Ao chamar o editor de consulta, você pode passar credenciais para o cluster usando um segredo no AWS Secrets Manager. Para passar credenciais dessa maneira, especifique o nome do segredo ou o nome do recurso da Amazon (ARN) do segredo.

Para obter mais informações sobre as permissões mínimas, consulte Criação e gerenciamento de segredos com o AWS Secrets Manager no Manual do usuário do AWS Secrets Manager.

Para armazenar suas credenciais em um segredo para um cluster do Amazon Redshift

1. Use o AWS Secrets Manager para criar um segredo que contenha credenciais para o cluster. Quando você escolher Armazenar um novo segredo, escolha Credenciais do cluster Redshift. Armazenar um valor para Nome de usuário (o usuário do banco de dados), Senha e Cluster do DB (identificador de cluster) em seu segredo.

   Para obter instruções, consulte Criar um segredo básico no Manual do usuário do AWS Secrets Manager.

2. Use o console do AWS Secrets Manager para visualizar os detalhes do segredo criado ou execute o comando `aws secretsmanager describe-secret` da AWS CLI.

Se optar por usar as credenciais de administrador do clusterAWS Secrets Manager, você poderá se conectar ao banco de dados usando as credenciais de administrador armazenadas no Secrets Manager.

## Como usar o editor de consulta

No exemplo a seguir, você usa o Query Editor para executar as seguintes tarefas:

- Executar comandos SQL.
- Exibir detalhes de execução da consulta.
- Salvar uma consulta.
- Fazer download de um conjunto de resultados da consulta.

Para concluir o exemplo a seguir, você precisa de um cluster existente do Amazon Redshift. Se você não tiver um cluster, crie um seguindo o procedimento descrito em Criar um cluster.

Para usar o editor de consulta no console do Amazon Redshift

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Query editor (Editor de consultas) e conecte-se a um banco de dados em seu cluster.
3. Para Schema (Esquema), escolha public (público) para criar uma tabela com base nesse esquema.
4. Insira o seguinte na janela do Query Editor e escolha Run (Executar) para criar uma nova tabela.

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

5. Escolha Clear (Limpar).
6. Insira o seguinte comando na janela do Query Editor e escolha Run (Executar) para adicionar linhas à tabela.

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

7. Escolha Clear (Limpar).
8. Insira o seguinte comando na janela do Query Editor e escolha Run (Executar) para consultar a nova tabela.

```
select * from shoes;
```

Os Query results (Resultados da consulta) exibem os resultados.

| Tipo de calçado | Cor |
|---|---|
| sandália | preta |
| mocassim | marrom |

9. Escolha Execution (Execução) para visualizar os detalhes da execução.
10. Escolha Data (Dados) e Export (Exportar) para fazer download dos resultados da consulta como um arquivo.

## Programar uma consulta

> **Important**
>
> O Editor de Consultas v2 do Amazon Redshift já oferece suporte ao agendamento de consultas. Recomendamos que você use o Editor de Consultas v2. Para ter mais informações, consulte Programar uma consulta com o editor de consultas v2.

Para criar uma programação para executar uma instrução SQL, você pode usar o editor de consulta no console do Amazon Redshift. Você pode criar uma programação para executar sua instrução SQL nos intervalos de tempo que correspondam às suas necessidades de negócios. Quando é hora da execução da consulta programada, o Amazon EventBridge inicia a consulta.

Como criar uma programação a fim de executar uma instrução SQL

1. Abra o console e o editor de consulta conforme descrito em Como usar o editor de consulta . Você só pode usar esse editor de consultas com clusters provisionados.
2. Selecione Programar para criar uma programação para executar uma instrução SQL.

   Quando você define a programação, fornece as seguintes informações:

   - Uma função do IAM usada para assumir as permissões necessárias para executar a consulta. Para ter mais informações, consulte Configurar permissões para programar uma consulta.
   - Os valores de autenticação para AWS Secrets Manager ou credenciais temporárias para autorizar o acesso ao cluster. Para ter mais informações, consulte Autenticar uma consulta programada.
   - O nome da consulta programada e uma única instrução SQL a ser executada.
   - A frequência de programação e opções de repetição ou um valor formatado cron.
   - Opcionalmente, você pode ativar as notificações do Amazon SNS para monitorar a consulta programada. Se a consulta estiver sendo executada, mas você não vir mensagens publicadas no tópico do SNS, consulte Minha regra está sendo acionada, mas eu não vejo nenhuma mensagem publicada no meu tópico do Amazon SNS no Manual do usuário do Amazon EventBridge.

Você também pode gerenciar e atualizar consultas programadas usando o console do Amazon Redshift. Dependendo da sua versão do console, as consultas programadas podem ser listadas nos seguintes locais:

- Na guia Programações da página de detalhes do seu cluster.
- Na guia Consultas programadas do editor de consulta.

Se escolher Nome da programação em um desses locais, é possível visualizar e editar a definição de sua consulta programada.

## Configurar permissões para programar uma consulta no console do Amazon Redshift

Para proramar consultas, o usuário do AWS Identity and Access Management (IAM) definindo a programação e a função do IAM associada à programação devem ser configurados da maneira a seguir.

Para o usuário do IAM conectado ao console do Amazon Redshift, faça o seguinte:

- Anexe a política `AmazonEventBridgeFullAccess` gerenciada pela AWS a um perfil do IAM.
- Anexe uma política com a permissão `sts:AssumeRole` da função do IAM que você especificou ao definir a instrução SQL agendada.

  O exemplo a seguir mostra uma política que assume uma função do IAM especificada.

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

Para a função do IAM especificada para permitir que o programador execute uma consulta, faça o seguinte:

- Certifique-se de que essa função do IAM especifique a entidade principal de serviço EventBridge (`events.amazonaws.com`). A seguir está um exemplo de relação de confiança.

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

Para obter mais informações sobre como criar uma função do IAM para eventos do EventBridge, consulte Permissões necessárias para usar o programador do Amazon EventBridge.

- Anexe a política `AmazonRedshiftDataFullAccess` gerenciada pela AWS ao perfil do IAM.
- Para permitir que os usuários visualizem o histórico de programações, edite o perfil do IAM para adicionar a permissão `sts:AssumeRole`.

Veja a seguir um exemplo de política de confiança em um perfil do IAM.

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

## Autenticar uma consulta programada

Quando você programar uma consulta, você usa um dos métodos de autenticação a seguir quando a consulta SQL é executada. Cada método requer uma combinação diferente de entrada do console do Amazon Redshift.

AWS Secrets Manager

Com este método, forneça um valor secreto para secret-arn que é armazenado no AWS Secrets Manager. Este segredo contém credenciais para se conectar ao seu banco de dados. O segredo deve ser marcado com a chave `RedshiftDataFullAccess`.

Para obter mais informações sobre as permissões mínimas, consulte Criação e gerenciamento de segredos com o AWS Secrets Manager no Manual do usuário do AWS Secrets Manager.

Credenciais temporárias

Com este método, forneça os valoers do banco de dados e db-user.

A política `AmazonRedshiftDataFullAccess` concede ao usuário do banco de dados chamado `redshift_data_api_user`permissão para `redshift:GetClusterCredentials`. Se você quiser usar um usuário de banco de dados diferente para executar a instrução SQL, adicione uma política à função do IAM para permitir `redshift:GetClusterCredentials`. O exemplo a seguir permite usuários do banco de dados `awsuser` e `myuser`.

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

## Criar uma regra do Amazon EventBridge que é executada quando uma consulta é concluída

Você pode criar uma regra de evento para enviar uma notificação quando uma consulta é concluída. Para ver o procedimento usando o console do Amazon EventBridge, consulte Creating Amazon EventBridge rules that react to events (Criar regras do Amazon EventBridge que reagem a eventos) no Amazon EventBridge User Guide (Guia do usuário do Amazon EventBridge. Para obter mais informações, consulte Padrões de eventos do Amazon EventBridge no Manual do usuário do Amazon EventBridge.

Por exemplo, o exemplo de evento a seguir é enviado quando uma consulta é `FINISHED`.

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
```

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

Você pode criar uma regra de padrão de evento para filtrar o evento.

```
{
    "source": [
        "aws.redshift-data"
    ],
    "detail-type": [
        "Redshift Data Statement Status Change"
    ],
    "detail": {
        "state": [
            "FINISHED"
        ]
    }
}
```

# Conectar-se a um data warehouse do Amazon Redshift usando ferramentas de cliente SQL

É possível se conectar a data warehouses do Amazon Redshift por meio de ferramentas de cliente SQL em conexões Java Database Connectivity (JDBC), Python e Open Database Connectivity

(ODBC). O Amazon Redshift não fornece nem instala nenhuma ferramenta ou biblioteca de cliente SQL. Para usar essas ferramentas ou bibliotecas para trabalhar com dados nos data warehouses, instale-as no computador cliente ou na instância do Amazon EC2. Você pode usar a maioria das ferramentas do cliente SQL que oferecem suporte aos drivers JDBC, Python ou ODBC.

Use a lista de seções no final deste tópico para ajudar você a percorrer o processo de configuração de seu computador cliente ou instância do Amazon EC2 para usar uma conexão JDBC, Python ou ODBC. Nesses tópicos, também são discutidas opções de segurança relacionadas para a conexão do cliente ao servidor. Além disso, encontre informações sobre como configurar e se conectar a partir de ferramentas do cliente SQL, como o SQL Workbench/J, uma ferramenta de terceiro e o Amazon Redshift RSQL. Experimente essas ferramentas se ainda não tiver uma ferramenta de business intelligence para usar. Também é possível usar esta seção para saber mais sobre como se conectar a um data warehouse por meio de programação. Por fim, se você encontrar problemas ao tentar se conectar ao data warehouse, poderá examinar as informações de solução de problemas para identificar soluções.

## Recomendações para conexão com ferramentas do cliente

Se você se conectar ao cluster do Redshift usando um endereço IP, isso poderá resultar em tempo de inatividade adicional quando houver interrupção ou perda de conexão e o cluster for colocado on-line em uma nova zona de disponibilidade (AZ). No entanto, se você ainda quiser que a aplicação se conecte ao Redshift utilizando um endereço IP, use o endereço IP privado anexado ao endpoint da nuvem privada virtual (VPC) do cluster. Você pode encontrar isso nos detalhes do cluster em Rede e segurança, na guia Propriedades.

> **Note**
>
> Se a aplicação usa o endereço IP do nó líder para acessar o cluster do Redshift, a prática recomendada é alterá-lo para usar o URL do endpoint do cluster. Para obter mais informações, consulte Configurar conexões no Amazon Redshift.

Tópicos


- Configurar conexões no Amazon Redshift
- Configurar as opções de segurança para conexões
- Conexão de código e ferramentas clientes
- Conectar-se com SQL Workbench/J

- Conectar-se ao data warehouse de forma programática
- Usar um perfil de autenticação para se conectar ao Amazon Redshift
- Solução de problemas de conexão no Amazon Redshift

# Configurar conexões no Amazon Redshift

Na próxima seção, saiba como configurar as conexões JDBC, Pyhton e ODBC para se conectar ao cluster pelas ferramentas do cliente SQL. Esta seção descreve como configurar conexões JDBC, Pyhton e ODBC. Também descreve como usar o Secure Sockets Layer (SSL) e os certificados de servidores para criptografar as comunicações entre o cliente e o servidor.

## Drivers JDBC, Pyhton e ODBC para o Amazon Redshift

Para trabalhar com dados no cluster, você precisa ter os drivers JDBC, Python ou ODBC para estabelecer a conexão do computador cliente ou da instância. Escreva o código de suas aplicações de modo que usem as operações de API de acesso a dados JDBC, Python ou ODBC e use as ferramentas do cliente SQL que oferecem suporte a JDBC, Pyhton ou ODBC.

O Amazon Redshift oferece drivers JDBC, Pyhton e ODBC para baixar. Esses drivers contam com suporte do AWS Support. Os drivers PostgreSQL não são testados e nem tê suporte da equipe do Amazon Redshift. Use os drivers específicos do Amazon Redshift ao se conectar a um cluster do Amazon Redshift. Os drivers do Amazon Redshift têm as seguintes vantagens:

- Compatível com IAM, SSO e autenticação federada.
- Compatível com novos tipos de dados do Amazon Redshift.
- Compatível com perfis de autenticação.
- Melhor performance em conjunto com aprimoramentos do Amazon Redshift.

Para obter mais informações sobre como baixar os drivers do JDBC e do ODBC e configurar as conexões para o cluster, consulte Configurar uma conexão para o driver JDBC versão 2.1 para o Amazon Redshift, Configurar o conector Python do Amazon Redshift e Configurar uma conexão ODBC.

Para obter mais informações sobre o gerenciamento de identidades do IAM, incluindo práticas recomendadas para perfis do IAM, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift.

### Encontrar a string de conexão do cluster

Para conectar-se ao cluster com a ferramenta do cliente SQL, você precisa ter a string de conexão do cluster. Você pode encontrar a string de conexão do cluster no console do Amazon Redshift, na página de detalhes de um cluster.

Para encontrar a string de conexão de um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters e o nome do cluster na lista para abrir os respectivos detalhes.
3. O URL do JDBC e URL do ODBC estão disponíveis, juntamente com detalhes adicionais, na seção Informações gerais. Cada string é baseada na região da AWS em que o cluster é executado. Clique no ícone ao lado da string de conexão apropriada para copiá-la.

Para se conectar a um endpoint de cluster, você pode usar o URL do endpoint de cluster de uma solicitação da API DescribeClusters. Veja a seguir um exemplo de URL de endpoint de cluster.

```
mycluster.cmeaswqeuae.us-east-2.redshift.amazonaws.com
```

Se você configurou um nome de domínio personalizado para o cluster, também poderá usá-lo para se conectar ao cluster. Para obter mais informações sobre como criar um nome de domínio personalizado, consulte Configurar um nome de domínio personalizado.

> **Note**
>
> Ao se conectar, não use o endereço IP de um nó do cluster nem o endereço IP do endpoint da VPC. Sempre use o endpoint do Redshift para evitar interrupção desnecessária. A única exceção ao uso do URL do endpoint é quando você utiliza um nome de domínio personalizado. Para obter mais informações, consulte Usar nome de domínio personalizado para conexões de clientes.

## Configurar uma conexão para o driver JDBC versão 2.1 para o Amazon Redshift

Você pode usar uma conexão do driver JDBC versão 2.1 para se conectar ao cluster do Amazon Redshift a partir de várias ferramentas de cliente SQL de terceiros. O conector JDBC do Amazon

Redshift oferece uma solução de código-fonte aberto. É possível navegar pelo código-fonte, solicitar aprimoramentos, relatar problemas e fornecer contribuições.

Para usar uma conexão JDBC, consulte as seções a seguir.

Tópicos


- Baixe o driver JDBC do Amazon Redshift, versão 2.1
- Instalar o driver JDBC do Amazon Redshift, versão 2.1
- Obter o URL do JDBC
- Construir o URL de conexão
- Configurando manutenções de atividade de TCP para a conexão JDBC
- Configurar sua conexão JDBC com o Apache Maven
- Configurar a autenticação e o SSL
- Configurar o registro em log do
- Conversão de tipos de dados
- Usando suporte a instruções preparadas
- Diferenças entre as versões 2.1 e 1.x do driver JDBC
- Criar arquivos de inicialização (.ini) para o driver JDBC versão 2.1
- Opções para a configuração do driver JDBC versão 2.1
- Versões anteriores do driver JDBC versão 2.1


## Baixe o driver JDBC do Amazon Redshift, versão 2.1

O Amazon Redshift oferece drivers para ferramentas compatíveis com a API JDBC 4.2. O nome da classe deste driver é `com.amazon.redshift.Driver`.

Para obter informações detalhadas sobre como instalar o driver JDBC, consulte as bibliotecas do driver JDBC e registre a classe do driver, consulte os tópicos a seguir.

Para cada computador em que você usa o driver Amazon Redshift JDBC versão 2.1, verifique se o Java Runtime Environment (JRE) 8.0 está instalado.

Se você usar o driver JDBC Amazon Redshift para autenticação de banco de dados, certifique-se de ter AWS SDK for Java 1.11.118 ou posterior em seu caminho de classe Java. Se você não tiver AWS SDK for Java instalado, baixe o arquivo ZIP com as bibliotecas dependentes de driver e driver compatíveis com JDBC 4.2 para o AWS SDK:

- Driver compatível com JDBC 4.2 versão 2.1 e bibliotecas dependentes do driver AWS SDK

  Este arquivo ZIP contém o driver compatível com JDBC 4.2 versão 2.1 e arquivos de biblioteca dependentes do driver AWS SDK para Java 1.x. Descompacte os arquivos jar dependentes no mesmo local que o driver JDBC. Somente o driver JDBC precisa estar no CLASSPATH.

  Este arquivo ZIP não inclui o AWS SDK for Java 1.x. No entanto, ele inclui as bibliotecas dependnetes de driver 1.x AWS SDK for Java que são necessárias para autenticação de banco de dados do AWS Identity and Access Management (IAM).

  Use este driver JDBC do Amazon Redshift com o AWS SDK necessário para a autenticação do banco de dados do IAM.

  Para instalar o AWS SDK for Java 1.x, consulte AWSSDK for Java 1.x no Guia do desenvolvedor do AWS SDK for Java.
- Driver compatível com JDBC 4.2 versão 2.1 (sem o AWS SDK)

Revise a licença do software JDBC versão 2.1 e altere o arquivo de log:

- Licença do driver JDBC versão 2.1
- Log de alteração do driver JDBC versão 2.1

Os drivers JDBC versão 1.2.27.1051 e posteriores oferecem suporte a procedimentos armazenados do Amazon Redshift. Para obter mais informações, consulte Como criar procedimentos armazenados no Amazon Redshift no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Instalar o driver JDBC do Amazon Redshift, versão 2.1

Para instalar a versão 2.1 do driver compatível com o Amazon Redshift JDBC 4.2 e as bibliotecas dependentes de driver para o AWS SDK, extraia os arquivos do arquivo ZIP para o diretório de sua preferência.

Para instalar o driver compatível com o Amazon Redshift JDBC 4.2 versão 2.1 (sem o AWS SDK), copie o arquivo JAR para o diretório de sua preferência.

Para acessar um armazenamento de dados do Amazon Redshift usando o driver JDBC do Amazon Redshift, você precisa executar a configuração conforme descrito a seguir.

Tópicos

- Referenciar as bibliotecas de driver JDBC
- Registrar a classe de driver

### Referenciar as bibliotecas de driver JDBC

A aplicação JDBC ou código Java que você usa para se conectar aos seus dados deve acessar os arquivos JAR do driver. Na aplicação ou código, especifique todos os arquivos JAR extraídos do arquivo ZIP.

#### Usar o driver em uma aplicação JDBC

As aplicações JDBC geralmente fornecem um conjunto de opções de configuração para adicionar uma lista de arquivos de biblioteca de drivers. Use as opções fornecidas para incluir todos os arquivos JAR do arquivo ZIP como parte da configuração do driver na aplicação. Para obter mais informações, consulte a documentação de sua aplicação JDBC.

#### Usar o driver no código Java

Você deve incluir todos os arquivos de biblioteca de driver no caminho da classe. Este é o caminho que o Java Runtime Environment procura por classes e outros arquivos de recursos. Para obter mais informações, consulte a documentação apropriada do Java SE para definir o caminho da classe para o seu sistema operacional.

- Windows: https://docs.oracle.com/javase/7/docs/technotes/tools/windows/classpath.html
- Linux e Solaris: https://docs.oracle.com/javase/7/docs/technotes/tools/solaris/classpath.html
- MacOS: o caminho padrão da classe MacOS é o diretório no qual o driver JDBC está instalado.

### Registrar a classe de driver

Certifique-se de registrar a classe apropriada para a sua aplicação. Use as seguintes classes para conectar o driver JDBC do Amazon Redshift aos armazenamentos de dados do Amazon Redshift:

- Classes `Driver` estendem `java.sql.Driver`.
- Classes `DataSource` estendem `javax.sql.DataSource` e `javax.sql.ConnectionPoolDataSource`.

O driver suporta os seguintes nomes de classe totalmente qualificados que são independentes da versão JDBC:

- `com.amazon.redshift.jdbc.Driver`
- `com.amazon.redshift.jdbc.DataSource`

O exemplo a seguir mostra como usar a classe DriverManager para estabelecer uma conexão para JDBC 4.2.

```
            private static Connection connectViaDM() throws Exception
{
Connection connection = null;
connection = DriverManager.getConnection(CONNECTION_URL);
return connection;
}
```

O exemplo a seguir mostra como usar a classe `DataSource` para estabelecer uma conexão.

```
 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;
}
```

Obter o URL do JDBC

Antes de se conectar ao seu cluster Amazon Redshift a partir de uma ferramenta de cliente SQL, você precisa saber o URL do JDBC do seu cluster. O URL do JDBC tem o seguinte formato: `jdbc:redshift://`*`endpoint`*`:`*`port`*`/`*`database`*.

Os campos do formato anterior possuem os valores a seguir.

| Campo | Valor |
| --- | --- |
| `jdbc` | O protocolo para a conexão. |
| `redshift` | O subprotocol que especifica o uso do driver Amazon Redshift para se conectar ao banco de dados. |
| *`endpoint`* | O endpoint do cluster Amazon Redshift. |
| *`port`* | O número da porta usado quando você iniciou o cluster. Se você tem um firewall, verifique se essa porta está aberta para uso. |
| *`database`* | O banco de dados que você criou para o cluster. |

Este é um exemplo de URL do JDBC: `jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev`

Certifique-se de inserir os valores de URL, por exemplo, valores de SessionToken, no formato codificado de URL.

Para obter informações sobre como obter sua conexão JDBC, consulte Encontrar a string de conexão do cluster.

Se a conexão do computador cliente com o banco de dados falhar, você pode tentar solucionar os possíveis problemas. Para obter mais informações, consulte Solução de problemas de conexão no Amazon Redshift.

Construir o URL de conexão

Use o URL de conexão para fornecer informações de conexão ao armazenamento de dados que você está acessando. A seguir está o formato da URL de conexão do driver JDBC do Amazon Redshift versão 2.1. Aqui, [Host] é o endpoint do servidor Amazon Redshift e [Port] é o número da porta Transmission Control Protocol (TCP) que o servidor usa para atender solicitações de clientes.

```
jdbc:redshift://[Host]:[Port]
```

Segue-se o formato de um URL de ligação que especifica algumas definições opcionais.

```
jdbc:redshift://[Host]:[Port]/[database];[Property1]=[Value];
```

```
[Property2]=[Value];
```

Por exemplo, suponha que você queira se conectar à porta 9000 em um cluster do Amazon Redshift na região Oeste dos EUA (Norte da Califórnia) na AWS. Você também deseja acessar o banco de dados chamado dev e autenticar a conexão usando um nome de usuário e senha do banco de dados. Nesse caso, use o URL de conexão a seguir.

```
jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/
dev;UID=amazon;PWD=amazon
```

Você pode usar os seguintes caracteres para separar as opções de configuração do restante da string de URL:

- ;
- ?

Por exemplo, as strings de URL a seguir são equivalentes:

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

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

Você pode usar os seguintes caracteres para separar as opções de configuração umas das outras na string de URL:

- ;
- &

Por exemplo, as strings de URL a seguir são equivalentes:

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

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

O exemplo de URL a seguir especifica um nível de log de 6 e o caminho para os logs.

```
jdbc:redshift://redshift.amazonaws.com:5439/dev;DSILogLevel=6;LogPath=/home/user/logs;
```

Não duplique propriedades no URL de conexão.

Para obter uma lista completa das opções de configuração que você pode especificar, consulte Opções para a configuração do driver JDBC versão 2.1.

> **Note**
>
> Ao se conectar, não use o endereço IP de um nó do cluster nem o endereço IP do endpoint da VPC. Sempre use o endpoint do Redshift para evitar interrupção desnecessária. A única exceção ao uso do URL do endpoint é quando você utiliza um nome de domínio personalizado. Para obter mais informações, consulte Usar nome de domínio personalizado para conexões de clientes.

### Configurando manutenções de atividade de TCP para a conexão JDBC

Por padrão, o driver JDBC do Amazon Redshift é configurado para usar keepalives TCP para evitar que o tempo limite das conexões se esgote. Você pode especificar quando o driver começa a enviar pacotes keepalive ou desligar o recurso definindo as propriedades relevantes no URL de conexão. Para obter mais informações sobre a sintaxe do URL de conexão, consulte Construir o URL de conexão.

| Propriedade | Descrição |
| --- | --- |
| `TCPKeepAlive` | Para desativar as keepalives de TCP, defina essa propriedade como `FALSE`. |

### Configurar sua conexão JDBC com o Apache Maven

O Apache Maven é uma ferramenta de gerenciamento e compreensão de projetos de software. O AWS SDK for Java é compatível com os projetos do Apache Maven. Para obter mais informações, consulte Usar o SDK com o Apache Maven no Guia do desenvolvedor do AWS SDK for Java.

Se você usa o Apache Maven, pode configurar e construir seus projetos para usar um driver JDBC do Amazon Redshift para se conectar ao seu cluster do Amazon Redshift. Para fazer isso, adicione o driver JDBC como uma dependência no arquivo `pom.xml` do projeto. Se você usa o Maven para compilar um projeto e deseja usar uma conexão JDBC, siga as etapas da próxima seção.

Configuração do driver de JDBC como uma dependência do Maven

Como configurar o driver JDBC como uma dependência do Maven

1. Adicione o repositório Amazon ou o repositório Maven Central à seção de repositórios do arquivo `pom.xml`.

   > **Note**
   >
   > O URL exibido no exemplo de código a seguir retornará um erro se for usado em um navegador. Use este URL somente no contexto de um projeto Maven.

   Para um repositório do Amazon Maven, use o seguinte.

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

   Para conectar-se usando Secure Sockets Layer (SSL), adicione o repositório a seguir ao arquivo `pom.xml`.

   ```
   <repositories>
       <repository>
         <id>redshift</id>
         <url>https://s3.amazonaws.com/redshift-maven-repository/release</url>
       </repository>
   </repositories>
   ```

   Para um repositório Maven Central, adicione o seguinte ao arquivo `pom.xml`:

   ```
   <repositories>
       <repository>
         <id>redshift</id>
         <url>https://repo1.maven.org/maven2</url>
       </repository>
   ```

```
</repositories>
```

2. Declare a versão do driver que deseja usar na seção de dependências do arquivo `pom.xml`.

   O Amazon Redshift oferece drivers para ferramentas compatíveis com a API JDBC 4.2. Para obter informações sobre a funcionalidade compatível com esses drivers, consulte Baixe o driver JDBC do Amazon Redshift, versão 2.1.

   Adicione uma dependência para o driver conforme mostrado a seguir.

   Substitua *`driver-version`* no exemplo a seguir com a versão do driver, por exemplo `2.1.0.1`.

   Para um driver compatível com JDBC 4.2, use o seguinte:

```
<dependency>
   <groupId>com.amazon.redshift</groupId>
   <artifactId>redshift-jdbc42</artifactId>
   <version>driver-version</version>
</dependency>
```

   O nome da classe deste driver é `com.amazon.redshift.Driver`.

Os drivers do Amazon Redshift Maven precisam das dependências opcionais a seguir quando você usa a autenticação de banco de dados do 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>
```

Atualização do driver para a versão mais recente

Para atualizar ou alterar o driver JDBC do Amazon Redshift para a versão mais recente, primeiro modifique a seção de versão da dependência para a versão mais recente do driver. Limpe seu projeto com o Maven Clean Plugin, conforme mostrado a seguir.

```
mvn clean
```

Configurar a autenticação e o SSL

Para proteger os dados contra acesso não autorizado, os armazenamentos de dados do Amazon Redshift exigem que todas as conexões sejam autenticadas usando credenciais do usuário. Alguns armazenamentos de dados também exigem conexões a serem feitas através do protocolo Secure Sockets Layer (SSL) com ou sem autenticação unidirecional.

O driver JDBC do Amazon Redshift versão 2.1 fornece suporte completo a esses protocolos de autenticação.

A versão SSL que o driver suporta depende da versão JVM que você está usando. Para obter informações sobre as versões SSL compatíveis com cada versão do Java, consulte Diagnosticar TLS, SSL e HTTPS no Blog de gerenciamento de produtos do grupo de plataformas Java.

A versão SSL usada para a conexão é a versão mais alta aceita pelo driver e pelo servidor, que é determinada no momento da conexão.

Configure o driver JDBC versão 2.1 do Amazon Redshift para autenticar a conexão de acordo com os requisitos de segurança do servidor do Redshift ao qual você está se conectando.

Você deve sempre fornecer seu nome de usuário e senha do Redshift para autenticar a conexão. Se o SSL estiver habilitado e for necessário no servidor, também poderá ser necessário configurar o driver para se conectar por meio do SSL. Você deve sempre fornecer seu nome de usuário e senha do Amazon Redshift para autenticar a conexão. ...

Você fornece as informações de configuração para o driver no URL de conexão. Para obter mais informações sobre a sintaxe do URL de conexão, consulte Construir o URL de conexão.

SSL indica TLS/SSL, ambos Transport Layer Security e Secure Sockets Layer. O driver suporta versões padrão do setor de TLS/SSL.

Usar somente nome de usuário e senha

Se o servidor ao qual você está se conectando não usar SSL, só será necessário fornecer seu nome de usuário e senha do Redshift para autenticar a conexão.

Como configurar a autenticação usando apenas o nome de usuário e a senha do Redshift

1. Defina a propriedade `UID` ao seu nome de usuário do Redshift para acessar o servidor do Amazon Redshift.
2. Defina a propriedade PWD como a senha correspondente ao seu nome de usuário do Redshift.

Usar SSL sem verificação de identidade

Se o servidor ao qual você está se conectando usar SSL, mas não exigir verificação de identidade, você poderá configurar o driver para usar uma fábrica SSL não validada.

Para configurar uma conexão SSL sem verificação de identidade

1. Defina a propriedade `UID` ao seu nome de usuário do Redshift para acessar o servidor do Amazon Redshift.
2. Defina a propriedade `PWD` como a senha correspondente ao seu nome de usuário do Redshift.
3. Defina a propriedade `SSLFactory` como `com.amazon.redshift.ssl.NonValidatingFactory`.

Usar autenticação SSL unidirecional

Se o servidor ao qual você está se conectando usar SSL e tiver um certificado, você poderá configurar o driver para verificar a identidade do servidor usando a autenticação unidirecional.

A autenticação unidirecional requer um certificado SSL assinado e confiável para verificar a identidade do servidor. Você pode configurar o driver para usar um certificado específico ou acessar um TrustStore que contém o certificado apropriado. Se você não especificar um certificado ou TrustStore, o driver usará o Java TrustStore padrão (normalmente `jssecacerts` ou `cacerts`).

Para configurar a autenticação SSL unidirecional

1. Defina a propriedade UID ao seu nome de usuário do Redshift para acessar o servidor do Amazon Redshift.
2. Defina a propriedade PWD como a senha correspondente ao seu nome de usuário do Redshift.
3. Defina a propriedade SSL como true.
4. Defina a propriedade SSLRootCert como o local do certificado CA raiz.
5. Se você não estiver usando um dos Java TrustStores padrão, execute uma das seguintes ações:
   - Para especificar um certificado de servidor, defina a propriedade SSLRootCert como o caminho completo do certificado.
   - Para especificar um TrustStore, faça o seguinte:
     a. Utilize o programa keytool para adicionar o certificado de servidor à TrustStore que pretende utilizar.
     b. Especifique a TrustStore e a senha a serem usadas ao iniciar a aplicação Java usando o driver. Por exemplo:

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

6. Escolha uma:
   - Para validar o certificado, defina a propriedade SSLMode como verify-ca.
   - Para validar o certificado e verificar o nome do host no certificado, defina a propriedade SSLMode como verify-full.

Configurar a autenticação do IAM

Se você estiver se conectando a um servidor do Amazon Redshift usando a autenticação do IAM, defina as propriedades a seguir como parte da cadeia de conexão da fonte de dados.

Para obter mais informações sobre a autenticação do IAM, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift.

Para usar a autenticação do IAM, use um dos seguintes formatos de string de conexão:

| String de conexão | Descrição |
| --- | --- |
| `jdbc:redshift:iam:// [host]:[port]/[db]` | Uma string de conexão regular. O driver infere o ClusterID e a região do host. |
| `jdbc:redshift:iam:// [cluster-id]: [region]/[db]` | O driver recupera informações do host, dado o ClusterID e a Região. |
| `jdbc:redshift:iam:// [host]/[db]` | O driver usa como padrão a porta 5439 e infere ClusterID e Região do host. Dependendo da porta selecionada ao criar, modificar ou migrar o cluster, permita o acesso à porta seleciona da. |

Especificar perfis

Se você estiver usando a autenticação do IAM, poderá especificar quaisquer propriedades de conexão adicionais obrigatórias ou opcionais sob um nome de perfil. Ao fazer isso, você pode evitar colocar certas informações diretamente na cadeia de conexão. Você especifica o nome do perfil na cadeia de conexão usando a propriedade Perfil.

Os perfis podem ser adicionados ao arquivo de credenciais AWS. O local padrão para esse arquivo é `~/.aws/credentials`.

Você pode alterar o valor padrão, definindo o caminho na seguinte variável de ambiente: `AWS_CREDENTIAL_PROFILES_FILE`

Para obter mais informações sobre perfis, consulte Trabalhar com credenciais da AWS no AWS SDK for Java.

Usar credenciais de perfil da instância

Se você estiver executando uma aplicação em uma instância do Amazon EC2 associada a uma função do IAM, você poderá se conectar usando as credenciais do perfil da instância.

Para fazer isso, use um dos formatos de string de conexão do IAM na tabela anterior e defina a propriedade de conexão dbuser como o nome de usuário do Amazon Redshift que você está se conectando como.

Para obter mais informações sobre perfis de instância, consulte Gerenciamento de acesso no Manual do usuário do IAM.

Usar provedores de credenciais.

O driver também oferece suporte a plugins de provedores de credenciais dos seguintes serviços:

- Serviço de Federação do Active Directory (AD FS)
- Serviço JSON Web Tokens (JWT)
- Serviço Microsoft Azure Active Directory (AD) e navegador e serviço Microsoft Azure Active Directory (AD)
- Serviço Okta
- Serviço PingFederate
- Navegador SAML para serviços SAML como Okta, Ping ou ADFS

Se você usar um desses serviços, o URL de conexão precisará especificar as seguintes propriedades:

- Plugin_Name — O caminho de classe totalmente qualificado para sua classe de plug-in do provedor de credenciais.
- IdP_Host: — O host do serviço que você está usando para autenticar no Amazon Redshift.
- IdP_Port — A porta na qual o host do serviço de autenticação escuta. Não é necessário para o Okta.
- Usuário — Nome do usuário do servidor idp_host.
- Senha — A senha associada ao nome do usuário idp_host.
- DbUser — O nome de usuário do Amazon Redshift em que você está se conectando.
- SSL_Insecure — Indica se o certificado do servidor IDP deve ser verificado.
- Client_ID — O ID do cliente associado ao nome de usuário no portal do Azure AD. Usado somente para o Azure AD.
- Client_Secret — O segredo do cliente associado ao ID do cliente no portal Azure AD. Usado somente para o Azure AD.
- IdP_Tenant — O ID de locatário do Azure AD para sua aplicação Amazon Redshift. Usado somente para o Azure AD.
- App_ID — O ID do aplicativo Okta para sua aplicação Amazon Redshift. Usado apenas para o Okta.

- App_Name — O nome da aplicação Okta opcional para sua aplicação Amazon Redshift. Usado apenas para o Okta.
- Partner_SPID — O valor SPID de parceiro opcional (ID do provedor de serviços). Usado somente para o PingFederate.

Se você estiver usando um plug-in de navegador para um desses serviços, o URL de conexão também pode incluir:

- Login_URL — O URL do recurso no site do provedor de identidades ao usar o Security Assertion Markup Language )SAML) ou os serviços do Azure AD por meio de um plug-in do navegador. Esse parâmetro é necessário se você estiver usando um plug-in do navegador.

- Listen_Port — A porta que o driver usa para obter a resposta SAML do provedor de identidades ao usar os serviços SAML ou Azure AD por meio de um plug-in de navegador.

- IdP_Response_Timeout — A quantidade de tempo, em segundos, que o driver aguarda pela resposta SAML do provedor de identidades ao usar os serviços SAML ou Azure AD por meio de um plug-in de navegador.

Para obter mais informações sobre as propriedades de string de conexão, consulte Opções para a configuração do driver JDBC versão 2.1.

Configurar o registro em log do

Você pode ativar o login no driver para ajudar no diagnóstico de problemas.

Você pode registrar as informações do driver usando os seguintes métodos:

- Para salvar informações registradas em arquivos.log, consulte Usar arquivos de log.
- Para enviar informações registradas em log para o LogStream ou LogWriter especificado no DriverManager, consulte Usar LogStream ou LogWriter.

Você fornece as informações de configuração para o driver no URL de conexão. Para obter mais informações sobre a sintaxe do URL de conexão, consulte Construir o URL de conexão.

Usar arquivos de log

Ative o registro somente por tempo suficiente para capturar um problema. O registro em log diminui a performance e pode consumir uma grande quantidade de espaço em disco.

Defina a chave LogLevel no URL de conexão para ativar o registro em logs e especifique a quantidade de detalhes incluídos nos arquivos de log. A tabela a seguir lista os níveis de registro fornecidos pelo driver JDBC versão 2.1 do Amazon Redshift, em ordem de menos detalhado para mais detalhado.

| Valor LogLevel | Descrição |
| --- | --- |
| 1 | Registre eventos de erros graves que farão com que o driver aborte. |
| 2 | Registre eventos de erro que podem permitir que o driver continue em execução. |
| 3 | Registre eventos que podem resultar em um erro se a ação não for executada. Esse nível de registro em log e os níveis de registro em log acima dele também registram as consultas do usuário. |
| 4 | Registre informações gerais que descrevem o andamento do driver. |
| 5 | Registre informações detalhadas que são úteis para depurar o driver. |
| 6 | Registre todas as atividades do driver. |

Para configurar o registro em log que usa arquivos de log

1. Defina a propriedade LogLevel para o nível desejado de informações a serem incluídas nos arquivos de log.
2. Defina a propriedade LogPath com o caminho completo para a pasta onde deseja salvar os arquivos de log.

Por exemplo, o seguinte URL de conexão habilita o nível de log 3 e salva os arquivos de log na pasta C:\temp: `jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/Default;DSILogLevel=3; LogPath=C:\temp`

3. Para garantir que as novas configurações entrem em vigor, reinicie a aplicação JDBC e reconecte-se ao servidor.

   O driver JDBC do Amazon Redshift produz os seguintes arquivos de log no local especificado na propriedade LogPath:

   - redshift_jdbc.log que registra a atividade do driver que não é específica para uma conexão.
   - Arquivo de log redshift_jdbc_connection_[Number]. para cada conexão feita com o banco de dados, onde [Number] é um número que identifica cada arquivo de log. Este arquivo registra a atividade do driver que é específica para a conexão.

Se o valor LogPath for inválido, o driver enviará as informações registradas para o fluxo de saída padrão (`System.out`)

Usar LogStream ou LogWriter

Ative o registro somente por tempo suficiente para capturar um problema. O registro em log diminui a performance e pode consumir uma grande quantidade de espaço em disco.

Defina a chave LogLevel no URL de conexão para ativar o registro em log e especifique a quantidade de detalhes enviados para o LogStream ou LogWriter especificado no DriverManager.

Para ativar o registro em log que usa o LogStream ou LogWriter:

1. Para configurar o driver para registrar informações gerais que descrevem o andamento do driver, defina a propriedade LogLevel como 1 ou INFO.
2. Para garantir que as novas configurações entrem em vigor, reinicie a aplicação JDBC e reconecte-se ao servidor.

Para desativar o registro em log que usa o LogStream ou LogWriter:

1. Remova a propriedade LogLevel do URL de conexão.
2. Para garantir que as novas configurações entrem em vigor, reinicie a aplicação JDBC e reconecte-se ao servidor.

## Conversão de tipos de dados

O driver JDBC versão 2.1 do Amazon Redshift é compatível com muitos formatos de dados comuns, convertendo entre tipos de dados do Amazon Redshift, SQL e Java.

A tabela a seguir lista os mapeamentos de tipo de dados compatíveis.

| Tipo do Amazon Redshift | Tipo SQL | Tipo Java |
|---|---|---|
| BIGINT | SQL_BIGINT | Longo |
| BOOLEAN | SQL_BIT | Booleano |
| CHAR | SQL_CHAR | String |
| DATA | SQL_TYPE_DATE | java.sql.Date |
| DECIMAL | SQL_NUMERIC | BigDecimal |
| DOUBLE PRECISION | SQL_DOUBLE | Double |
| GEOMETRY | SQL_ LONGVARBINARY | byte[] |
| INTEGER | SQL_INTEGER | Inteiro |
| OID | SQL_BIGINT | Longo |
| SUPER | SQL_LONGVARCHAR | String |
| REAL | SQL_REAL | Float |
| SMALLINT | SQL_SMALLINT | Short |
| TEXT | SQL_VARCHAR | String |
| TIME | SQL_TYPE_TIME | java.sql.Time |
| TIMETZ | SQL_TYPE_TIME | java.sql.Time |
| TIMESTAMP | SQL_TYPE_ TIMESTAMP | java.sql.Timestamp |
| TIMESTAMPTZ | SQL_TYPE_ TIMESTAMP | java.sql.Timestamp |

| Tipo do Amazon Redshift | Tipo SQL | Tipo Java |
|---|---|---|
| VARCHAR | SQL_VARCHAR | String |

Usando suporte a instruções preparadas

O driver JDBC do Amazon Redshift é compatível com instruções preparadas. Você pode usar instruções preparadas para melhorar a performance de consultas parametrizadas que precisam ser executadas várias vezes durante a mesma conexão.

Uma instrução preparada é uma instrução SQL que é compilada no lado do servidor, mas não é executada imediatamente. A instrução compilada é armazenada no servidor como um objeto PreparedStatement até que você feche o objeto ou a conexão. Enquanto esse objeto existe, você pode executar a instrução preparada tantas vezes quantas forem necessárias usando diferentes valores de parâmetro, sem ter que compilar a instrução novamente. Essa sobrecarga reduzida permite que o conjunto de consultas seja executado mais rapidamente.

Para obter mais informações sobre instruções preparadas, consulte “Usando instruções preparadas” no Tutorial básico do JDBC Basics da Oracle.

Você pode preparar uma instrução que contenha várias consultas. Por exemplo, a seguinte instrução preparada contém duas consultas INSERT:

```
PreparedStatement pstmt = conn.prepareStatement("INSERT INTO
MyTable VALUES (1, 'abc'); INSERT INTO CompanyTable VALUES
(1, 'abc');");
```

Tenha cuidado para que essas consultas não dependam dos resultados de outras consultas que são especificadas dentro da mesma instrução preparada. Como as consultas não são executadas durante a etapa de preparação, os resultados ainda não foram retornados e não estão disponíveis para outras consultas na mesma instrução preparada.

Por exemplo, a seguinte instrução preparada, que cria uma tabela e, em seguida, insere valores nessa tabela recém-criada, não é permitida:

```
PreparedStatement pstmt = conn.prepareStatement("CREATE
TABLE MyTable(col1 int, col2 varchar); INSERT INTO myTable
VALUES (1, 'abc');");
```

Se você tentar preparar essa instrução, o servidor retorna um erro informando que a tabela de destino (MyTable) ainda não existe. A consulta CREATE deve ser executada antes que a consulta INSERT possa ser preparada.

Diferenças entre as versões 2.1 e 1.x do driver JDBC

Esta seção descreve as diferenças nas informações retornadas pelas versões 2.1 e 1.x do driver JDBC. O driver JDBC versão 1.x foi descontinuado.

A tabela a seguir lista as informações DatabaseMetadata retornadas pelas funções GetDatabaseProductName() e getDatabaseProductVersion() para cada versão do driver JDBC. O driver JDBC versão 2.1 obtém os valores ao estabelecer a conexão. O driver JDBC versão 1.x obtém os valores como resultado de uma consulta.

| Versão do driver JDBC | Resultado getDatabaseProductName() | Resultado getDatabaseProductVersion() |
|---|---|---|
| 2.1 | Redshift | 8.0.2 |
| 1.x | PostgreSQL | 08.00.0002 |

A tabela a seguir lista as informações DatabaseMetadata retornadas pela função getTypeInfo para cada versão do driver JDBC.

| Versão do driver JDBC | Resultado do getTypeInfo |
|---|---|
| 2.1 | Consistente com tipos de dados do Redshift |
| 1.x | Consistente com tipos de dados do PostgreSQL |

Criar arquivos de inicialização (.ini) para o driver JDBC versão 2.1

Com os arquivos de inicialização (.ini) para o driver JDBC versão 2.1 do Amazon Redshift , você pode especificar parâmetros de configuração no nível do sistema. Por exemplo, os parâmetros de autenticação IdP federados podem variar para cada aplicação. O arquivo .ini fornece um local comum para clientes SQL obterem os parâmetros de configuração necessários.

Você pode criar um arquivo de inicialização (.ini) do driver JDBC versão 2.1 que contém opções de configuração para clientes SQL. O nome padrão do arquivo é `rsjdbc.ini`. O driver JDBC versão 2.1 verifica o arquivo.ini nos seguintes locais, listados em ordem de precedência:

- Parâmetro `IniFile` no URL de conexão ou na caixa de diálogo de propriedade de conexão do cliente SQL. Certifique-se de que o parâmetro `IniFile` contém o caminho completo para o arquivo .ini, incluindo o nome do arquivo. Para obter mais informações sobre o parâmetro `IniFile`, consulte iniFile. Se o parâmetro `IniFile` especifica incorretamente o local do arquivo.ini, um erro é exibido.
- Variáveis de ambiente como AMAZON_REDSHIFT_JDBC_INI_FILE com o caminho completo, incluindo o nome do arquivo. Você pode usar `rsjdbc.ini` ou especificar um nome de arquivo. Se a variável de ambiente AMAZON_REDSHIFT_JDBC_INI_FILE especificar incorretamente o local do arquivo.ini, um erro será exibido.
- Diretório onde o arquivo JAR do driver está localizado.
- Diretório inicial do usuário.
- Diretório temporário do sistema.

Você pode organizar o arquivo.ini em seções, por exemplo [DRIVER]. Cada seção contém pares de chave-valor que especificam vários parâmetros de conexão. Você pode usar o parâmetro `IniSection` para especificar uma seção no arquivo.ini. Para obter mais informações sobre o parâmetro `IniSection`, consulte IniSection.

Segue-se um exemplo do formato de arquivo.ini, com seções para [DRIVER], [DEV], [QA] e [PROD]. A seção [DRIVER] pode ser aplicada a qualquer conexão.

```
[DRIVER]
key1=val1
key2=val2

[DEV]
key1=val1
key2=val2

[QA]
key1=val1
key2=val2

[PROD]
```

```
key1=val1
key2=val2
```

O driver JDBC versão 2.1 carrega parâmetros de configuração dos seguintes locais, listados em ordem de precedência:

- Parâmetros de configuração padrão no código da aplicação.
- [DRIVER] do arquivo.ini, se incluído.
- Parâmetros de configuração de seção personalizada, se a `IniSection` é fornecida no URL de conexão ou na caixa de diálogo de propriedade de conexão do cliente SQL.
- Propriedades do objeto de propriedade de conexão especificado na chamada `getConnection`.
- Parâmetros de configuração especificados no URL de conexão.

### Opções para a configuração do driver JDBC versão 2.1

A seguir, você pode encontrar descrições para as opções que podem ser especificadas para a versão 2.1 do driver JDBC do Amazon Redshift. As opções não diferenciam letras maiúsculas de minúsculas.

Você pode definir propriedades de configuração usando o URL de conexão. Para obter mais informações, consulte Construir o URL de conexão.

Tópicos


- AccessKeyID
- AllowDBuserOverride
- App_ID
- App_Name
- ApplicationName
- AuthProfile
- AutoCreate
- Client_ID
- Client_Secret
- ClusterID
- Compactação

- connectTimeout
- connectionTimezone
- databaseMetadataCurrentDbOnly
- DbUser
- DbGroups
- DBNAME
- defaultRowFetchSize
- DisableIsValidQuery
- enableFetchRingBuffer
- enableMultiSqlSupport
- fetchRingBufferSize
- ForceLowercase
- groupFederation
- HOST
- IAMDisableCache
- IAMDuration
- Identity_Namespace
- IdP_Host
- IdP_Port
- IdP_Tenant
- IdP_Response_Timeout
- iniFile
- IniSection
- isServerless
- Login_URL
- loginTimeout
- loginToRp
- LogLevel
- LogPath

- OverrideSchemaPatternType
- Partner_SPID
- Senha
- Plugin_Name
- PORT
- Preferred_Role
- Perfil
- PWD
- queryGroup
- readOnly
- Região
- reWriteBatchedInserts
- reWriteBatchedInsertsSize
- roleArn
- roleSessionName
- scope
- SecretAccessKey
- SessionToken
- serverlessAcctId
- serverlessWorkGroup
- socketFactory
- socketTimeout
- SSL
- SSL_Insecure
- SSLCert
- SSLFactory
- SSLkey
- SSLMode
- SSLPassword

- SSLRootCert
- StsEndpointUrl
- tcpKeepAlive
- UID
- Usuário
- webIdentityToken

AccessKeyID

- Valor padrão: nenhum
- Tipo de dados – String

É possível especificar esse parâmetro para inserir a chave de acesso do IAM para o usuário ou o perfil. Normalmente, você pode localizar a chave observando e string existente ou perfil de usuário. Se você especificar esse parâmetro, também deverá especificar o parâmetro `SecretAccessKey`. Se for transmitido no URL de JDBC, o AccessKeyID deverá ser codificado por URL.

Esse parâmetro é opcional.

AllowDBuserOverride

- Valor padrão: 0
- Tipo de dados – String

Esta opção especifica se o driver usa o valor `DbUser` a partir da declaração SAML ou o valor especificado na propriedade de conexão `DbUser` no URL de conexão.

Esse parâmetro é opcional.

1

O driver usa o valor `DbUser` da declaração SAML.

Se a declaração SAML não especificar um valor para `DBUser`, o driver usa o valor especificado na propriedade de conexão `DBUser`. Se a propriedade de conexão também não especificar um valor, o driver usará o valor especificado no perfil de conexão.

0

O driver usa o valor `DBUser` especificado no valor de propriedade de conexão. `DBUser`.

Se a conexão `DBUser` não especificar um valor, o driver usará o valor especificado no perfil de conexão. Se o perfil de conexão também não especificar um valor, o driver usará o valor da declaração SAML.

App_ID

- Valor padrão – Nenhum
- Tipo de dados – String

O ID exclusivo fornecido pela OKTA associado à sua aplicação Amazon Redshift.

Este parâmetro é necessário se autenticar através do serviço Okta.

App_Name

- Valor padrão – Nenhum
- Tipo de dados – String

O nome da aplicação Okta que você usa para autenticar a conexão com o Amazon Redshift.

Esse parâmetro é opcional.

ApplicationName

- Valor padrão: null
- Tipo de dados: string

O nome da aplicação a ser passado ao Amazon Redshift para fins de auditoria.

Esse parâmetro é opcional.

AuthProfile

- Valor padrão – Nenhum
- Tipo de dados – String

O nome do perfil de autenticação a ser usado para conexão com o Amazon Redshift.

Esse parâmetro é opcional.

AutoCreate

- Valor padrão: false
- Tipo de dados – Booleano

Esta opção especifica se o driver faz com que um novo usuário seja criado quando o usuário especificado não existe.

Esse parâmetro é opcional.

verdadeiro

Se o usuário especificado por `DBUser` ou ID exclusivo (UID) não existir, um novo usuário com esse nome será criado.

false

O driver não faz com que novos usuários sejam criados. Se o usuário especificado não existir, a autenticação falhará.

Client_ID

- Valor padrão – Nenhum
- Tipo de dados – String

O ID do cliente a ser usado ao autenticar a conexão usando o serviço Azure AD.

Esse parâmetro é necessário se autenticar por meio do serviço Azure AD.

Client_Secret

- Valor padrão – Nenhum
- Tipo de dados – String

O Segredo do cliente a ser usado ao autenticar a conexão usando o serviço Azure AD.

Esse parâmetro é necessário se autenticar por meio do serviço Azure AD.

ClusterID

- Valor padrão – Nenhum
- Tipo de dados – String

O nome do cluster do Amazon Redshift ao qual você quer se conectar. O driver tenta detectar esse parâmetro a partir de um determinado host. Se você estiver usando um Network Load Balancer (NLB) e se conectando via IAM, o driver não conseguirá detectá-lo, por isso é possível configurá-lo usando essa opção de conexão.

Esse parâmetro é opcional.

Compactação

- Valor padrão: desativado
- Tipo de dados – String

O método de compactação usado na comunicação via protocolo com fio entre o servidor do Amazon Redshift e o cliente ou o driver.

Esse parâmetro é opcional.

Especifique os seguintes valores:

- lz4

  Define o método de compactação usado na comunicação via protocolo com fio com o Amazon Redshift como lz4.
- off

  Não usa a compactação na comunicação via protocolo com fio com o Amazon Redshift.

connectTimeout

- Valor padrão: 10
- Tipo de dados: inteiro

O valor de tempo limite a ser usado para operações de conexão de soquete. Se o tempo necessário para estabelecer uma conexão do Amazon Redshift exceder esse valor, a conexão será considerada indisponível. O tempo limite é especificado em segundos. O valor 0 significa que nenhum tempo limite foi especificado.

Esse parâmetro é opcional.

connectionTimezone

- Valor padrão: LOCAL
- Tipo de dados – String

O fuso horário no nível da sessão.

Esse parâmetro é opcional.

Especifique os seguintes valores:

LOCAL

Configura o fuso horário no nível da sessão para o fuso horário JVM LOCAL.

SERVER

Configura o fuso horário no nível da sessão de acordo com o fuso horário definido para o usuário no servidor Amazon Redshift. Você pode configurar fusos horários no nível da sessão para usuários com o seguinte comando:

```
ALTER USER
[...]
SET TIMEZONE TO [...];
```

databaseMetadataCurrentDbOnly

- Valor padrão: true
- Tipo de dados – Booleano

Esta opção especifica se a API de metadados recupera dados de todos os bancos de dados acessíveis ou somente do banco de dados conectado.

Esse parâmetro é opcional.

Especifique os seguintes valores:

verdadeiro

A aplicação recupera metadados de um único banco de dados.

false

A aplicação recupera metadados de todos os bancos de dados acessíveis.

DbUser

- Valor padrão – Nenhum
- Tipo de dados – String

O ID de usuário a ser usado com sua conta do Amazon Redshift. Você pode usar um ID que não existe no momento se você tiver habilitado a propriedade AutoCreate.

Esse parâmetro é opcional.

DbGroups

- Valor padrão – PUBLIC
- Tipo de dados – String

Uma lista separada por vírgulas de nomes de grupos de bancos de dados existentes que `DBUser` ingressa à sessão atual.

Esse parâmetro é opcional.

DBNAME

- Valor padrão: null
- Tipo de dados – String

É o nome do banco de dados ao qual se conectar. Você pode usar essa opção para especificar o nome do banco de dados na URL da conexão JDBC.

Esse parâmetro é obrigatório. Você deve especificar o nome do banco de dados, na URL da conexão ou nas propriedades de conexão da aplicação cliente.

defaultRowFetchSize

- Valor padrão: 0
- Tipo de dados — Inteiro

Esta opção especifica um valor padrão para getFetchSize.

Esse parâmetro é opcional.

Especifique os seguintes valores:

0

Obtém todas as linhas em uma única operação.

Inteiro positivo

Número de linhas a serem obtidas do banco de dados para cada iteração de busca do ResultSet.

DisableIsValidQuery

- Valor padrão – False
- Tipo de dados – Booleano

Esta opção especifica se o driver envia uma nova consulta de banco de dados ao usar o método Connection.isValid() para determinar se a conexão de banco de dados está ativa.

Esse parâmetro é opcional.

verdadeiro

O driver não envia uma consulta ao usar Connection.isValid() para determinar se a conexão de banco de dados está ativa. Isso pode fazer com que o driver identifique incorretamente a conexão de banco de dados como ativa se o servidor de banco de dados foi encerrado inesperadamente.

false

O driver envia uma consulta ao usar Connection.isValid() para determinar se a conexão de banco de dados está ativa.

enableFetchRingBuffer

- Valor padrão: true
- Tipo de dados – Booleano

Esta opção especifica que o driver obtém linhas usando um buffer de anel em um thread separado. O parâmetro fetchRingBufferSize especifica o tamanho do buffer do anel.

Se uma transação detectar uma instrução que contém vários comandos SQL separados por pontos e vírgulas, o buffer circular de busca dessa transação será definido como false. O valor de enableFetchRingBuffer não muda.

Esse parâmetro é opcional.

enableMultiSqlSupport

- Valor padrão: true
- Tipo de dados – Booleano

Esta opção especifica se deseja processar vários comandos SQL separados por ponto-e-vírgula em uma instrução.

Esse parâmetro é opcional.

Especifique os seguintes valores:

verdadeiro

O driver processa vários comandos SQL, separados por ponto-e-vírgula, em um objeto de instrução.

false

O driver retorna um erro para vários comandos SQL em uma única instrução.

fetchRingBufferSize

- Valor padrão – 1G
- Tipo de dados – String

Esta opção especifica o tamanho do buffer de anel usado ao buscar o conjunto de resultados. Você pode especificar um tamanho em bytes, por exemplo, 1K para 1 KB, 5000 para 5.000 bytes, 1M para 1 MB, 1G para 1 GB e assim por diante. Você também pode especificar uma porcentagem de memória de heap. O driver para de buscar linhas ao atingir o limite. A busca é retomada quando a aplicação lê linhas e libera espaço no buffer de anel.

Esse parâmetro é opcional.

ForceLowercase

- Valor padrão: false
- Tipo de dados – Booleano

Esta opção especifica se o driver coloca em minúsculas todos os grupos de banco de dados (DbGroups) enviados do provedor de identidades para o Amazon Redshift ao usar a autenticação única.

Esse parâmetro é opcional.

verdadeiro

O driver coloca em minúsculas todos os grupos de banco de dados que são enviados do provedor de identidades.

false

O driver não altera grupos de banco de dados.

groupFederation

- Valor padrão: false
- Tipo de dados – Booleano

Essa opção especifica se grupos de IDP do Amazon Redshift serão usados ou não. Isso é compatível com a API GetClusterCredentialsV2.

Esse parâmetro é opcional.

verdadeiro

Use grupos de provedores de identidade (IDP) do Amazon Redshift.

false

Use a API STS e GetClusterCredentials para federação de usuários e especifique explicitamente DbGroups para a conexão.

HOST

- Valor padrão: null
- Tipo de dados – String

O nome de host do servidor do Amazon Redshift ao qual se conectar. Você pode usar essa opção para especificar o nome de host na URL da conexão JDBC.

Esse parâmetro é obrigatório. Você deve especificar o nome do host, na URL da conexão ou nas propriedades de conexão da aplicação cliente.

IAMDisableCache

- Valor padrão: false
- Tipo de dados – Booleano

Essa opção especifica se as credenciais do IAM são armazenadas em cache.

Esse parâmetro é opcional.

verdadeiro

As credenciais do IAM não são armazenadas em cache.

false

As credenciais do IAM são armazenadas em cache. Isso melhora a performance quando solicitações para o API Gateway são limitadas, por exemplo.

IAMDuration

- Valor padrão – 900

- Tipo de dados — Inteiro

O período de tempo, em segundos, até que as credenciais temporárias do IAM expirem.

- Valor mínimo – 900
- Valor máximo – 3.600

Esse parâmetro é opcional.

Identity_Namespace

- Valor padrão – Nenhum
- Tipo de dados – String

O namespace da identidade a ser utilizado durante a autenticação usando IdpTokenAuthPlugin. Isso ajuda o Redshift a determinar qual instância do IAM Identity Center usar.

Se houver apenas uma instância do IAM Identity Center existente ou se o namespace da identidade padrão estiver definido, esse parâmetro será opcional; do contrário, ele será necessário.

IdP_Host

- Valor padrão – Nenhum
- Tipo de dados – String

O host IdP (provedor de identidades) que você está usando para autenticar no Amazon Redshift. Isso pode ser especificado na string de conexão ou em um perfil.

Esse parâmetro é opcional.

IdP_Port

- Valor padrão – Nenhum
- Tipo de dados – String

A porta usada por um IdP (provedor de identidades). Você pode especificar a porta na string da conexão ou em um perfil. A porta padrão é 5439. Dependendo da porta selecionada ao criar, modificar ou migrar o cluster, permita o acesso à porta selecionada.

Esse parâmetro é opcional.

IdP_Tenant

- Valor padrão – Nenhum
- Tipo de dados – String

O ID de locatário do Azure AD para sua aplicação Amazon Redshift.

Esse parâmetro é necessário se autenticar por meio do serviço Azure AD.

IdP_Response_Timeout

- Valor padrão – 120
- Tipo de dados — Inteiro

A quantidade de tempo, em segundos, que o driver aguarda pela resposta SAML do provedor de identidades ao usar os serviços SAML ou Azure AD por meio de um plug-in de navegador.

Esse parâmetro é opcional.

iniFile

- Valor padrão – Nenhum
- Tipo de dados – String

O caminho completo do arquivo .ini, incluindo o nome do arquivo. Por exemplo:

```
IniFile="C:\tools\rsjdbc.ini"
```

Para obter informações sobre o arquivo .ini, consulte Criar arquivos de inicialização (.ini) para o driver JDBC versão 2.1.

Esse parâmetro é opcional.

IniSection

- Valor padrão – Nenhum

- Tipo de dados – String

O nome de uma seção no arquivo.ini que contém as opções de configuração. Para obter informações sobre o arquivo .ini, consulte Criar arquivos de inicialização (.ini) para o driver JDBC versão 2.1.

O exemplo a seguir especifica a seção [Prod] do arquivo.ini:

```
IniSection="Prod"
```

Esse parâmetro é opcional.

isServerless

- Valor padrão: false
- Tipo de dados – Booleano

Essa opção especifica se o host do endpoint do Amazon Redshift é uma instância com tecnologia sem servidor. O driver tenta detectar esse parâmetro a partir de um determinado host. Se você estiver usando um Network Load Balancer (NLB), o driver não conseguirá detectá-lo, então é possível configurá-lo aqui.

Esse parâmetro é opcional.

verdadeiro

O host do endpoint do Amazon Redshift é uma instância com tecnologia sem servidor.

false

O host do endpoint do Amazon Redshift é um cluster provisionado.

Login_URL

- Valor padrão – Nenhum
- Tipo de dados – String

A URL do recurso no site do provedor de identidades ao usar os serviços SAML ou Azure AD por meio de um plug-in do navegador.

Esse parâmetro é necessário se autenticar com os serviços SAML ou Azure AD por meio de um plug-in de navegador.

loginTimeout

- Valor padrão: 0
- Tipo de dados — Inteiro

O número de segundos a aguardar antes de atingir o tempo limite ao conectar e autenticar no servidor. Se o tempo para estabelecer a conexão for maior do que esse limite, a conexão é cancelada.

Quando esta propriedade é definida como 0, as conexões não atingem o tempo limite.

Esse parâmetro é opcional.

loginToRp

- Valor padrão: `urn:amazon:webservices`
- Tipo de dados – String

A relação de confiança de parte confiável que você deseja usar para o tipo de autenticação do AD FS.

Esse parâmetro é opcional.

LogLevel

- Valor padrão: 0
- Tipo de dados — Inteiro

Use essa propriedade para ativar ou desativar o registro em logs no driver e especificar a quantidade de detalhes incluídos nos arquivos de log.

Habilite o registro em log somente o tempo suficiente para capturar um problema. O registro em log diminui a performance e pode consumir uma grande quantidade de espaço em disco.

Esse parâmetro é opcional.

Defina o parâmetro com um dos seguintes valores:

0

Desative todos os registros em log.

1

Habilita o registro em logs no nível FATAL, que registra eventos de erro muito graves que levarão o driver a anular.

2

Habilita o registro em logs no nível ERROR, que registra eventos de erro que ainda permitem que o driver continue sendo executado.

3

Habilite o log no nível WARNING, que registra eventos que podem resultar em um erro se a ação não for executada.

4

Habilita o registro em logs no nível INFO, que registra informações gerais que descrevem o progresso do driver.

5

Habilita o registro em logs no nível DEBUG, que registra informações detalhadas que sejam úteis para depurar o driver.

6

Habilita o registro em log no nível TRACE, que registra todas as atividades do driver.

Quando o registro em log está habilitado, o driver produz os seguintes arquivos de log no local especificado na propriedade `LogPath`:

- **`redshift_jdbc.log`** — Arquivo que registra a atividade do driver que não é específica para uma conexão.
- **`redshift_jdbc_connection_[Number].log`** — Arquivo para cada conexão feita com o banco de dados, onde `[Number]` é um número que distingue cada arquivo de log dos outros. Este arquivo registra a atividade do driver que é específica para a conexão.

Se o valor LogPath for inválido, o driver envia as informações registradas para o fluxo de saída padrão, `System.out`.

LogPath

- Valor padrão – O diretório de trabalho atual.
- Tipo de dados – String

O caminho completo para a pasta onde o driver salva arquivos de log quando a propriedade DSILogLevel está habilitada.

Para ter certeza de que o URL de conexão é compatível com todas as aplicações JDBC, recomendamos que você escape as barras invertidas (\) no caminho do arquivo digitando outra barra invertida.

Esse parâmetro é opcional.

OverrideSchemaPatternType

- Valor padrão: null
- Tipo de dados: inteiro

Esta opção especifica se o tipo de consulta usado em chamadas de getTables deve ser substituído.

0

Nenhuma consulta universal de esquema

1

Consulta de esquema local

2

Consulta de esquema externo

Esse parâmetro é opcional.

Partner_SPID

- Valor padrão – Nenhum

- Tipo de dados – String

O valor SPID (ID do provedor de serviços) do parceiro a ser usado ao autenticar a conexão usando o serviço PingFederate.

Esse parâmetro é opcional.

Senha

- Valor padrão – Nenhum
- Tipo de dados – String

Ao se conectar usando a autenticação do IAM por meio de um IDP, essa é a senha do servidor IDP_Host. Ao usar a autenticação padrão, isso pode ser usado para a senha do banco de dados do Amazon Redshift em vez de PWD.

Esse parâmetro é opcional.

Plugin_Name

- Valor padrão – Nenhum
- Tipo de dados – String

O nome de classe totalmente qualificado para implementar um plugin de provedor de credenciais específico.

Esse parâmetro é opcional.

Algumas opções compatíveis estão listadas:

- **`AdfsCredentialsProvider`**: Serviço de Federação do Active Directory.
- **`AzureCredentialsProvider`**: Serviço Microsoft Azure Active Directory (AD).
- **`BasicJwtCredentialsProvider`**: Serviço JSON Web Tokens (JWT)
- **`BasicSamlCredentialsProvider`**: credenciais de Security Assertion Markup Language (SAML) que você pode usar com muitos provedores de serviços SAML.
- **`BrowserAzureCredentialsProvider`**: navegador do Serviço Microsoft Azure Active Directory (AD).

- **`BrowserAzureOAuth2CredentialsProvider`**: navegador do Serviço Microsoft Azure Active Directory (AD) para autenticação nativa.
- **`BrowserSamlCredentialsProvider`**: navegador SAML para serviços SAML como Okta, Ping ou ADFS.
- **`IdpTokenAuthPlugin`**: um plug-in de autorização que aceita um token do centro de identidade (IdC) ou tokens de identidade baseados em JSON (JWT) do OpenID Connect (OIDC) de qualquer provedor de identidades da web vinculado ao IdC.
- **`OktaCredentialsProvider`**: serviço do Okta.
- **`PingCredentialsProvider`**: serviço do PingFederate.

PORT

- Valor padrão: null
- Tipo de dados: inteiro

A porta do servidor do Amazon Redshift ao qual se conectar. Você pode usar essa opção para especificar a porta na URL da conexão JDBC.

Esse parâmetro é opcional.

Preferred_Role

- Valor padrão – Nenhum
- Tipo de dados – String

A função do IAM que você deseja assumir durante a conexão com o Amazon Redshift.

Esse parâmetro é opcional.

Perfil

- Valor padrão – Nenhum
- Tipo de dados – String

O nome do perfil a ser usado para autenticação do IAM. Este perfil contém quaisquer propriedades de conexão adicionais não especificadas na cadeia de conexão.

Esse parâmetro é opcional.

PWD

- Valor padrão – Nenhum
- Tipo de dados – String

A senha correspondente ao nome de usuário do Amazon Redshift que você forneceu usando o UID da propriedade.

Esse parâmetro é opcional.

queryGroup

- Valor padrão: null
- Tipo de dados – String

Esta opção atribui uma consulta a uma fila em tempo de execução atribuindo sua consulta ao grupo de consulta apropriado. O grupo de consulta está definido para a sessão. Todas as consultas que são executadas na conexão pertencem a esse grupo de consultas.

Esse parâmetro é opcional.

readOnly

- Valor padrão: false
- Tipo de dados – Booleano

Essa propriedade especifica se o driver está em modo somente leitura.

Esse parâmetro é opcional.

verdadeiro

A conexão está no modo somente leitura e não pode gravar no armazenamento de dados.

false

A conexão não está no modo somente leitura e pode gravar no armazenamento de dados.

Região

- Valor padrão: null
- Tipo de dados – String

Esta opção especifica a opção da região da AWS em que o cluster está localizado. Se você especificar a opção StsEndPoint, a opção Região será ignorada. A operação de API `GetClusterCredentials` do Redshift também usa a opção Região.

Esse parâmetro é opcional.

reWriteBatchedInserts

- Valor padrão: false
- Tipo de dados – Booleano

Esta opção permite a otimização para reescrever e combinar instruções INSERT compatíveis em lotes.

Esse parâmetro é opcional.

reWriteBatchedInsertsSize

- Valor padrão – 128
- Tipo de dados — Inteiro

Esta opção permite a otimização para reescrever e combinar instruções INSERT compatíveis em lotes. Este valor deve aumentar exponencialmente na potência de 2.

Esse parâmetro é opcional.

roleArn

- Valor padrão – Nenhum
- Tipo de dados – String

O nome do recurso da Amazon (ARN) da função. Certifique-se de especificar esse parâmetro ao especificar BasicJwtCredentialsProvider para a opção Plugin_Name. Especifique o ARN no seguinte formato:

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

Esse parâmetro será necessário se você especificar BasicJwtCredentialsProvider para a opção Plugin_Name.

roleSessionName

- Valor padrão: jwt_redshift_session
- Tipo de dados – String

Um identificador para a sessão de função assumida. Normalmente, você passa o nome ou identificador que está associado ao usuário da aplicação. As credenciais de segurança temporárias que o aplicativo usa estão associadas a esse usuário. É possível especificar esse parâmetro quando você especificar BasicJwtCredentialsProvider para a opção Plugin_Name.

Esse parâmetro é opcional.

scope

- Valor padrão – Nenhum
- Tipo de dados – String

Uma lista separada por espaços de escopos com os quais o usuário pode consentir. Você especifica esse parâmetro para que sua aplicação do Microsoft Azure possa obter consentimento para APIs que você deseja chamar. É possível especificar esse parâmetro ao especificar BrowserAzureOAuth2CredentialsProvider para a opção Plugin_Name.

Esse parâmetro é obrigatório para o plug-in BrowserAzureOAuth2CredentialsProvider.

SecretAccessKey

- Valor padrão – Nenhum
- Tipo de dados – String

A chave de acesso do IAM para o usuário ou função. Se for especificado, AccessKeyID também deve ser especificado. Se for transmitido no URL de JDBC, o SecretAccessKey deverá ser codificado por URL.

Esse parâmetro é opcional.

SessionToken

- Valor padrão – Nenhum
- Tipo de dados – String

O token temporário de sessão do IAM associado à função do IAM que você está usando para autenticar. Se for passado no URL de JDBC, o token de sessão temporário do IAM deverá ser codificado por URL.

Esse parâmetro é opcional.

serverlessAcctId

- Valor padrão: null
- Tipo de dados – String

O ID da conta do Amazon Redshift Serverless. O driver tenta detectar esse parâmetro a partir de um determinado host. Se você estiver usando um Network Load Balancer (NLB), o driver não conseguirá detectá-lo, então é possível configurá-lo aqui.

Esse parâmetro é opcional.

serverlessWorkGroup

- Valor padrão: null
- Tipo de dados – String

O nome do grupo de trabalho do Amazon Redshift Serverless. O driver tenta detectar esse parâmetro a partir de um determinado host. Se você estiver usando um Network Load Balancer (NLB), o driver não conseguirá detectá-lo, então é possível configurá-lo aqui.

Esse parâmetro é opcional.

socketFactory

- Valor padrão: null
- Tipo de dados – String

Esta opção especifica uma fábrica de soquetes para criação de soquetes.

Esse parâmetro é opcional.

socketTimeout

- Valor padrão: 0
- Tipo de dados — Inteiro

O número de segundos de espera nas operações de leitura de um soquete antes de se atingir o tempo limite. Se a operação demorar mais do que esse limite, a conexão será fechada. Quando esta propriedade é definida como 0, a conexão não atinge o tempo limite.

Esse parâmetro é opcional.

SSL

- Valor padrão: TRUE
- Tipo de dados – String

Use esta propriedade para ativar ou desativar o SSL para a conexão.

Esse parâmetro é opcional.

Especifique os seguintes valores:

VERDADEIRO

O driver se conecta ao servidor por meio de SSL.

FALSE

O driver se conecta ao servidor sem usar SSL. Essa opção não é compatível com a autenticação do IAM.

Você também pode configurar a propriedade AuthMech.

SSL_Insecure

- Valor padrão – true
- Tipo de dados – String

Esta propriedade indica se o certificado de servidor de hosts IDP deve ser verificado.

Esse parâmetro é opcional.

Especifique os seguintes valores:

verdadeiro

O driver não verifica a autenticidade do certificado do servidor IDP.

false

O driver verifica a autenticidade do certificado do servidor IDP.

SSLCert

- Valor padrão – Nenhum
- Tipo de dados – String

O caminho completo de um arquivo .pem ou .crt que contém certificados CA confiáveis adicionais para verificar a instância do servidor Amazon Redshift do quando o SSL for usado.

Este parâmetro é necessário se SSLKey for especificado.

SSLFactory

- Valor padrão – Nenhum
- Tipo de dados – String

A fábrica SSL a ser usada ao se conectar ao servidor por meio de TLS/SSL sem usar um certificado de servidor.

SSLkey

- Valor padrão – Nenhum
- Tipo de dados – String

O caminho completo do arquivo .der que contém o arquivo de chave PKCS8 para verificar os certificados especificados em SSLCert.

Este parâmetro é necessário se SSLCert for especificado.

SSLMode

- Valor padrão – verify-ca
- Tipo de dados – String

Use essa propriedade para especificar como o driver valida certificados quando TLS/SSL está habilitado.

Esse parâmetro é opcional.

Especifique os seguintes valores:

verify-ca

O driver verifica se o certificado vem de uma autoridade de certificação (CA) confiável.

verify-full

O controlador verifica se o certificado vem de uma AC fidedigna e se o nome de host no certificado corresponde ao nome de host especificado na URL de ligação.

SSLPassword

- Valor padrão: 0
- Tipo de dados – String

A senha para o arquivo de chave criptografada especificado em SSLKey.

Esse parâmetro é necessário se SSLKey for especificado e o arquivo de chave for criptografado.

SSLRootCert

- Valor padrão – Nenhum
- Tipo de dados – String

O caminho completo de um arquivo .pem ou .crt que contém o certificado CA raiz que verificará a instância do Amazon Redshift Server do quando o SSL for usado.

StsEndpointUrl

- Valor padrão: null
- Tipo de dados – String

É possível especificar um endpoint AWS Security Token Service (AWS STS). Se você especificar essa opção, a opção Região será ignorada. Você só pode especificar um protocolo seguro (HTTPS) para esse endpoint.

tcpKeepAlive

- Valor padrão: TRUE
- Tipo de dados – String

Use essa propriedade para ativar ou desativar keepalives TCP.

Esse parâmetro é opcional.

Especifique os seguintes valores:

VERDADEIRO

O driver usa keepalives TCP para evitar que o tempo limite das conexões se esgote.

FALSE

O driver não usa keepalives TCP.

UID

- Valor padrão – Nenhum

- Tipo de dados – String

O nome de usuário do banco de dados que você usa para acessar o banco de dados.

Esse parâmetro é obrigatório.

Usuário

- Valor padrão – Nenhum
- Tipo de dados – String

Ao se conectar usando a autenticação do IAM por meio de um IDP, esse é o nome de usuário do servidor idp_host. Ao usar a autenticação padrão, isso pode ser usado para o nome de usuário do banco de dados do Amazon Redshift.

Esse parâmetro é opcional.

webIdentityToken

- Valor padrão – Nenhum
- Tipo de dados – String

O token de acesso OAuth 2.1 ou token OpenID Connect ID fornecido pelo provedor de identidades. Sua aplicação deve obter esse token autenticando o usuário da sua aplicação com um provedor de identidades da web. Certifique-se de especificar esse parâmetro ao especificar BasicJwtCredentialsProvider para a opção Plugin_Name.

Esse parâmetro será necessário se você especificar BasicJwtCredentialsProvider para a opção Plugin_Name.

Versões anteriores do driver JDBC versão 2.1

Baixe uma versão anterior do driver JDBC versão 2.1 do Amazon Redshift somente se sua ferramenta exigir uma versão específica do driver.

Estes são os drivers anteriores da versão 2.1 do driver JDBC compatíveis com JDBC 4.2:

- 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

## Configurar o conector Python do Amazon Redshift

Ao usar o conector Amazon Redshift para Python, é possível integrar o trabalho com o AWS SDK para Python (Boto3) e também pandas e Python numéricos (NumPy). Para obter mais informações, consulte o repositório de pandas no GitHub. Para obter mais informações sobre o NumPy, consulte o repositório do NumPy no GitHub.

O conector Python do Amazon Redshift oferece uma solução de código aberto. É possível navegar pelo código-fonte, solicitar aprimoramentos, relatar problemas e fornecer contribuições.

Para usar o conector Python do Amazon Redshift, verifique se tem o Python versão 3.6 ou posterior. Para obter mais informações, consulte o Contrato de licença do driver do Amazon Redshift Python.

O conector Python do Amazon Redshift oferece:

- Autenticação do AWS Identity and Access Management (IAM). Para obter mais informações, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift.

- Autenticação do provedor de identidade usando acesso à API federada. O acesso à API federada é compatível com provedores de identidade corporativa, tais como:
  - Azure AD. Para obter mais informações, consulte a publicação no blog AWS Big Data Federate Amazon Redshift access with Microsoft Azure AD single sign-on.
  - Serviços de Federação do Active Directory. Para obter mais informações, consulte a publicação no blog AWS Big Data Federate access to your Amazon Redshift cluster with Active Directory Federation Services (AD FS): Part 1.
  - Okta. Para obter mais informações, consulte a publicação no blog AWS Big Data Federate Amazon Redshift access with Okta as an identity provider.
  - PingFederate. Para obter mais informações, consulte o site do PingFederate.
  - JumpCloud. Para obter mais informações, consulte o site do JumpCloud.
- Tipo de dados do Amazon Redshift.

O conector Python do Amazon Redshift implementa o Python Database API Specification 2.0. Para obter mais informações, consulte PEP 249—Python Database API Specification v2.0 no site da Python.

Tópicos


- Instalar o conector Python do Amazon Redshift
- Opções de configuração para o conector Python do Amazon Redshift
- Importar o conector Python
- Integrar o conector Python ao NumPy
- Integrar o conector Python a pandas
- Usar plugins do provedor de identidade
- Exemplos de uso do conector Python do Amazon Redshift
- Referência de API para o conector Python do Amazon Redshift


## Instalar o conector Python do Amazon Redshift

Utilize qualquer um dos métodos a seguir para instalar o conector Python do Amazon Redshift:

- Python Package Index (PyPI)
- Conda
- Clonar o repositório do GitHub

Instalar o conector Python pelo PyPI

Para instalar o conector Python so Python Package Index (PyPI), você pode usar o pip. Para fazer isso, execute o comando a seguir.

```
>>> pip install redshift_connector
```

É possível instalar o conector em um ambiente virtual. Para fazer isso, execute o comando a seguir.

```
>>> pip install redshift_connector
```

Opcionalmente, você pode instalar pandas e NumPy com o conector.

```
>>> pip install "redshift_connector[full]"
```

Para obter mais informações sobre o pip, consulte o site do pip.

Instalar o conector Python pelo Conda

Você pode instalar o conector Python pelo Anaconda.org.

```
>>>conda install -c conda-forge redshift_connector
```

Instalar o conector Python clonando o repositório GitHub da AWS

Para instalar o conector Python a partir da origem, clone o repositório GitHub da AWS. Depois de instalar o Python e o virtualenv, configure o ambiente e instale as dependências necessárias executando os comandos a seguir.

```
$ 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
```

Opções de configuração para o conector Python do Amazon Redshift

A seguir, você encontra descrições para as opções que podem ser especificadas para conector Python do Amazon Redshift.

access_key_id

- Valor padrão: nenhum
- Tipo de dados: string

O ID de chave de acesso da função do IAM ou o usuário do IAM configurado para autenticação do banco de dados do IAM.

Esse parâmetro é opcional.

allow_db_user_override

- Valor padrão: false
- Tipo de dados: booliano

Verdadeiro

Especifica que o conector usa o valor `DbUser` da declaração Security Assertion Markup Language (SAML).

Falso

Especifica que o valor no parâmetro de conexão `DbUser` é usado.

Esse parâmetro é opcional.

app_name

- Valor padrão: nenhum
- Tipo de dados: string

O nome da aplicação do provedor de identidade (IdP) usado para autenticação.

Esse parâmetro é opcional.

auth_profile

- Valor padrão: nenhum
- Tipo de dados: string

O nome de um perfil de autenticação do Amazon Redshift com propriedades de conexão como JSON. Para obter mais informações sobre como nomear parâmetros de conexão, consulte a classe `RedshiftProperty`. A classe `RedshiftProperty` armazena parâmetros de conexão fornecidos pelo usuário final e, se aplicável, gerados durante o processo de autenticação do IAM (por exemplo, credenciais temporárias do IAM). Para obter mais informações, consulte a classe RedShiftProperty.

Esse parâmetro é opcional.

auto_create

- Valor padrão: false
- Tipo de dados: booliano

Um valor que indica se é necessário criar o usuário, caso o usuário não exista.

Esse parâmetro é opcional.

client_id

- Valor padrão: nenhum
- Tipo de dados: string

O ID do cliente do Azure IdP.

Esse parâmetro é opcional.

client_secret

- Valor padrão: nenhum
- Tipo de dados: string

O segredo do cliente do Azure IdP.

Esse parâmetro é opcional.

cluster_identifier

- Valor padrão: nenhum
- Tipo de dados: string

O identificador de clusters do cluster do Amazon Redshift.

Esse parâmetro é opcional.

credentials_provider

- Valor padrão: nenhum
- Tipo de dados: string

O IdP usado para autenticação com o Amazon Redshift. Estes são valores válidos:

- `AdfsCredentialsProvider`
- `AzureCredentialsProvider`
- `BrowserAzureCredentialsProvider`
- `BrowserSamlCredentialsProvider`
- `IdpTokenAuthPlugin`: um plug-in de autorização que aceita um token do centro de identidade (IdC) ou tokens de identidade baseados em JSON (JWT) do OpenID Connect (OIDC) de qualquer provedor de identidades da web vinculado ao IdC.
- `PingCredentialsProvider`
- `OktaCredentialsProvider`

Esse parâmetro é opcional.

banco de dados

- Valor padrão: nenhum
- Tipo de dados: string

O nome do banco de dados ao qual deseja se conectar.

Esse parâmetro é opcional.

database_metadata_current_db_only

- Valor padrão: true
- Tipo de dados: booliano

Um valor que indica se uma aplicação oferece suporte a catálogos de unidades de compartilhamento de dados de vários bancos de dados. O valor padrão True indica que a aplicação não oferece suporte a catálogos de unidades de compartilhamento de dados de vários bancos de dados para compatibilidade com versões anteriores.

Esse parâmetro é opcional.

db_groups

- Valor padrão: nenhum
- Tipo de dados: string

Uma lista separada por vírgulas de nomes de grupos de bancos de dados existentes que o usuário indicou pelo DbUser ingressa à sessão atual.

Esse parâmetro é opcional.

db_user

- Valor padrão: nenhum
- Tipo de dados: string

O ID de usuário a ser usado com o Amazon Redshift.

Esse parâmetro é opcional.

endpoint_url

- Valor padrão: nenhum
- Tipo de dados: string

A URL do endpoint do Amazon Redshift. Essa opção é apenas para uso interno da AWS.

Esse parâmetro é obrigatório.

group_federation

- Valor padrão: false
- Tipo de dados: booliano

Essa opção especifica se grupos de IDP do Amazon Redshift serão usados ou não.

Esse parâmetro é opcional.

verdadeiro

Use grupos de provedores de identidade (IDP) do Amazon Redshift.

false

Use a API STS e GetClusterCredentials para federação de usuários e especifique explicitamente os db_groups para a conexão.

host

- Valor padrão: nenhum
- Tipo de dados: string

O nome de host do cluster do Amazon Redshift.

Esse parâmetro é opcional.

iam

- Valor padrão: false
- Tipo de dados: booliano

A autenticação do IAM está habilitada.

Esse parâmetro é obrigatório.

iam_disable_cache

- Valor padrão: false
- Tipo de dados: booliano

Essa opção especifica se as credenciais do IAM são armazenadas em cache. Por padrão, as credenciais do IAM são armazenadas em cache. Isso melhora a performance quando solicitações para o API Gateway têm controle de utilização.

Esse parâmetro é opcional.

identity_namespace

- Valor padrão: null
- Tipo de dados: string

O namespace da identidade a ser utilizado durante a autenticação usando IdpTokenAuthPlugin. Isso ajuda o Redshift a determinar qual instância do centro de identidade usar.

Se houver apenas uma instância do centro de identidade existente ou se o namespace da identidade padrão estiver definido, esse parâmetro será opcional. Caso contrário, ele será obrigatório.

idpPort

- Valor padrão: 7890
- Tipo de dados: inteiro

A porta de escuta para a qual o IdP envia a declaração SAML.

Esse parâmetro é obrigatório.

idp_response_timeout

- Valor padrão: 120
- Tipo de dados: inteiro

O tempo limite para recuperar a declaração SAML do IdP.

Esse parâmetro é obrigatório.

idp_tenant

- Valor padrão: nenhum
- Tipo de dados: string

O IdP locatário.

Esse parâmetro é opcional.

listen_port

- Valor padrão: 7890
- Tipo de dados: inteiro

A porta de escuta para a qual o IdP envia a declaração SAML.

Esse parâmetro é opcional.

login_url

- Valor padrão: nenhum
- Tipo de dados: string

O URL de autenticação única para o IdP.

Esse parâmetro é opcional.

max_prepared_statations

- Valor padrão: 1000
- Tipo de dados: inteiro

O número máximo de instruções preparadas que podem ser abertas simultaneamente.

Esse parâmetro é obrigatório.

numeric_to_float

- Valor padrão: false
- Tipo de dados: booliano

Essa opção especifica se o conector converte valores do tipo dados numéricos de decimal.Decimal para float. Por padrão, o conector recebe valores do tipo dados numéricos como decimal.Decimal e não os converte.

Não recomendamos habilitar numeric_to_float para casos de uso que exigem precisão, pois os resultados podem ser arredondados.

Para obter mais informações sobre decimal.Decimal e as compensações entre ele e float, consulte decimal — Aritmética de ponto fixo decimal e ponto flutuante no site do Python.

Esse parâmetro é opcional.

partner_sp_id

- Valor padrão: nenhum
- Tipo de dados: string

O ID do Partner SP usado para autenticação com Ping.

Esse parâmetro é opcional.

password

- Valor padrão: nenhum
- Tipo de dados: string

A senha a ser usada para autenticação.

Esse parâmetro é opcional.

porta

- Valor padrão: 5439
- Tipo de dados: inteiro

O número da porta do cluster Amazon Redshift.

Esse parâmetro é obrigatório.

preferred_role

- Valor padrão: nenhum
- Tipo de dados: string

A função do IAM preferencial para a conexão atual.

Esse parâmetro é opcional.

principal_arn

- Valor padrão: nenhum
- Tipo de dados: string

O nome do recurso da Amazon (ARN) do usuário ou perfil do IAM para o qual você está gerando uma política. É recomendável anexar uma política a um perfil e, depois, anexar o perfil ao usuário, para acesso.

Esse parâmetro é opcional.

profile

- Valor padrão: nenhum
- Tipo de dados: string

O nome de um perfil em um arquivo de credenciais da AWS que contém credenciais da AWS.

Esse parâmetro é opcional.

provider_name

- Valor padrão: nenhum
- Tipo de dados: string

O nome do provedor de autenticação nativa do Redshift.

Esse parâmetro é opcional.

região

- Valor padrão: nenhum
- Tipo de dados: string

A Região da AWS onde o cluster está localizado.

Esse parâmetro é opcional.

role_arn

- Valor padrão: nenhum
- Tipo de dados: string

O nome do recurso da Amazon (ARN) da função que o autor da chamada deve assumir. Esse parâmetro é usado pelo provedor indicado por `JwtCredentialsProvider`.

Para o provedor `JwtCredentialsProvider`, esse parâmetro é obrigatório. Senão, esse parâmetro é opcional.

role_session_name

- Valor padrão: jwt_redshift_session
- Tipo de dados: string

Um identificador para a sessão de função assumida. Normalmente, você passa o nome ou identificador que está associado ao usuário que está usando a aplicação. As credenciais de segurança temporárias que o aplicativo usa estão associadas a esse usuário. Esse parâmetro é usado pelo provedor indicado por `JwtCredentialsProvider`.

Esse parâmetro é opcional.

scope

- Valor padrão: nenhum
- Tipo de dados: string

Uma lista separada por espaços de escopos com os quais o usuário pode consentir. Você especifica esse parâmetro para que sua aplicação possa obter consentimento para APIs que você deseja chamar. É possível especificar esse parâmetro ao especificar BrowserAzureOAuth2CredentialsProvider para a opção Plugin_Name.

Esse parâmetro é obrigatório para o plug-in BrowserAzureOAuth2CredentialsProvider.

secret_access_key_id

- Valor padrão: nenhum
- Tipo de dados: string

A chave de acesso secreta da função do IAM ou o usuário configurado para autenticação do banco de dados do IAM.

Esse parâmetro é opcional.

session_token

- Valor padrão: nenhum
- Tipo de dados: string

O ID de chave de acesso da função do IAM ou o usuário do IAM configurado para autenticação do banco de dados do IAM. Esse parâmetro será necessário se as credenciais temporárias da AWS estiverem em uso.

Esse parâmetro é opcional.

serverless_acct_id

- Valor padrão: nenhum
- Tipo de dados: string

O ID da conta do Amazon Redshift Serverless.

Esse parâmetro é opcional.

serverless_work_group

- Valor padrão: nenhum
- Tipo de dados: string

O nome do grupo de trabalho do Amazon Redshift Serverless.

Esse parâmetro é opcional.

ssl

- Valor padrão: true
- Tipo de dados: booliano

O Secure Sockets Layer (SSL) está habilitado.

Esse parâmetro é obrigatório.

ssl_insecure

- Valor padrão: true
- Tipo de dados: booliano

Um valor que especifica se o certificado do servidor dos hosts IdP deve ser verificado.

Esse parâmetro é opcional.

sslmode

- Valor padrão: verify-ca
- Tipo de dados: string

A segurança da conexão com o Amazon Redshift. Você pode especificar qualquer um destes valores:

- verify-ca
- verify-full

Esse parâmetro é obrigatório.

timeout

- Valor padrão: nenhum
- Tipo de dados: inteiro

O número de segundos antes de a conexão com o servidor atingir o tempo limite.

Esse parâmetro é opcional.

token

- Valor padrão: null

- Tipo de dados: string

O centro de identidade (IdC) forneceu um token de acesso ou um token de identidade baseado em JSON (JWT) do OpenID Connect (OIDC) fornecido por um provedor de identidades da web vinculado ao IdC. Sua aplicação deve gerar esse token autenticando o usuário da sua aplicação com o IdC ou um provedor de identidades da web vinculado ao IdC.

Esse parâmetro só é necessário durante a autenticação usando IdpTokenAuthPlugin.

token_type

- Valor padrão: null
- Tipo de dados: string

O tipo de token que está sendo usado no IdpTokenAuthPlugin.

Esse parâmetro só é necessário durante a autenticação usando IdpTokenAuthPlugin.

Especifique os seguintes valores:

- `ACCESS_TOKEN`: especifique esse valor se você estiver usando um token de acesso fornecido pelo centro de identidade (IdC).
- `EXT_JWT`: especifique esse valor se você estiver usando um token de identidade baseado em JSON (JWT) do OpenID Connect (OIDC) fornecido por um provedor de identidades da web externo que está vinculado ao IdC.

usuário

- Valor padrão: nenhum
- Tipo de dados: string

O nome do usuário a ser usado para autorização.

Esse parâmetro é opcional.

web_identity_token

- Valor padrão: nenhum

- Tipo de dados: string

O token de acesso OAuth 2.0 ou token OpenID Connect ID fornecido pelo provedor de identidade. Verifique se sua aplicação obtém esse token autenticando o usuário que está usando a aplicação com um provedor de identidade da Web. O provedor indicado por `JwtCredentialsProvider` usa este parâmetro.

Para o provedor `JwtCredentialsProvider`, esse parâmetro é obrigatório. Senão, esse parâmetro é opcional.

Importar o conector Python

Para importar o conector Python, execute o comando a seguir.

```
>>> import redshift_connector
```

Importar NumPy e conectar-se ao Amazon Redshift

Para importar o conector Python do Amazon Redshift e o Python numérico (NumPy), execute os comandos a seguir.

```
import redshift_connector
import numpy
```

Para se conectar a um cluster do Amazon Redshift usando credenciais da AWS, execute o comando a seguir.

```
conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
 )
```

Integrar o conector Python ao NumPy

A seguir, veja um exemplo de integração do conector Python ao 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)
```

Veja os resultados a seguir.

```
[['One Hundred Years of Solitude' 'Gabriel García Márquez']
['A Brief History of Time' 'Stephen Hawking']]
```

Integrar o conector Python a pandas

A seguir, veja um exemplo de integração do conector Python a pandas.

```
>>> import pandas

#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
     host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
     port=5439,
     database='dev',
     user='awsuser',
     password='my_password'
  )

# Create a Cursor object
>>> cursor = conn.cursor()
```

```
# Query and receive result set
cursor.execute("select * from book")
result: pandas.DataFrame = cursor.fetch_dataframe()
print(result)
```

Usar plugins do provedor de identidade

Para obter informações gerais sobre como usar plugins do provedor de identidade, consulte Opções para fornecer credenciais do IAM. Para obter mais informações sobre o gerenciamento de identidades do IAM, incluindo práticas recomendadas para perfis do IAM, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift.

Autenticação com o plugin do provedor de identidade ADFS

Veja a seguir um exemplo de uso do plugin do provedor de identidade do Serviço de Federação do Active Directory (ADFS) para autenticar um usuário que se conecta a um banco de dados do 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'
)
```

Autenticação com o plugin do provedor de identidade do Azure

Veja a seguir um exemplo de autenticação com o plugin do provedor de identidade do Azure. Você pode criar valores para um `client_id` e `client_secret` para uma aplicação Azure Enterprise, conforme mostrado a seguir.

```
>>>  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'
)
```

Autenticação com o plugin do provedor de identidade do Azure Browser

Veja a seguir um exemplo de uso do plugin do provedor de identidade do Azure Browser para autenticar um usuário que se conecta a um banco de dados do Amazon Redshift.

A autenticação multifator ocorre no navegador, no qual as credenciais de login são fornecidas pelo usuário.

```
>>>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',
)
```

Autenticação com o plugin do provedor de identidade Okta

Veja a seguir um exemplo de autenticação com o plugin do provedor de identidade do Okta. Você pode obter os valores para `idp_host`, `app_id` e `app_name` pela aplicação 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'
)
```

Autenticação com JumpCloud com um plugin genérico de provedor de identidade de navegador SAML

Veja a seguir um exemplo de uso do JumpCloud com um plugin genérico de provedor de identidade de navegador SAML para autenticação.

O parâmetro password é obrigatório. Porém, não é necessário inserir esse parâmetro, pois a autenticação multifator ocorre no navegador.

```
>>> 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'
)
```

Exemplos de uso do conector Python do Amazon Redshift

Veja a seguir exemplos de como usar o conector Python do Amazon Redshift. Para executá-los, primeiro instale o conector Python. Para obter mais informações sobre a instalação do conector Python do Amazon Redshift, consulte Instalar o conector Python do Amazon Redshift. Para obter mais informações sobre as opções de configuração que você pode usar com o conector Python, consulte Opções de configuração para o conector Python do Amazon Redshift.

Tópicos

- Conectar-se a um cluster do Amazon Redshift e consultá-lo usando credenciais da AWS
- Habilitar o autocommit
- Configurar o estilo de parâmetro do cursor
- Usar COPY para copiar dados de um bucket do Amazon S3 e UNLOAD para gravar dados nele

Conectar-se a um cluster do Amazon Redshift e consultá-lo usando credenciais da AWS

O exemplo a seguir mostra como você se conecta com um cluster do Amazon Redshift usando credenciais da AWS, consulta uma tabela e recupera os resultados da consulta.

```
#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'])
```

Habilitar o autocommit

A propriedade autocommit é desativada por padrão, conforme a Python Database API Specification. Use os comandos a seguir para ativar a propriedade autocommit da conexão depois de executar um comando de reversão para garantir que uma transação não esteja em andamento.

```
#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
```

Configurar o estilo de parâmetro do cursor

O estilo de parâmetro de um cursor pode ser modificado por meio de cursor.paramstyle. O estilo de parâmetro padrão usado é `format`. Os valores válidos para o estilo de parâmetro são `qmark`, `numeric`, `named`, `format` e `pyformat`.

Veja a seguir exemplos do uso de vários estilos de parâmetros para transmitir parâmetros para um exemplo de instrução SQL.

```
# qmark
redshift_connector.paramstyle = 'qmark'
sql = 'insert into foo(bar, jar) VALUES(?, ?)'
cursor.execute(sql, (1, "hello world"))

# numeric
redshift_connector.paramstyle = 'numeric'
sql = 'insert into foo(bar, jar) VALUES(:1, :2)'
cursor.execute(sql, (1, "hello world"))

# named
redshift_connector.paramstyle = 'named'
sql = 'insert into foo(bar, jar) VALUES(:p1, :p2)'
cursor.execute(sql, {"p1":1, "p2":"hello world"})

# format
redshift_connector.paramstyle = 'format'
sql = 'insert into foo(bar, jar) VALUES(%s, %s)'
cursor.execute(sql, (1, "hello world"))

# pyformat
redshift_connector.paramstyle = 'pyformat'
sql = 'insert into foo(bar, jar) VALUES(%(bar)s, %(jar)s)'
cursor.execute(sql, {"bar": 1, "jar": "hello world"})
```

Usar COPY para copiar dados de um bucket do Amazon S3 e UNLOAD para gravar dados nele

O exemplo a seguir mostra como copiar dados de um bucket do Amazon S3 para uma tabela e descarregar dessa tabela de volta no bucket.

Um arquivo de texto chamado `category_csv.txt`, que contém os dados a seguir, é carregado em um bucket do 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"
```

Veja a seguir um exemplo do código Python, que primeiro se conecta ao banco de dados do Amazon Redshift. Em seguida, cria uma tabela chamada `category` e copia os dados CSV do bucket do S3 para a tabela.

```
#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'])
```

Se você não definiu `autocommit` como true, confirme com `conn.commit()` depois de executar as instruções `execute()`.

Os dados são descarregados no arquivo `unloaded_category_csv.text0000_part00` no bucket do S3, com o seguinte conteúdo:

```
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"
```

## Referência de API para o conector Python do Amazon Redshift

A seguir, você encontrará uma descrição das operações de API do conector Python do Amazon Redshift.

### redshift_connector

A seguir, você encontrará uma descrição da operação de API `redshift_connector`.

`connect(user, database, password[, port, …])`

Estabelece uma conexão com um cluster do Amazon Redshift. Essa função valida a entrada do usuário, autentica opcionalmente usando um plugin do provedor de identidade e cria um objeto de conexão.

`apilevel`

O nível DBAPI compatível, atualmente “2.0".

`paramstyle`, `str(object=’’) -> str str(bytes_or_buffer[, encoding[, errors]]) -> str`

O estilo de parâmetro da API do banco de dados a ser usado globalmente.

### Conexão

A seguir, você encontrará uma descrição das operações de API de conexão para o conector Python do Amazon Redshift.

`__init__(user, password, database[, host, …])`

Inicializa um objeto de conexão bruta.

`cursor`

Cria um objeto cursor vinculado a essa conexão.

`commit`

Confirma a transação de banco de dados atual.

`rollback`

Reverte a transação de banco de dados atual.

`close`

Encerra a conexão com o banco de dados.

`execute(cursor, operation, vals)`

Executa os comandos SQL especificados. Você pode fornecer os parâmetros como uma sequência ou como um mapeamento, conforme o valor de `redshift_connector.paramstyle`.

`run(sql[, stream])`

Executa os comandos SQL especificados. Se preferir, você também pode fornecer um fluxo a ser usado com o comando COPY.

`xid(format_id, global_transaction_id, …)`

Crie um ID de transação. Somente o parâmetro `global_transaction_id` é usado em postgres. O format_id e o branch_qualifier não são usados em postgres. O `global_transaction_id` pode ser qualquer identificador de string compatível com postgres que retorne uma tupla (`format_id`, `global_transaction_id`, `branch_qualifier`).

`tpc_begin(xid)`

Inicia uma transação TPC com um ID de transação `xid` consistindo em um ID de formato, ID de transação global e qualificador de ramificação.

`tpc_prepare`

Executa a primeira fase de uma transação iniciada com .tpc_begin.

`tpc_commit([xid])`

Quando chamado sem argumentos, o .tpc_commit confirma uma transação TPC previamente preparada com .tpc_prepare().

`tpc_rollback([xid])`

Quando chamado sem argumentos, o .tpc_rollback reverte uma transação TPC.

`tpc_recover`

Retorna uma lista de IDs de transação pendentes adequadas para uso com .tpc_commit(xid) ou .tpc_rollback(xid).

Cursor

A seguir, você encontrará uma descrição da operação de API de cursor.

`__init__(connection[, paramstyle])`

Inicializa um objeto cursor bruto.

`insert_data_bulk(filename, table_name, parameter_indices, column_names, delimiter, batch_size)`

Executa uma instrução INSERT em massa.

`execute(operation[, args, stream, …])`

Executa uma operação de banco de dados.

`executemany(operation, param_sets)`

Prepara uma operação de banco de dados e a executa para todas as sequências de parâmetros ou mapeamentos fornecidos.

`fetchone`

Busca a próxima linha de um conjunto de resultados de consulta.

`fetchmany([num])`

Busca o próximo conjunto de linhas de um resultado da consulta.

`fetchall`

Busca todas as linhas restantes de um resultado da consulta.

`close`

Encerra o cursor agora.

`__iter__`

É possível iterar um objeto de cursor para recuperar as linhas de uma consulta.

`fetch_dataframe([num])`

Retorna um dataframe dos últimos resultados da consulta.

`write_dataframe(df, table)`

Grava o mesmo dataframe de estrutura em um banco de dados do Amazon Redshift.

`fetch_numpy_array([num])`

Retorna uma matriz NumPy dos últimos resultados da consulta.

`get_catalogs`

O Amazon Redshift não oferece suporte a vários catálogos a partir de uma única conexão. O Amazon Redshift retorna somente o catálogo atual.

`get_tables([catalog, schema_pattern, …])`

Retorna as tabelas públicas exclusivas que são definidas pelo usuário dentro do sistema.

`get_columns([catalog, schema_pattern, …])`

Retorna uma lista de todas as colunas de uma tabela específica em um banco de dados do Amazon Redshift.

### Plugin AdfsCredentialsProvider

Veja a seguir a sintaxe da operação de API do plugin AdfsCredentialsProvider do conector Python do Amazon Redshift.

```
redshift_connector.plugin.AdfsCredentialsProvider()
```

### Plugin AzureCredentialsProvider

Veja a seguir a sintaxe da operação de API do plugin AzureCredentialsProvider do conector Python do Amazon Redshift.

```
redshift_connector.plugin.AzureCredentialsProvider()
```

### Plugin BrowserAzureCredentialsProvider

Veja a seguir a sintaxe da operação de API do plugin BrowserAzureCredentialsProvider do conector Python do Amazon Redshift.

```
redshift_connector.plugin.BrowserAzureCredentialsProvider()
```

Plugin BrowserSamlCredentialsProvider

Veja a seguir a sintaxe da operação de API do plugin BrowserSamlCredentialsProvider do conector Python do Amazon Redshift.

```
redshift_connector.plugin.BrowserSamlCredentialsProvider()
```

Plugin OktaCredentialsProvider

Veja a seguir a sintaxe da operação de API do plugin OktaCredentialsProvider do conector Python do Amazon Redshift.

```
redshift_connector.plugin.OktaCredentialsProvider()
```

Plugin PingCredentialsProvider

Veja a seguir a sintaxe da operação de API do plugin PingCredentialsProvider do conector Python do Amazon Redshift.

```
redshift_connector.plugin.PingCredentialsProvider()
```

Plugin SamlCredentialsProvider

Veja a seguir a sintaxe da operação de API do plugin SamlCredentialsProvider do conector Python do Amazon Redshift.

```
redshift_connector.plugin.SamlCredentialsProvider()
```

## Integração do Amazon Redshift para o Apache Spark

O Apache Spark é um modelo de programação e estrutura de processamento distribuído que ajuda você a realizar machine learning, processamento de fluxo ou análises de gráficos. Semelhante ao Apache Hadoop, o Spark é um sistema de processamento distribuído de código-fonte aberto comumente utilizado para cargas de trabalho Big Data. O Spark tem um mecanismo de execução otimizado de gráfico acíclico direcionado (DAG) e armazena ativamente os dados na memória. Isso pode aumentar a performance, especialmente para determinados algoritmos e consultas interativas.

Essa integração fornece um conector do Spark que você pode usar para criar aplicações do Apache Spark que leem e gravam dados no Amazon Redshift e no Amazon Redshift Serverless. Essas aplicações não comprometem a performance nem a consistência transacional dos dados. Essa integração é incluída automaticamente no Amazon EMR e AWS Glue, portanto você pode executar imediatamente trabalhos do Apache Spark que acessam e carregam dados no Amazon Redshift como parte de seus pipelines de ingestão e transformação de dados.

No momento, é possível usar as versões 3.3.0 e 3.3.1, 3.3.2 e 3.4.0 do Spark com essa integração.

Essa integração fornece o seguinte:

- Autenticação do AWS Identity and Access Management (IAM). Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.
- Aplicação de predicados e consultas para melhorar a performance.
- Tipo de dados do Amazon Redshift.
- Conectividade com o Amazon Redshift e o Amazon Redshift Serverless.

Considerações e limitações ao usar o conector do Spark

- O URI de tempdir aponta para uma localização do Amazon S3. Esse diretório temporário não é limpo automaticamente e pode incorrer custos adicionais. Recomendamos usar as políticas de ciclo de vida do Amazon S3 no Guia do usuário do Amazon Simple Storage Service para definir as regras de retenção para o bucket do Amazon S3.
- Por padrão, as cópias entre o Amazon S3 e o Redshift não funcionam se o bucket do S3 e o cluster do Redshift estiverem em regiões da AWS diferentes. Para usar regiões da AWS separadas, defina o parâmetro `tempdir_region` como a região do bucket do S3 usado para `tempdir`.
- Gravações entre regiões entre o S3 e o Redshift ao gravar dados do Parquet usando o parâmetro `tempformat`.
- Recomendamos usar a criptografia no lado do servidor do Amazon S3 para criptografar os buckets do Amazon S3 usados.
- Recomendamos bloquear o acesso público aos buckets do Amazon S3.
- Recomendamos que o cluster do Amazon Redshift não esteja acessível ao público.
- Recomendamos ativar o registro em log de auditoria do Amazon Redshift.
- Recomendamos ativar a criptografia em repouso do Amazon Redshift.

- Recomendamos ativar SSL para a conexão JDBC do Spark no Amazon EMR ao Amazon Redshift.
- Recomendamos transmitir um perfil do IAM usando o parâmetro `aws_iam_role` para o parâmetro de autenticação do Amazon Redshift.

### Autenticação com o conector do Spark

O diagrama a seguir descreve a autenticação entre o Amazon S3, o Amazon Redshift, o driver do Spark e os executores do Spark.

### Autenticação entre Redshift e Spark

Você pode usar o driver JDBC versão 2 fornecido pelo Amazon Redshift para se conectar ao Amazon Redshift com o conector do Spark especificando as credenciais de login. Para usar o IAM, configure o URL do JDBC para usar a autenticação do IAM. Para se conectar a um cluster do Redshift pelo Amazon EMR ou AWS Glue, certifique-se de que seu perfil do IAM tenha as permissões necessárias para recuperar credenciais temporárias do IAM. A lista a seguir descreve todas as permissões que seu perfil do IAM precisa para recuperar credenciais e executar operações do Amazon S3.

- Redshift:GetClusterCredentials (para clusters provisionados do Redshift)
- Redshift:DescribeClusters (para clusters provisionados do Redshift)
- Redshift:GetWorkgroup (para grupos de trabalho do Amazon Redshift sem servidor)
- Redshift:GetCredentials (para grupos de trabalho do Amazon Redshift Serverless)
- s3:ListBucket
- s3:GetBucket
- s3:GetObject
- s3:PutObject
- s3:GetBucketLifecycleConfiguration

Para obter mais informações sobre GetClusterCredentials, consulte Políticas de recursos para GetClusterCredentials.

Você também deve garantir que o Amazon Redshift possa assumir o perfil do IAM durante as operações `COPY` e `UNLOAD`.

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

Se você estiver usando o driver JDBC mais recente, o driver gerenciará automaticamente a transição de um certificado autoassinado do Amazon Redshift para um certificado do ACM. No entanto, você deve especificar as opções de SSL para o URL de JDBC.

Veja a seguir um exemplo de como especificar o URL do driver JDBC e `aws_iam_role` para se conectar ao 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()
```

Autenticação entre Amazon S3 e Spark

Se você estiver usando um perfil do IAM para realizar a autenticação entre Spark e Amazon S3, use um dos métodos a seguir:

- O AWS SDK para Java tentará encontrar credenciais da AWS automaticamente usando a cadeia de provedores de credenciais padrão implementada pela classe DefaultAWSCredentialsProviderChain. Para obter mais informações, consulte Utilização da cadeia de fornecedores de credenciais padrão.
- Você pode especificar chaves da AWS usando as propriedades de configuração do Hadoop. Por exemplo, se sua configuração de `tempdir` apontar para um sistema de arquivos `s3n://`, defina

as propriedades `fs.s3n.awsAccessKeyId` e `fs.s3n.awsSecretAccessKey` em um arquivo de configuração XML do Hadoop ou chame `sc.hadoopConfiguration.set()` para alterar a configuração global do Hadoop do Spark.

Por exemplo, se estiver usando o sistema de arquivos s3n, adicione:

```
sc.hadoopConfiguration.set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3n.awsSecretAccessKey", "YOUR_SECRET_ACCESS_KEY")
```

Para o sistema de arquivos s3a, adicione:

```
sc.hadoopConfiguration.set("fs.s3a.access.key", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3a.secret.key", "YOUR_SECRET_ACCESS_KEY")
```

Se estiver usando o Python, use as seguintes operações:

```
sc._jsc.hadoopConfiguration().set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc._jsc.hadoopConfiguration().set("fs.s3n.awsSecretAccessKey",
 "YOUR_SECRET_ACCESS_KEY")
```

- Codifique as chaves de autenticação no URL de `tempdir`. Por exemplo, o URI `s3n://ACCESSKEY:SECRETKEY@bucket/path/to/temp/dir` codifica o par de chaves (`ACCESSKEY`, `SECRETKEY`).

Autenticação entre Redshift e Amazon S3

Se você estiver usando os comandos COPY e UNLOAD em sua consulta, também deverá conceder ao Amazon S3 acesso ao Amazon Redshift para executar consultas em seu nome. Para fazer isso, primeiro autorize o Amazon Redshift a acessar outros serviços da AWS, depois autorize as operações COPY e UNLOAD usando perfis do IAM.

Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.

Integração com o AWS Secrets Manager

Você pode recuperar suas credenciais de nome de usuário e senha do Redshift de um segredo armazenado no AWS Secrets Manager. Para fornecer automaticamente as credenciais do Redshift,

use o parâmetro `secret.id`. Para obter mais informações sobre como criar um segredo de credenciais do Redshift, consulte Criar um segredo do banco de dados do AWS Secrets Manager.

| GroupID | ArtifactID | Revisões compatíveis | Descrição |
|---|---|---|---|
| com.amazonaws.secretsmanager | aws-secretsmanager-jdbc | 1.0.12 | A Biblioteca de Conexão SQL para Java do AWS Secrets Manager permite que os desenvolvedores Java se conectem facilmente aos bancos de dados SQL usando segredos armazenados no AWS Secrets Manager. |

> **Note**
>
> Confirmação: esta documentação contém exemplos de código e linguagem desenvolvidos pela Apache Software Foundation e licenciados sob a licença Apache 2.0.

Melhorias de performance com aplicação

O conector do Spark realiza automaticamente a aplicação de predicados e consultas para otimizar a performance. Esse suporte significa que, se você estiver usando uma função compatível em sua consulta, o conector do Spark transformará a função em uma consulta SQL e executará a consulta no Amazon Redshift. Essa otimização resulta em menos dados sendo recuperados, para que o Apache Spark possa processar menos dados e ter melhor performance. Por padrão, a aplicação é ativada automaticamente. Para desativá-la, defina `autopushdown` como 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()
```

As funções a seguir são compatíveis com a aplicação. Se você estiver usando uma função que não está nessa lista, o conector do Spark executará a função no Spark no lugar do Amazon Redshift, resultando em uma performance não otimizada. Para obter uma lista completa das funções no Spark, consulte Funções integradas.

- Funções de agregação
  - avg
  - count
  - max
  - min
  - soma
  - stddev_samp
  - stddev_pop
  - var_samp
  - var_pop
- Operadores boolianos
  - em
  - isnull
  - isnotnull
  - contém
  - endswith
  - startswith
- Operadores lógicos
  - e
  - or
  - not (ou !)
- Funções matemáticas

- +
- -
- *
- /
- - (unário)
- abs
- acos
- asin
- atan
- ceil
- cos
- exp
- floor
- greatest
- least
- log10
- pi
- pow
- round
- sin
- sqrt
- tan

- Funções diversas
  - cast
  - coalesce
  - decimal
  - se
  - em
- Operadores relacionais
  - !=

  - =
  - >
  - >=
  - <
  - <=
- Funções de string
  - ascii
  - lpad
  - rpad
  - translate
  - upper
  - lower
  - length
  - trim
  - ltrim
  - rtrim
  - like
  - substring
  - concat
- Funções de data e hora
  - add_months
  - data
  - date_add
  - date_sub
  - date_trunc
  - timestamp
  - trunc
- Operadores matemáticos
  - CheckOverflow
  - PromotePrecision

- Operações relacionais
  - Aliases (por exemplo, AS)
  - CaseWhen
  - Distinto
  - InSet
  - Junções e junções cruzadas
  - Limites
  - Unions, union all
  - ScalarSubquery
  - Sorts (crescente e decrescente)
  - UnscaledValue

Outras opções de configuração

Alterar o tamanho máximo das colunas de string

O Redshift cria colunas de string como colunas de texto ao criar tabelas, que são armazenadas como VARCHAR(256). Se você quiser colunas que ofereçam suporte a tamanhos maiores, poderá usar maxlength para especificar o comprimento máximo das colunas de string. Veja a seguir um exemplo de como especificar `maxlength`.

```
columnLengthMap.foreach { case (colName, length) =>
  val metadata = new MetadataBuilder().putLong("maxlength", length).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

Definir um tipo de coluna

Para definir um tipo de coluna, use o campo `redshift_type`.

```
columnTypeMap.foreach { case (colName, colType) =>
  val metadata = new MetadataBuilder().putString("redshift_type", colType).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

Definir uma codificação de compressão em uma coluna

Para usar uma codificação de compressão específica em uma coluna, use o campo de codificação. Para obter uma lista completa das codificações de compressão compatíveis, consulte Codificações de compressão.

Definir uma descrição para uma coluna

Para definir uma descrição, use o campo `description`.

Autenticação entre Redshift e Amazon S3

Por padrão, o resultado é descarregado no Amazon S3 no formato parquet. Para descarregar o resultado como um arquivo de texto delimitado por barras, especifique a opção a seguir.

```
.option("unload_s3_format", "TEXT")
```

Executa instruções de aplicação lentamente

| Parâmetro | Obrigatório | Padrão | Descrição |
|---|---|---|---|
| spark.datasource.redshift.community.autopushdown.lazyMode | Não | Verdadeiro | Especifica se o conector deve executar lentamente as instruções de aplicação do Redshift.<br><br>Se for verdadeiro, o conector Spark recuperará todos os modelos e as informações relacionados antes de executar a consulta, o que geralmente melhora a performance. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| | | | Se for falso, o conector Spark executará as instruções de aplicação imediatamente no thread principal do driver do Spark e será serializado em todas as expressões. |

Parâmetros do conector

O mapa de parâmetros ou `OPTIONS` no Spark SQL é compatível com as seguintes configurações.

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| dbtable | Sim, a menos que a consulta seja especificada | N/D | A tabela para criar ou ler no Redshift. Este parâmetro é necessário ao salvar dados no Redshift. |
| consulta | Sim, a menos que dbtable seja especificado | N/D | A consulta para ler do Redshift. |
| user | Não | N/D | O nome de usuário do Redshift. Deve ser usado com o parâmetro password. Válido somente se o usuário e a senha não forem parâmetros no URL. Usar os |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| | | | dois causará um erro. |
| password | Não | N/D | A senha do Redshift. Deve ser usado com o parâmetro user. Válido somente se o usuário e a senha não forem parâmetros no URL. Usar os dois causará um erro. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| url | Não | N/D | Um URL de JDBC. O formato é jdbc:subprotocol://host:port/database?user=username&password=password.<br><br>O subprotocolo pode ser postgresql ou Redshift, dependendo do driver JDBC que você carregou. Observe que um driver compatível com o Redshift deve estar no classpath e corresponder a esse URL.<br><br>O host e a porta devem apontar para o nó principal do Redshift, então você deve configurar grupos de segurança e/ou VPC para permitir o acesso de sua aplicação de driver.<br><br>O banco de dados é o nome do banco de dados do Redshift.<br><br>O usuário e a senha são credenciais para |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| | | | acessar o banco de dados, que devem estar incorporadas nesse URL para JDBC, e o usuário do banco de dados deve ter as permissões necessárias para acessar a tabela. |
| aws_iam_role | Somente se estiver usando perfis do IAM para autorizar operações COPY/ UNLOAD do Redshift | N/D | ARN totalmente especificado do perfil do IAM anexado ao cluster do Redshift. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| forward_spark_s3_credentials | Não | Falso | Indica se essa biblioteca deve descobrir automaticamente as credenciais que o Spark usa para se conectar ao Amazon S3 e se deve encaminhar essas credenciais para o Redshift pelo driver JDBC. Essas credenciais são enviadas como parte da consulta JDBC. Portanto, recomendamos que você habilite a criptografia SSL com conexão JDBC ao usar essa opção. |
| temporary_aws_access_key_id | Não | N/D | Chave de acesso da AWS. Você deve ter permissões de gravação no bucket do S3. |
| temporary_aws_secret_access_key | Não | N/D | A chave de acesso secreta da AWS que corresponde à chave de acesso. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| temporary_aws_session_token | Não | N/D | Token de sessão da AWS que corresponde à chave de acesso fornecida. |
| tempdir | Não | N/D | Um local gravável no Amazon S3. Usado para descarregar dados durante a leitura e dados do Avro para serem carregados no Redshift durante a gravação. Se você estiver usando uma fonte de dados do Redshift para o Spark como parte de um pipeline de ETL normal, poderá ser útil definir uma política de ciclo de vida em um bucket e usá-lo como um local temporário para esses dados. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| jdbcdriver | Não | Determinado pelo subprotocolo do URL de JDBC | O nome da classe do driver JDBC a ser usado. Essa classe deve estar no classpath. Na maioria dos casos, não deve ser necessári o especificar essa opção, pois o nome de classe do driver apropriado deve ser determinado automaticamente pelo subprotocolo do URL de JDBC. |
| diststyle | Não | Even | O estilo de distribui ção do Redshift a ser usado ao criar uma tabela. As opções válidas são EVEN, KEY ou ALL. Ao usar KEY, você também deve definir uma chave de distribuição com a opção distkey. |
| distkey | Não, a menos que esteja usando DISTSTYLE_KEY | N/D | O nome de uma coluna na tabela para usar como chave de distribuição ao criar uma tabela. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| sortkeyspec | Não | N/D | Uma definição completa de chave de classificação do Redshift. |
| include_column_list | Não | Falso | Indica se essa biblioteca deve extrair automatic amente as colunas do esquema e adicioná-las ao comando COPY de acordo com as opções de mapeamento de colunas. |
| descrição | Não | N/D | Uma descrição da tabela. A descrição é definida com o comando SQL COMMENT e aparece na maioria das ferramentas de consulta. Veja os metadados de `description` para definir descrições em colunas individuais. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| preactions | Não | N/D | Uma lista delimitada por ponto e vírgula dos comandos SQL a serem executados antes de carregar o comando COPY. Pode ser útil para executar comandos DELETE ou similares antes de carregar novos dados.<br>Se o comando contiver %s, o nome da tabela será formatado antes do tempo de execução (caso você esteja usando uma tabela de preparação).<br>Se esse comando falhar, ele será tratado como uma exceção. Se você estiver usando uma tabela de preparação, as alterações serão revertidas e restaurarão a tabela de backup se preactions falhar. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| extracopyoptions | Não | N/D | Uma lista de opções extras para anexar ao comando COPY do Redshift ao carregar dados (como `TRUNCATECOLUMNS` ou `MAXERROR n`). Consulte Parâmetro opcional para obter uma lista completa dos parâmetros disponíveis.<br><br>Observe que, como essas opções são anexadas ao final do comando `COPY`, você só pode usar opções que façam sentido no final do comando. Isso deve abranger a maioria dos casos de uso possíveis. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| sse_kms_key | Não | N/D | O ID da chave do AWS KMS a ser usado para criptografia do lado do servidor no S3 durante a operação UNLOAD do Redshift, em vez da criptografia padrão da AWS. O perfil do IAM do Redshift deve ter acesso à chave do KMS para gravar com ele, e o perfil do IAM do Spark deve ter acesso à chave para as operações de leitura. A leitura de dados criptogra fados não requer alterações (a AWS resolve isso), desde que o perfil do IAM do Spark tenha o acesso adequado. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| tempformat | Não | AVRO | O formato no qual salvar arquivos temporários no Amazon S3 ao gravar no Redshift. Os valores válidos são AVRO, CSV e CSV GZIP (CSV compactado). |
| csvnullstring (experimental) | Não | Nulo | O valor da string a ser gravado para nulos ao usar o tempformat CSV. Deve ser um valor que não aparece nos dados reais. |
| autopushdown | Não | Verdadeiro | Indica se é necessário realizar aplicação de predicados e consultas ao capturar e analisar os planos lógicos do Spark para operações SQL. As operações são traduzidas em uma consulta SQL e executadas no Redshift para melhorar a performance. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| autopushdown.s3_result_cache | Não | Falso | Armazene a consulta SQL em cache para descarregar dados do mapeamento de caminhos do Amazon S3 na memória, para que a mesma consulta não precise ser executada novamente na mesma sessão do Spark. Só é compatível quando o parâmetro autopushdown está ativado. Não recomendamos usar esse parâmetro ao misturar operações de leitura e gravação, pois os resultados armazenados em cache podem conter informações obsoletas. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| unload_s3_format | Não | Parquet | O formato para descarregar os resultados da consulta. As opções válidas são Parquet e Text, que especificam o descarregamento dos resultados da consulta no formato de texto delimitado por barras. |
| extraunloadoptions | Não | N/D | Opções extras para anexar ao comando UNLOAD do Redshift. Não há garantia de que todas as opções funcionem, pois algumas opções podem entrar em conflito com outras opções definidas no conector. |
| copydelay | Não | 30000 | O atraso (em ms) entre novas tentativas de operações COPY do Redshift. |
| copyretrycount | Não | 2 | O número de novas tentativas para operações COPY do Redshift. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| tempdir_region | Não | N/D | A região da AWS em que `tempdir` está localizado. A configuração dessa opção melhora a performance do conector para interações com `tempdir` além de fornecer automatic amente esse valor como parte das operações COPY e UNLOAD durante as operações de leitura e gravação do conector.<br><br>Essa configuração é recomendada nas seguintes situações:<br><br>1) Quando o conector estiver em execução fora da AWS, pois a descoberta automátic a da região falhará e afetará negativam ente a performance do conector.<br><br>2) Quando `tempdir` estiver em uma região diferente do |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| | | | cluster do Redshift, pois o uso dessa configuração diminui a necessidade de fornecer a região manualmente usando os parâmetros `extracopyoptions` e `extraunloadoptions`. `tempdir` não pode estar em uma região diferente do cluster do Redshift ao usar `PARQUET` como `tempformat`, mesmo que esteja usando esse parâmetro.<br><br>3) Quando o conector estiver em execução em uma região diferente de `tempdir`, pois melhora a performance de acesso de `tempdir` do conector. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| secret.id | Não | N/D | O nome ou ARN do segredo armazenado no AWS Secrets Manager. É possível usar esse parâmetro para fornecer automaticamente as credenciais do Redshift, mas somente se o usuário, a senha e as credenciais de `DbUser` não forem passadas para o URL do JDBC ou como outras opções. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| secret.region | Não | N/D | A região da AWS principal, como Leste dos EUA (N. da Virgínia), para pesquisar o valor de `secret.id` .<br><br>Se você não especificar essa região, o conector tentará usar a Cadeia de fornecedores de credenciais padrão para resolver a região de `secret.id` . Em alguns casos (por exemplo, se você estiver usando o conector fora da AWS), o conector não conseguirá encontrar a região. Recomendamos o uso dessa configuração nas seguintes situações:<br><br>1) Quando o conector está em execução fora da AWS, pois a descoberta automática de região falhará e |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| | | | impedirá a autentica ção com o Redshift<br><br>Quando o conector estiver em execução em uma região diferente de `secret.id` , pois melhora a performan ce de acesso do segredo do conector. |
| secret.vpcEndpointUrl | Não | N/D | O URL do endpoint de DNS do PrivateLi nk para AWS Secrets Manager ao substitui r a Cadeia de fornecedores de credenciais padrão. |
| secret.vpcEndpoint Region | Não | N/D | A região do endpoint de DNS do PrivateLi nk para AWS Secrets Manager ao substitui r a Cadeia de fornecedores de credenciais padrão. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| jdbc.* | Não | N/D | Parâmetros adicionais a serem transmitidos ao driver JDBC subjacente, em que o caractere curinga é o nome do parâmetro JDBC, como jdbc.ssl. Observe que o prefixo `jdbc` será removido antes de ser transmitido ao driver JDBC. Para ver todas as opções possíveis para o driver JDBC do Redshift, consulte Opções para a configuração do driver JDBC versão 2.1. |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| label | Não | " " | Um identificador a ser incluído no grupo de consultas definido ao executar consultas com o conector. Deve ter 100 caracteres ou menos e todos os caracteres devem ser `unicodeId entifierParts` válidos. Se o identificador tiver mais de 100 caracteres, o excesso será removido. Ao executar uma consulta com o conector, o grupo de consultas será definido como uma string no formato JSON, como `{"spark-redshift-connector":{"svc":"","ver":"5.1.0-amzn-1-spark_3.3","op":"Read","lbl":""}}`) |

| Parâmetro | Obrigatório | Padrão | Descrição |
| --- | --- | --- | --- |
| | | | . Essa opção substitui o valor da chave `lbl`. |

> **Note**
>
> Confirmação: esta documentação contém exemplos de código e linguagem desenvolvidos pela Apache Software Foundation e licenciados sob a licença Apache 2.0.

Tipos de dados compatíveis

Os seguintes tipos de dados no Amazon Redshift são compatíveis com o conector do Spark. Para obter uma lista completa dos tipos de dados compatíveis no Amazon Redshift, consulte Tipos de dados. Se um tipo de dado não está na tabela abaixo, ele não é compatível com o conector do Spark.

| Tipo de dados | Aliases |
| --- | --- |
| SMALLINT | INT2 |
| INTEGER | INT, INT4 |
| BIGINT | INT8 |
| DECIMAL | NUMERIC |
| REAL | FLOAT4 |
| DOUBLE PRECISION | FLOAT8, FLOAT |
| BOOLEAN | BOOL |
| CHAR | CHARACTER, NCHAR, BPCHAR |
| VARCHAR | CHARACTER VARYING, NVARCHAR, TEXT |

| Tipo de dados | Aliases |
| --- | --- |
| DATE | |
| TIMESTAMP | Time stamp sem fuso horário |
| TIMESTAMPTZ | Time stamp com fuso horário |
| SUPER | |
| TIME | Hora sem fuso horário |
| TIMETZ | Hora com fuso horário |
| VARBYTE | VARBINARY, BINARY VARYING |

Tipos de dados complexos

É possível usar o conector Spark para ler e gravar tipos de dados complexos do Spark, como `ArrayType`, `MapType` e `StructType` de e para as colunas do tipo de dados SUPER do Redshift. Se você fornecer um esquema durante uma operação de leitura, os dados na coluna serão convertidos em seus tipos complexos correspondentes no Spark, incluindo qualquer tipo aninhado. Além disso, se `autopushdown` estiver habilitado, a projeção de atributos aninhados, valores de mapas e índices de matriz será enviada ao Redshift para que toda a estrutura de dados aninhada não precise mais ser descarregada ao acessar apenas uma parte dos dados.

Quando você grava DataFrames pelo conector, qualquer coluna do tipo `MapType`(usando `StringType`) `StructType` ou `ArrayType` é gravada em uma coluna de tipo de dados SUPER do Redshift. Ao escrever essas estruturas de dados aninhadas, o parâmetro `tempformat` deve ser do tipo `CSV`, `CSV GZIP` ou `PARQUET`. Usar `AVRO` causará uma exceção. Gravar uma estrutura de dados `MapType` que tem um tipo de chave diferente de `StringType` também causará uma exceção.

StructType

O exemplo a seguir demonstra como criar uma tabela com um tipo de dados SUPER que contém uma estrutura.

```
create table contains_super (a super);
```

Depois, é possível usar o conector para consultar um campo `StringType` `hello` da coluna a de SUPER na tabela usando um esquema como no exemplo a seguir.

```
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")
```

O exemplo a seguir demonstra como escrever uma estrutura na coluna a.

```
import org.apache.spark.sql.types._
import org.apache.spark.sql._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", StructType(StructField("hello",
 StringType) ::Nil)) :: Nil)
val data = sc.parallelize(Seq(Row(Row("world"))))
val mydf = sqlContext.createDataFrame(data, schema)

mydf.write.format("io.github.spark_redshift_community.spark.redshift").
option("url", jdbcUrl).
option("dbtable", tableName).
option("tempdir", tempS3Dir).
option("tempformat", "CSV").
mode(SaveMode.Append).save
```

### MapType

Se você preferir usar um `MapType` para representar seus dados, poderá usar uma estrutura de dados `MapType` no esquema e recuperar o valor correspondente a uma chave no mapa. Observe que todas as chaves na estrutura de dados `MapType` deve ser do tipo String e todos os valores devem ser do mesmo tipo, como int.

O exemplo a seguir demonstra como obter o valor da chave `hello` na coluna `a`.

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", MapType(StringType, IntegerType))::Nil)

val helloDF = sqlContext.read
    .format("io.github.spark_redshift_community.spark.redshift")
    .option("url", jdbcURL )
    .option("tempdir", tempS3Dir)
    .option("dbtable", "contains_super")
    .schema(schema)
    .load().selectExpr("a['hello']")
```

### ArrayType

Se a coluna contiver uma matriz em vez de uma estrutura, você poderá usar o conector para consultar o primeiro elemento na matriz.

```
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]")
```

Limitações

O uso de tipos de dados complexos com o conector do Spark tem as seguintes limitações:

- Todos os nomes de campos de estrutura aninhados e chaves de mapa devem estar em letras minúsculas. Se estiver consultando nomes de campos complexos com letras maiúsculas, uma solução alternativa é tentar omitir o esquema e usar a função `from_json` do Spark para converter a string retornada localmente.
- Qualquer campo de mapa usado em operações de leitura ou gravação precisa ter apenas chaves `StringType`.
- Somente `CSV`, `CSV GZIP` e `PARQUET` são valores de formato temporário compatíveis para gravar tipos complexos no Redshift. Tentar usar `AVRO` lançará uma exceção.

## Configurar uma conexão para o driver ODBC versão 2.x para o Amazon Redshift

Você pode usar uma conexão ODBC para se conectar ao seu cluster Amazon Redshift a partir de muitas ferramentas e aplicações de cliente SQL de terceiros. Se sua ferramenta cliente oferece suporte ao JDBC, é possível optar por usar esse tipo de conexão em vez de usar o ODBC, devido à facilidade de configuração que o JDBC oferece. No entanto, se sua ferramenta cliente não for compatível com JDBC, siga as etapas nesta seção para configurar uma conexão ODBC em seu computador cliente ou instância do Amazon EC2.

O Amazon Redshift fornece drivers ODBC de 64 bits para sistemas operacionais Linux e Windows. Os drivers ODBC de 32 bits foram descontinuados. Atualmente, não há suporte para o macOS X. Outras atualizações de drivers ODBC de 32bits não serão lançadas, exceto para patches de segurança urgentes. Para baixar e instalar drivers ODBC para macOS X e para sistemas operacionais de 32 bits, consulte Configurar uma conexão ODBC.

Para obter as informações mais recentes sobre as alterações do driver ODBC, consulte o log de alterações.

Tópicos

- Obter o URL do ODBC
- Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows
- Instalar e configurar o driver ODBC do Amazon Redshift no Linux

- Configurar a autenticação
- Conversão de tipos de dados
- Configuração das opções do driver ODBC
- Versões anteriores do driver ODBC

### Obter o URL do ODBC

O Amazon Redshift exibe o URL do ODBC para o cluster no console do Amazon Redshift. Este URL contém as informações necessárias para a configuração da conexão entre o computador cliente e o banco de dados.

O URL do ODBC tem o seguinte formato:

```
Driver={driver}; Server=endpoint_host; Database=database_name; UID=user_name;
 PWD=password; Port=port_number
```

Os campos do formato anterior possuem os seguintes valores:

Valores de campo de URL do ODBC

| Campo | Valor |
| --- | --- |
| *Driver* | O nome do driver ODBC de 64 bits a ser usado: Amazon Redshift ODBC Driver (x64) (Driver ODBC do Amazon Redshift (x64)) |
| *Server* | O host do endpoint do cluster Amazon Redshift. |
| *Database* | O banco de dados que você criou para o cluster. |
| *UID* | O nome do usuário de uma conta de usuário de banco de dados que tem a permissão para se conectar ao banco de dados. Embora esse valor seja uma permissão de nível de banco de dados, não uma permissão de nível de cluster, é possível usar a conta de usuário administrador do Redshift que você configurou quando iniciou o cluster. |
| *PWD* | A senha da conta de usuário de banco de dados para se conectar ao banco de dados. |

| Campo | Valor |
| --- | --- |
| *Port* | O número da porta usado quando você iniciou o cluster. Se você tem um firewall, certifique-se de que essa porta está aberta para uso. |

Este é um exemplo de URL de 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
```

Para obter informações sobre onde encontrar o URL do ODBC, consulte Encontrar a string de conexão do cluster.

Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows

Requisitos do sistema

Você deve instalar o driver ODBC do Amazon Redshift em computadores clientes que tenham acesso um data warehouse do Amazon Redshift. Para cada computador onde o driver é instalado, os seguintes requisitos mínimos do sistema devem ser atendidos:

- Direitos de administrador na máquina.
- A máquina atende aos seguintes requisitos do sistema:
  - Um dos seguintes sistemas operacionais:
    - Windows 10 ou 8.1.
    - Windows Server 2019, 2016 ou 2012.
  - 100 MB de espaço em disco disponível.
  - Visual C++ redistribuível para Visual Studio 2015 para Windows de 64 bits instalado. É possível baixar o pacote de instalação em Baixe o Visual C++ redistribuível para Visual Studio 2022 no site da Microsoft.

### Instalar o driver ODBC do Amazon Redshift

Use o procedimento a seguir para baixar e instalar os drivers ODBC do Amazon Redshift para sistemas operacionais Windows. Use apenas um driver diferente se estiver executando uma aplicação de terceiros certificada para uso com o Amazon Redshift e que exija um driver específico.

Para baixar e instalar o driver ODBC:

1. Baixe o seguinte driver: Driver ODBC de 64 bits versão 2.1.0.0

   O nome desse driver é Amazon Redshift ODBC Driver (x64).

   > **Note**
   >
   > Os drivers ODBC de 32 bits foram descontinuados. Outras atualizações não serão lançadas, exceto para patches de segurança urgentes. Para baixar e instalar drivers ODBC para sistemas operacionais de 32 bits, consulte Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows.

2. Analise a licença do driver ODBC do Amazon Redshift versão 2.x.
3. Clique duas vezes no arquivo .msi e, em seguida, siga os passos do assistente para instalar o driver.

### Criação de uma entrada de DSN do sistema para uma conexão ODBC

Depois de baixar e instalar o driver ODBC, adicione uma entrada de nome de origem dos dados (DSN) ao computador cliente ou instância do Amazon EC2. As ferramentas de cliente SQL podem usar essa fonte de dados para se conectar ao banco de dados do Amazon Redshift.

Recomendamos a criação de um DSN de sistema em vez de um DSN de usuário. Algumas aplicações podem carregar dados usando uma conta de usuário de banco de dados diferente e podem não conseguir detectar DSNs de usuário criados em outra conta de usuário de banco de dados.

> **Note**
>
> Para realizar a autenticação usando as credenciais do AWS Identity and Access Management (IAM) ou do provedor de identidades (IdP), serão necessárias etapas

adicionais. Para obter mais informações, consulte Configurar uma conexão JDBC ou ODBC para usar credenciais do IAM.

Crie uma entrada de DSN de sistema para uma conexão ODBC:

1. No menu Start (Iniciar), abra "Fontes de dados ODBC". Escolha ODBC Data sources (Fontes de dados ODBC).

   Certifique-se de escolher o Administrador de origem dos dados ODBC que tem a mesma quantidade de bits da aplicação cliente que você está usando para se conectar ao Amazon Redshift.
2. Em ODBC Data Source Administrator (Administrador de fonte de dados ODBC), escolha a guia Driver e localize a seguinte pasta do driver: Amazon Redshift ODBC Driver (x64) (Driver ODBC do Amazon Redshift (x64)).
3. Selecione a guia DSN de sistema a fim de configurar o driver para todos os usuários no computador, ou a guia DSN de usuário a fim de configurar o driver apenas para sua conta de usuário de banco de dados.
4. Escolha Add. A janela Create New Data Source é exibida.
5. Escolha o Amazon Redshift ODBC driver (x64) (Driver ODBC do Amazon Redshift (x64)) e, em seguida, escolha Finish (Concluir). A janela Configuração de DSN do driver ODBC do Amazon Redshift é exibida.
6. Na seção Connection Settings (Configurações de conexão), insira as seguintes informações:

   Nome da fonte de dados

   Insira um nome para a fonte de dados. Por exemplo, se você seguiu o Guia de conceitos básicos do Amazon Redshift, pode digitar `exampleclusterdsn` para facilitar a lembrança do cluster que associa a este DSN.

   Servidor

   Especifique o host de endpoint do cluster do Amazon Redshift. Você pode encontrar essas informações no console do Amazon Redshift na página de detalhes do cluster. Para obter mais informações, consulte Configurar conexões no Amazon Redshift.

   Porta

Insira o número da porta que o banco de dados usa. Dependendo da porta selecionada ao criar, modificar ou migrar o cluster, permita o acesso à porta selecionada.

Banco de dados

Insira o nome do banco de dados do Amazon Redshift. Se você iniciou o cluster sem especificar um nome de banco de dados, insira `dev`. Caso contrário, use o nome escolhido durante o processo de inicialização. Se você seguiu o Guia de conceitos básicos do Amazon Redshift, insira `dev`.

7. Na seção Authentication (Autenticação), especifique as opções de configuração para configurar a autenticação padrão ou do IAM.
8. Escolha SSL Options (Opções SSL) e especifique um valor para o seguinte:

   Modos de autenticação

   Escolha um modo para tratar o Secure Sockets Layer (SSL). Em um ambiente de teste, você pode usar `prefer`. No entanto, para ambientes de produção e quando um intercâmbio de dados seguro for necessário, use `verify-ca` ou `verify-full`.
9. Na guia Proxy, especifique qualquer configuração de conexão proxy.
10. Na guia Cursor, especifique opções sobre como retornar os resultados de consultas ao aplicativo ou ferramenta do cliente SQL.
11. Em Opções avançadas, especifique valores para `logLevel`, `logPath`, `compression` e outras opções.
12. Escolha Testar. Se o computador cliente puder se conectar ao banco de dados Amazon Redshift, a seguinte mensagem será exibida: Connection successful (Conexão bem-sucedida). Se a conexão do computador cliente com o banco de dados falhar, você poderá solucionar os possíveis problemas gerando um arquivo de log e entrando em contato com o suporte da AWS. Para obter informações sobre como gerar logs, consulte (LINK).
13. Escolha OK.

## Instalar e configurar o driver ODBC do Amazon Redshift no Linux

### Requisitos do sistema

Você deve instalar o driver ODBC do Amazon Redshift em computadores clientes que tenham acesso um data warehouse do Amazon Redshift. Para cada computador onde o driver é instalado, os seguintes requisitos mínimos do sistema devem ser atendidos:

- Acesso root na máquina.
- Uma das distribuições seguintes:
  - Red Hat® Enterprise Linux® (RHEL) 8 ou posterior
  - CentOS 8 ou posterior
- 150 MB de espaço em disco disponível.
- unixODBC 2.2.14 ou posterior.
- glibc 2.26 ou posterior.

### Instalar o driver ODBC do Amazon Redshift

Para baixar e instalar o driver ODBC do Amazon Redshift versão 2.x para Linux:

1. Baixe o seguinte driver: Driver RPM de 64 bits versão 2.1.10.0

   > **Note**
   >
   > Os drivers ODBC de 32 bits foram descontinuados. Outras atualizações não serão lançadas, exceto para patches de segurança urgentes.

2. Navegue até o local onde você salvou o download do pacote e execute um dos comandos a seguir. Use o comando que corresponde a sua distribuição do Linux.

   Em sistemas operacionais RHEL e CentOS, execute o seguinte comando:

   ```
   yum --nogpgcheck localinstall RPMFileName
   ```

   Substitua `RPMFileName` pelo nome do arquivo de pacote do RPM. Por exemplo, o comando a seguir demonstra a instalação do driver de 64 bits:

```
yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-2.x.xx.xxxx.x86_64.rpm
```

Utilização de um gerenciador de driver ODBC para configurar o driver ODBC no Linux

No Linux, utilize o gerenciador de driver ODBC para configurar as definições de conexão ODBC. Os gerenciadores de driver ODBC usam arquivos de configuração para definir e configurar as fontes de dados e os drivers ODBC. O gerenciador de driver ODBC a ser usado dependerá do sistema operacional em uso.

Configuração do driver ODBC usando o gerenciador de driver unixODBC

Os arquivos a seguir são necessários para configurar o driver ODBC do Amazon Redshift:

- `amazon.redshiftodbc.ini`
- `odbc.ini`
- `odbcinst.ini`

Se você fez a instalação no local padrão, o arquivo de configuração do `amazon.redshiftodbc.ini` estará localizado em `/opt/amazon/redshiftodbcx64`.

Além disso, em `/opt/amazon/redshiftodbcx64`, é possível encontrar exemplos de arquivos `odbc.ini` e `odbcinst.ini`. Você pode usar esses arquivos como exemplos para configurar o driver ODBC do Amazon Redshift e o nome da origem dos dados (DSN).

Não é recomendado o uso do diretório de instalação do driver ODBC do Amazon Redshift para os arquivos de configuração. Os arquivos de exemplo do diretório instalado devem ser usados somente para servir de modelo. Se você reinstalar o driver ODBC do Amazon Redshift posteriormente ou atualizar para uma versão mais recente, o diretório de instalação será substituído. Você perderá todas as alterações feitas nos arquivos do diretório de instalação.

Para evitar isso, copie o arquivo `amazon.redshiftodbc.ini` para um diretório diferente do diretório de instalação. Se você copiar esse arquivo no diretório base do usuário, adicione um ponto (.) ao início do nome do arquivo para torná-lo um arquivo oculto.

Para os arquivos `odbc.ini` e `odbcinst.ini`, use os arquivos de configuração do diretório inicial do usuário ou crie versões em um outro diretório. Por padrão, os sistemas operacionais Linux devem ter um arquivo `odbc.ini` e um `odbcinst.ini` no diretório inicial do usuário (`/home/$USER` ou `~/.`). Esses arquivos padrão são arquivos ocultos, o que é indicado pelo ponto (.) na frente do

nome de cada arquivo. Esses arquivos são exibidos somente ao usar o sinalizador `-a` para listar o conteúdo do diretório.

Qualquer que seja a opção escolhida para os arquivos `odbc.ini` e `odbcinst.ini`, modifique os arquivos para adicionar as informações do driver e da configuração de DSN. Se você criar arquivos, também precisará definir as variáveis do ambiente para especificar onde esses arquivos de configuração estão localizados.

Por padrão, os gerenciadores de driver ODBC são configurados para usar versões ocultas dos arquivos de configuração `odbc.ini` e `odbcinst.ini` (chamados `.odbc.ini` e `.odbcinst.ini`) localizadas no diretório inicial. Eles também são configurados para usar o arquivo `amazon.redshiftodbc.ini` do diretório de instalação do driver. Se você armazenar esses arquivos de configuração em outro lugar, defina as variáveis de ambiente descritas a seguir para que o gerenciador de driver possa localizar os arquivos.

Se você estiver usando o unixODBC, faça o seguinte:

- Defina `ODBCINI` para o caminho completo e o nome de arquivo do arquivo `odbc.ini`.
- Defina `ODBCSYSINI` para o caminho completo do diretório que contém o arquivo `odbcinst.ini`.
- Defina `AMAZONREDSHIFTODBCINI` para o caminho completo e o nome de arquivo do arquivo `amazon.redshiftodbc.ini`.

Veja a seguir um exemplo de definição das variáveis acima:

```
export ODBCINI=/usr/local/odbc/odbc.ini
export ODBCSYSINI=/usr/local/odbc
export AMAZONREDSHIFTODBCINI=/etc/amazon.redshiftodbc.ini
```

Configuração de uma conexão usando um nome de fonte de dados (DSN) no Linux

Ao conectar-se ao datastore usando um nome da fonte de dados (DSN), configure o arquivo `odbc.ini` para definir nomes de fonte de dados (DSNs). Defina as propriedades no arquivo `odbc.ini` para criar um DSN que especifique as informações de conexão para o armazenamento de dados.

Use o seguinte formato nos sistemas operacionais 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
```

O exemplo a seguir mostra a configuração do `odbc.ini` com driver ODBC de 64 bits em sistemas operacionais Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift ODBC Driver (x64)

[Amazon_Redshift_x64]
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932Database=dev
locale=en-US
```

Configurar uma conexão sem um DSN no Linux

Para se conectar ao armazenamento de dados por meio de uma conexão que não tenha um DSN, defina o driver no arquivo `odbcinst.ini`. Depois, forneça uma string de conexão sem DSN no aplicativo.

Use o seguinte formato nos sistemas operacionais Linux:

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

O exemplo a seguir mostra a configuração do `odbcinst.ini` com driver ODBC de 64 bits em sistemas operacionais 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
```

Configurar a autenticação

Para proteger os dados contra acesso não autorizado, os armazenamentos de dados do Amazon Redshift exigem que todas as conexões sejam autenticadas usando credenciais do usuário.

A seguinte tabela ilustra as opções de conexão necessárias e opcionais para cada método de autenticação que pode ser usado para se conectar ao driver ODBC do Amazon Redshift versão 2.x:

Método de autenticação ODBC e opções de conexão obrigatórias e opcionais

| Método de autenticação | Obrigatório | Opcional |
| --- | --- | --- |
| Padrão | • Host<br>• Porta<br>• Banco de dados<br>• UID<br>• Senha | |
| Perfil do IAM | • Host<br>• Porta<br>• Banco de dados<br>• IAM<br>• Perfil | • ClusterID<br>• Região<br>• AutoCreate<br>• EndpointURL<br>• StsEndpointURL<br>• InstanceProfile |

| Método de autenticação | Obrigatório | Opcional |
| --- | --- | --- |
| | | **Note**<br>ClusterID e Region (Região) deverão ser definidos em Host se eles não estiverem definidos separadam ente. |
| Credenciais do IAM | • Host<br>• Porta<br>• Banco de dados<br>• IAM<br>• AccessKeyID<br>• SecretAccessKey | • ClusterID<br>• Região<br>• AutoCreate<br>• EndpointURL<br>• StsEndpointURL<br>• SessionToken<br>• UID<br><br>**Note**<br>ClusterID e Region (Região) deverão ser definidos em Host se eles não estiverem definidos separadam ente. |

| Método de autenticação | Obrigatório | Opcional |
| --- | --- | --- |
| AD FS | • Host<br>• Porta<br>• Banco de dados<br>• IAM<br>• plugin_name<br>• UID<br>• Senha<br>• IdP_Host<br>• IdP_Port | • ClusterID<br>• Região<br>• AutoCreate<br>• EndpointUrl<br>• StsEndpointUrl<br>• Preferred_Role<br>• loginToRp<br>• SSL_Insecure<br><br>**Note**<br>ClusterID e Region (Região) deverão ser definidos em Host se eles não estiverem definidos separadam ente. |

| Método de autenticação | Obrigatório | Opcional |
| --- | --- | --- |
| Azure AD | • Host<br>• Porta<br>• Banco de dados<br>• IAM<br>• plugin_name<br>• UID<br>• Senha<br>• IdP_Tenant<br>• Client_ID<br>• Client_Secret | • ClusterID<br>• Região<br>• AutoCreate<br>• EndpointUrl<br>• StsEndpointUrl<br>• Preferred_Role<br>• dbgroups_filter<br><br>**Note**<br>ClusterID e Region (Região) deverão ser definidos em Host se eles não estiverem definidos separadam ente. |
| JWT | • Host<br>• Porta<br>• Banco de dados<br>• IAM<br>• plugin_name<br>• web_identity_token | • provider_name |

| Método de autenticação | Obrigatório | Opcional |
| --- | --- | --- |
| Okta | • Host<br>• Porta<br>• Banco de dados<br>• IAM<br>• plugin_name<br>• UID<br>• Senha<br>• IdP_Host<br>• App_Name<br>• App_ID | • ClusterID<br>• Região<br>• AutoCreate<br>• EndpointUrl<br>• StsEndpointUrl<br>• Preferred_Role<br><br>**Note**<br>ClusterID e Region (Região) deverão ser definidos em Host se eles não estiverem definidos separadam ente. |

| Método de autenticação | Obrigatório | Opcional |
| --- | --- | --- |
| Ping Federate | • Host<br>• Porta<br>• Banco de dados<br>• IAM<br>• plugin_name<br>• UID<br>• Senha<br>• IdP_Host<br>• IdP_Port | • ClusterID<br>• Região<br>• AutoCreate<br>• EndpointUrl<br>• StsEndpointUrl<br>• Preferred_Role<br>• SSL_Insecure<br>• partner_spid<br><br>**Note**<br>ClusterID e Region (Região) deverão ser definidos em Host se eles não estiverem definidos separadam ente. |

| Método de autenticação | Obrigatório | Opcional |
| --- | --- | --- |
| Azure AD do navegador | • Host<br>• Porta<br>• Banco de dados<br>• IAM<br>• plugin_name<br>• IdP_Tenant<br>• Client_ID<br>• UID | • ClusterID<br>• Região<br>• AutoCreate<br>• EndpointUrl<br>• StsEndpointUrl<br>• Preferred_Role<br>• dbgroups_filter<br>• IdP_Response_Timeout<br>• listen_port<br><br>**Note**<br>ClusterID e Region (Região) deverão ser definidos em Host se eles não estiverem definidos separadam ente. |

| Método de autenticação | Obrigatório | Opcional |
| --- | --- | --- |
| SAML do navegador | • Host<br>• Porta<br>• Banco de dados<br>• IAM<br>• plugin_name<br>• login_url<br>• UID | • ClusterID<br>• Região<br>• AutoCreate<br>• EndpointUrl<br>• StsEndpointUrl<br>• Preferred_Role<br>• dbgroups_filter<br>• IdP_Response_Timeout<br>• listen_port<br><br>**Note**<br>ClusterID e Region (Região) deverão ser definidos em Host se eles não estiverem definidos separadam ente. |
| Perfil de autorização | • Host<br>• Porta<br>• Banco de dados<br>• AccessKeyID<br>• SecretAccessKey | |

| Método de autenticação | Obrigatório | Opcional |
| --- | --- | --- |
| Azure AD OAUTH2 do navegador | • Host<br>• Porta<br>• Banco de dados<br>• IAM<br>• plugin_name<br>• IdP_Tenant<br>• Client_ID<br>• UID | • ClusterID<br>• Região<br>• EndpointUrl<br>• IdP_Response_Timeout<br>• listen_port<br>• scope<br>• provider_name<br><br>**Note**<br>ClusterID e Region (Região) deverão ser definidos em Host se eles não estiverem definidos separadam ente. |

Utilização de um serviço de credenciais externas

Além do suporte interno para AD FS, Azure AD e Okta, a versão Windows do driver ODBC do Amazon Redshift também é compatível com outros serviços de credenciais. O driver pode autenticar conexões usando qualquer plug-in de provedor de credenciais baseado em SAML de sua escolha.

Como configurar um serviço de credenciais externas no Windows:

1. Crie um perfil do IAM que especifique o plug-in do provedor de credenciais e outros parâmetros de autenticação conforme necessário. O perfil deve ser codificado em ASCII e deve conter o seguinte par de valores-chave, em que `PluginPath` é o caminho completo para o aplicativo do plugin:

   ```
   plugin_name = PluginPath
   ```

   Por exemplo:

```
plugin_name = C:\Users\kjson\myapp\CredServiceApp.exe
```

Para obter informações sobre como criar um perfil, consulte Usar um perfil de configuração no Guia de gerenciamento de clusters do Amazon Redshift.

2. Configure o driver para usar esse perfil. O driver detecta e usa as configurações de autenticação especificadas no perfil.

### Conversão de tipos de dados

O driver ODBC do Amazon Redshift versão 2.x é compatível com muitos formatos de dados comuns, convertendo entre tipos de dados do Amazon Redshift, SQL e Java.

A tabela a seguir lista os mapeamentos de tipo de dados compatíveis.

| Tipo do Amazon Redshift | Tipo SQL |
|---|---|
| BIGINT | SQL_BIGINT |
| BOOLEAN | SQL_BIT |
| CHAR | SQL_CHAR |
| DATA | SQL_TYPE_DATE |
| DECIMAL | SQL_NUMERIC |
| DOUBLE PRECISION | SQL_DOUBLE |
| GEOGRAPHY | SQL_ LONGVARBINARY |
| GEOMETRY | SQL_ LONGVARBINARY |
| INTEGER | SQL_INTEGER |
| REAL | SQL_REAL |
| SMALLINT | SQL_SMALLINT |
| SUPER | SQL_LONGVARCHAR |

| Tipo do Amazon Redshift | Tipo SQL |
|---|---|
| TEXT | SQL_LONGVARCHAR |
| TIME | SQL_TYPE_TIME |
| TIMETZ | SQL_TYPE_TIME |
| TIMESTAMP | SQL_TYPE_ TIMESTAMP |
| TIMESTAMPTZ | SQL_TYPE_ TIMESTAMP |
| VARBYTE | SQL_LONGVARBINARY |
| VARCHAR | SQL_VARCHAR |

Configuração das opções do driver ODBC

É possível usar opções de configuração de driver para controlar o comportamento do driver ODBC Amazon Redshift. As opções do driver não diferenciam letras maiúsculas de minúsculas.

No Microsoft Windows, você normalmente define as opções de driver ao configurar um nome de fonte de dados (DSN). Também é possível definir as opções de driver na string de conexão estabelecendo a conexão de forma programática ou adicionando/alterando as chaves de registro em `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\`*`your_DSN`*. Para obter mais informações sobre a configuração de um DSN, consulte Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows.

No Linux, defina as opções de configuração do driver nos arquivos `odbc.ini` e `amazon.redshiftodbc.ini`, conforme descrito em Use um gerenciador de driver ODBC para configurar o driver nos sistemas operacionais Linux e macOS X. As opções de configuração definidas em um arquivo `amazon.redshiftodbc.ini` aplicam-se a todas as conexões. Em contrapartida, as opções de configuração definidas em um arquivo `odbc.ini` são específicas de uma conexão. As opções de configuração definidas em `odbc.ini` têm precedência sobre as opções de configuração definidas em `amazon.redshiftodbc.ini`.

Veja a seguir descrições para as opções que podem ser especificadas para o driver ODBC do Amazon Redshift versão 2.x:

AccessKeyID

- Valor padrão: nenhum
- Tipo de dados – String

A chave de acesso do IAM para o usuário ou função. Se definir esse parâmetro, você também deverá especificar SecretAccessKey.

Esse parâmetro é opcional.

app_id

- Valor padrão – Nenhum
- Tipo de dados – String

O ID exclusivo fornecido pela OKTA associado à sua aplicação Amazon Redshift.

Esse parâmetro é opcional.

app_name

- Valor padrão – Nenhum
- Tipo de dados – String

O nome da aplicação Okta que você usa para autenticar a conexão com o Amazon Redshift.

Esse parâmetro é opcional.

AuthProfile

- Valor padrão – Nenhum
- Tipo de dados – String

O perfil de autenticação usado para gerenciar as configurações de conexão. Se definir esse parâmetro, você também deverá configurar AccessKeyID e SecretAccessKey.

Esse parâmetro é opcional.

AuthType

- Valor padrão: padrão
- Tipo de dados – String

Esta opção especifica o modo de autenticação que o driver usa quando você configura um DSN usando a caixa de diálogo ODBC Driver DSN Setup (Configuração de DSN do driver ODBC) do Amazon Redshift:

- Padrão: autenticação padrão usando seu nome de usuário e senha do Amazon Redshift.
- Perfil da AWS: autenticação do IAM usando um perfil.
- Credenciais do IAM da AWS: autenticação do IAM usando credenciais do IAM.
- Provedor de identidades: AD FS: autenticação do IAM usando os Serviços de Federação do Active Directory (AD FS).
- Provedor de identidades (plug-in de autenticação): um plug-in de autorização que aceita um token do centro de identidade (IdC) ou tokens de identidade baseados em JSON (JWT) do OpenID Connect (OIDC) de qualquer provedor de identidades da web vinculado ao IdC.
- Provedor de identidades: Azure AD: autenticação do IAM usando um portal do Azure AD.
- Provedor de identidades: JWT: autenticação do IAM usando um JSON Web Token (JWT).
- Provedor de identidades: Okta: autenticação do IAM usando Okta.
- Provedor de identidade: PingFederate: autenticação do IAM usando PingFederate.

Essa opção está disponível somente quando você configura um DSN usando a caixa de diálogo ODBC Driver DSN Setup (Configuração de DSN do driver ODBC) do Amazon Redshift no driver do Windows. Quando você configura uma conexão usando uma string de conexão ou uma máquina que não seja Windows, o driver determina automaticamente se deve usar Padrão, Perfil da AWS ou Autenticação de Credenciais de IAM da AWS com base em suas credenciais especificadas. Para usar um provedor de identidades, você deve configurar a propriedade plugin_name.

Esse parâmetro é obrigatório.

AutoCreate

- Valor padrão: 0
- Tipo de dados: booleano

Um booleano especificando se o driver cria um novo usuário quando o usuário especificado não existe.

- 1 | TRUE: se o usuário especificado pelo UID não existir, o driver criará um novo usuário.
- 0 | FALSE: o driver não criará um novo usuário. Se o usuário especificado não existir, a autenticação falhará.

Esse parâmetro é opcional.

CaFile

- Valor padrão – Nenhum
- Tipo de dados – String

O caminho do arquivo para o arquivo de certificado da CA usado para algumas formas de autenticação do IAM.

Esse parâmetro está disponível apenas no Linux.

Esse parâmetro é opcional.

client_id

- Valor padrão – Nenhum
- Tipo de dados – String

O ID do cliente associado ao aplicativo Amazon Redshift no Azure AD.

Esse parâmetro é necessário se autenticar por meio do serviço Azure AD.

client_ secret

- Valor padrão – Nenhum
- Tipo de dados – String

A chave secreta associada à sua aplicação Amazon Redshift no Azure AD.

Esse parâmetro é necessário se autenticar por meio do serviço Azure AD.

ClusterId

- Valor padrão – Nenhum
- Tipo de dados – String

O nome do cluster do Amazon Redshift ao qual você deseja se conectar. Ele é usado para autenticação do IAM. O ID do cluster não está especificado no parâmetro Server (Servidor).

Esse parâmetro é opcional.

compression

- Valor padrão: desativado
- Tipo de dados – String

O método de compactação usado na comunicação via protocolo com fio entre o servidor do Amazon Redshift e o cliente ou o driver.

Especifique os seguintes valores:

- lz4: define o método de compactação usado na comunicação via protocolo com fio com o Amazon Redshift como `lz4`.
- zstd: define o método de compactação usado na comunicação via protocolo com fio com o Amazon Redshift como `zstd`.
- off: não usa a compactação na comunicação via protocolo com fio com o Amazon Redshift.

Esse parâmetro é opcional.

Banco de dados

- Valor padrão – Nenhum
- Tipo de dados – String

O nome do banco de dados do Amazon Redshift que você deseja acessar.

Esse parâmetro é obrigatório.

DatabaseMetadataCurrentDbOnly

- Valor padrão - 1
- Tipo de dados: booleano

Um booleano especificando se o driver retorna metadados de vários bancos de dados e clusters.

- 1 | TRUE: o driver só retorna metadados do banco de dados atual.
- 0 | FALSE. O driver retorna metadados de vários bancos de dados e clusters do Amazon Redshift.

Esse parâmetro é opcional.

dbgroups_filter

- Valor padrão – Nenhum
- Tipo de dados – String

A expressão regular que você pode especificar para filtrar DbGroups recebidos da resposta SAML para o Amazon Redshift ao usar os tipos de autenticação Azure, Azure do navegador e SAML do navegador.

Esse parâmetro é opcional.

Driver

- Valor padrão - Driver ODBC do Amazon Redshift (x64)
- Tipo de dados – String

O nome do driver. O único valor com suporte é Driver ODBC do Amazon Redshift (x64).

Esse parâmetro será obrigatório se você não configurar o DSN.

DSN

- Valor padrão – Nenhum
- Tipo de dados – String

O nome da fonte de dados do driver. O aplicativo especifica o DSN na API SQLDriverConnect.

Esse parâmetro será obrigatório se você não configurar o Driver.

EndpointUrl

- Valor padrão – Nenhum
- Tipo de dados – String

O endpoint substituto usado para se comunicar com o Amazon Redshift Coral Service para autenticação do IAM.

Esse parâmetro é opcional.

ForceLowercase

- Valor padrão: 0
- Tipo de dados: booleano

Um booliano que especifica se o driver coloca em letras minúsculas todos os DbGroups enviados do provedor de identidades para o Amazon Redshift ao usar a autenticação única.

- 1 | TRUE: o driver coloca em letras minúsculas todos os DbGroups que são enviados do provedor de identidades.
- 0 | FALSE: o driver não altera os DbGroups.

Esse parâmetro é opcional.

group_federation

- Valor padrão: 0
- Tipo de dados: booleano

Um booliano que especifica se a API `getClusterCredentialsWithIAM` é usada para obter credenciais temporárias de cluster em clusters provisionados. Essa opção permite que os usuários do IAM se integrem aos perfis do banco de dados do Redshift em clusters provisionados. Essa opção não se aplica a namespaces do Redshift sem servidor.

- 1 | TRUE: o driver usa a API `getClusterCredentialsWithIAM` para obter credenciais temporárias de cluster em clusters provisionados.

- 0 | FALSE: o driver usa a API `getClusterCredentials` padrão para obter credenciais temporárias de cluster em clusters provisionados.

Esse parâmetro é opcional.

https_proxy_host

- Valor padrão – Nenhum
- Tipo de dados – String

O nome do host ou endereço IP do servidor de proxy por meio do qual você deseja transmitir processos de autenticação do IAM.

Esse parâmetro é opcional.

https_proxy_password

- Valor padrão – Nenhum
- Tipo de dados – String

A senha que você utiliza para acessar o servidor proxy. Ele é usado para autenticação do IAM.

Esse parâmetro é opcional.

https://proxy_port

- Valor padrão – Nenhum
- Tipo de dados: inteiro

O número da porta que o servidor proxy usa para escutar as conexões do cliente. Ele é usado para autenticação do IAM.

Esse parâmetro é opcional.

https_proxy_username

- Valor padrão – Nenhum
- Tipo de dados – String

O nome de usuário que você usa para acessar o servidor de proxy. Ele é usado para autenticação do IAM.

Esse parâmetro é opcional.

IAM

- Valor padrão: 0
- Tipo de dados: booleano

Um booleano especificando se o driver usa um método de autenticação do IAM para autenticar a conexão.

- 1 | TRUE: o driver usa um dos métodos de autenticação do IAM (usando uma chave de acesso e um par de chaves secretas, um perfil ou um serviço de credenciais).
- 0 | FALSE. O driver usa autenticação padrão (usando o nome de usuário e a senha do banco de dados).

Esse parâmetro é opcional.

identity_namespace

- Valor padrão – Nenhum
- Tipo de dados – String

O namespace da identidade a ser utilizado durante a autenticação usando IdpTokenAuthPlugin. Isso ajuda o Redshift a determinar qual instância do IAM Identity Center usar.

Se houver apenas uma instância do IAM Identity Center existente ou se o namespace da identidade padrão estiver definido, esse parâmetro será opcional; do contrário, ele será necessário.

idp_host

- Valor padrão – Nenhum
- Tipo de dados – String

O host IdP (provedor de identidades) que você está usando para autenticar no Amazon Redshift.

Esse parâmetro é opcional.

idp_port

- Valor padrão – Nenhum
- Tipo de dados: inteiro

A porta para um IdP (provedor de identidades) que você está usando para autenticar no Amazon Redshift. Dependendo da porta selecionada ao criar, modificar ou migrar o cluster, permita o acesso à porta selecionada.

Esse parâmetro é opcional.

idp_response_timeout

- Valor padrão – 120
- Tipo de dados — Inteiro

Quantos segundos o driver aguarda pela resposta SAML do provedor de identidades ao usar os serviços SAML ou Azure AD por meio de um plug-in de navegador.

Esse parâmetro é opcional.

idp_tenant

- Valor padrão – Nenhum
- Tipo de dados – String

O ID do locatário Azure AD associado à sua aplicação Amazon Redshift.

Esse parâmetro é necessário se autenticar por meio do serviço Azure AD.

idp_use_https_proxy

- Valor padrão: 0
- Tipo de dados: booleano

Um booleano especificando se o driver passa os processos de autenticação para provedores de identidade (IdP) por meio de um servidor de proxy.

- 1 | TRUE: o driver transmite processos de autenticação do IdP por meio de um servidor de proxy.
- 0 | FALSE. O driver não transmite processos de autenticação do IdP por meio de um servidor de proxy.

Esse parâmetro é opcional.

InstanceProfile

- Valor padrão: 0
- Tipo de dados: booleano

Um booleano especificando se o driver usa o perfil de instância do Amazon EC2, quando configurado, para usar um perfil para autenticação.

- 1 | TRUE: o driver usa o perfil de instância do Amazon EC2.
- 0 | FALSE. Em vez disso, o driver usa o perfil de funções encadeadas especificado pela opção Nome do perfil (Profile (Perfil)).

Esse parâmetro é opcional.

KeepAlive

- Valor padrão - 1
- Tipo de dados: booleano

Um booleano que especifica se o driver usa keepalives TCP para evitar que o tempo limite das conexões se esgote.

- 1 | TRUE: o driver usa keepalives TCP para evitar que o tempo limite das conexões se esgote.
- 0 | FALSE. O driver não usa keepalives TCP.

Esse parâmetro é opcional.

KeepAliveCount

- Valor padrão: 0

- Tipo de dados — Inteiro

O número de pacotes de keepalive de TCP que podem ser perdidos antes que a conexão seja considerada interrompida. Quando esse parâmetro está definido como 0, o driver usa o sistema padrão para essa configuração.

Esse parâmetro é opcional.

KeepAliveInterval

- Valor padrão: 0
- Tipo de dados — Inteiro

O número de segundos entre cada retransmissão de keepalive de TCP. Quando esse parâmetro está definido como 0, o driver usa o sistema padrão para essa configuração.

Esse parâmetro é opcional.

KeepAliveTime

- Valor padrão: 0
- Tipo de dados — Inteiro

O número de segundos de inatividade antes que o driver envie um pacote de manutenções de atividade de TCP. Quando esse parâmetro está definido como 0, o driver usa o sistema padrão para essa configuração.

Esse parâmetro é opcional.

listen_port

- Valor padrão - 7890
- Tipo de dados: inteiro

A porta que o driver usa para receber a resposta SAML do provedor de identidades ao usar os serviços SAML ou Azure AD por meio de um plug-in de navegador.

Esse parâmetro é opcional.

login_url

- Valor padrão – Nenhum
- Tipo de dados – String

A URL do recurso no site do provedor de identidades ao usar o plug-in SAML de navegador genérico.

Esse parâmetro é necessário se autenticar com os serviços SAML ou Azure AD por meio de um plug-in de navegador.

loginToRp

- Valor padrão - urn:amazon:webservices
- Tipo de dados – String

A relação de confiança de parte confiável que você deseja usar para o tipo de autenticação do AD FS.

Essa string é opcional.

LogLevel

- Valor padrão: 0
- Tipo de dados — Inteiro

Use essa propriedade para habilitar ou desabilitar o registro em log no driver e especificar a quantidade de detalhes incluídos nos arquivos de log. Recomendamos que você ative o registro em log apenas por tempo suficiente para capturar um problema, pois o registro em log diminui o desempenho e pode consumir uma grande quantidade de espaço em disco.

Define a propriedade com um dos seguintes valores:

- 0: OFF. Desative todos os registros em log.
- 1: ERROR. Registra em log eventos de erro que podem permitir que o driver continue em execução mas produza um erro.
- 2: API_CALL. Registra em log chamadas de função da API ODBC com valores de argumento de função.

- 3: INFO. Registra em log informações gerais que descrevem o andamento do driver.
- 4: MSG_PROTOCOL. Registra em log informações detalhadas do protocolo de mensagens do driver.
- 5: DEBUG. Registra em log todas as atividades do driver
- 6: DEBUG_APPEND. Continue anexando registros em log para todas as atividades do driver.

Quando o registro em log está habilitado, o driver produz os seguintes arquivos de log no local especificado na propriedade LogPath:

- Um arquivo `redshift_odbc.log.1` que registra em log a atividade do driver que ocorre durante o handshake de uma conexão.
- Um arquivo `redshift_odbc.log` para todas as atividades do driver depois que uma conexão é estabelecida com o banco de dados.

Esse parâmetro é opcional.

LogPath

- Valor padrão - O diretório TEMP específico do sistema operacional
- Tipo de dados – String

O caminho completo para a pasta onde o driver salva arquivos de log quando LogLevel é maior que 0.

Esse parâmetro é opcional.

Min_TLS

- Valor padrão: o valor mínimo.
- Tipo de dados – String

A versão mínima do TLS/SSL que o driver permite que o datastore use para criptografar conexões. Por exemplo, se o TLS 1.3 for especificado, o TLS 1.2 não poderá ser usado para criptografar conexões.

Min_TLS aceita os seguintes valores:

- 1.2: A conexão deve usar pelo menos TLS 1.2. Essa é a versão mínima de TLS necessária para conexões do Amazon Redshift.
- 1.3: a conexão deve usar pelo menos TLS 1.3. Recomendamos o TLS 1.3.

Esse parâmetro é opcional.

partner_spid

- Valor padrão – Nenhum
- Tipo de dados – String

O valor SPID (ID do provedor de serviços) do parceiro a ser usado ao autenticar a conexão usando o serviço PingFederate.

Esse parâmetro é opcional.

Senha | PWS

- Valor padrão – Nenhum
- Tipo de dados – String

A senha correspondente ao nome de usuário do banco de dados que você forneceu no campo Usuário (UID | Usuário | LogonID).

Esse parâmetro é opcional.

plugin_name

- Valor padrão – Nenhum
- Tipo de dados – String

O nome do plug-in do provedor de credenciais que você deseja usar para autenticação.

Os valores a seguir são aceitos:

- `ADFS`: use os serviços de federação do Active Directory para autenticação.
- `AzureAD`: use o Serviço Microsoft Azure Active Directory (AD) para autenticação.

- `BrowserAzureAD`: use um plug-in de navegador para o Serviço Microsoft Azure Active Directory (AD) para autenticação.
- `BrowserSAML`: use um plug-in do navegador para serviços SAML como Okta ou Ping para autenticação.
- `IdpTokenAuthPlugin`: um plug-in de autorização que aceita um token do centro de identidade (IdC) ou tokens de identidade baseados em JSON (JWT) do OpenID Connect (OIDC) de qualquer provedor de identidades da web vinculado ao IdC.
- `JWT`: use um JSON Web Token (JWT) para autenticação.
- `Ping`: use o serviço PingFederate para autenticação.
- `Okta`: use o serviço Okta para autenticação.

Esse parâmetro é opcional.

Porta | PortNumber

- Valor padrão - 5439
- Tipo de dados: inteiro

O número da porta TCP que o servidor Amazon Redshift usa para escutar as conexões do cliente.

Esse parâmetro é opcional.

preferred_role

- Valor padrão – Nenhum
- Tipo de dados – String

A função que você deseja assumir durante a conexão com o Amazon Redshift. Ele é usado para autenticação do IAM.

Esse parâmetro é opcional.

Perfil

- Valor padrão – Nenhum
- Tipo de dados – String

O nome do perfil da AWS de usuário usado para autenticar no Amazon Redshift.

- Se o parâmetro Use Instance Profile (a propriedade InstanceProfile) for definido como 1 | TRUE, essa configuração terá precedência e o driver usará o perfil de instância do Amazon EC2.
- O local padrão do arquivo de credenciais que contém perfis é `~/.aws/Credentials`. O ambiente `AWS_SHARED_CREDENTIALS_FILE` pode ser usado para apontar para um arquivo de credenciais diferente.

Esse parâmetro é opcional.

provider_name

- Valor padrão – Nenhum
- Tipo de dados – String

O provedor de autenticação criado pelo usuário usando a consulta CREATE IDENTITY PROVIDER. Ele é usado na autenticação nativa do Amazon Redshift.

Esse parâmetro é opcional.

ProxyHost

- Valor padrão – Nenhum
- Tipo de dados – String

O nome do host ou endereço IP do servidor de proxy ao qual você quer se conectar.

Esse parâmetro é opcional.

ProxyPort

- Valor padrão – Nenhum
- Tipo de dados: inteiro

O número da porta que o servidor proxy usa para escutar as conexões do cliente.

Esse parâmetro é opcional.

ProxyPwd

- Valor padrão – Nenhum
- Tipo de dados – String

A senha que você utiliza para acessar o servidor proxy.

Esse parâmetro é opcional.

ProxyUid

- Valor padrão – Nenhum
- Tipo de dados – String

O nome de usuário que você usa para acessar o servidor de proxy.

Esse parâmetro é opcional.

ReadOnly

- Valor padrão: 0
- Tipo de dados: booleano

Um booleano especificando se o driver está em modo somente leitura.

- 1 | TRUE: a conexão está no modo somente leitura e não pode gravar no datastore.
- 0 | FALSE: a conexão não está no modo somente leitura e pode gravar no datastore.

Esse parâmetro é opcional.

região

- Valor padrão – Nenhum
- Tipo de dados – String

Substitua AWS pela região em que seu cluster está localizado.

Esse parâmetro é opcional.

SecretAccessKey

- Valor padrão – Nenhum
- Tipo de dados – String

A chave secreta do IAM para o usuário ou função. Se definir esse parâmetro, você também deverá configurar AccessKeyID.

Esse parâmetro é opcional.

SessionToken

- Valor padrão – Nenhum
- Tipo de dados – String

O token temporário de sessão do IAM associado ao perfil do IAM que você está usando para autenticar.

Esse parâmetro é opcional.

Servidor | HostName | Host

- Valor padrão – Nenhum
- Tipo de dados – String

O servidor do endpoint para conectar-se.

Esse parâmetro é obrigatório.

ssl_insecure

- Valor padrão: 0
- Tipo de dados: booleano

Um booleano especificando se o driver verifica a autenticidade do certificado do servidor IdP.

- 1 | TRUE: o driver não verifica a autenticidade do certificado do servidor IDP.
- 0 | FALSE: o driver verifica a autenticidade do certificado do servidor idP.

Esse parâmetro é opcional.

SSLMode

- Valor padrão: `verify-ca`
- Tipo de dados – String

O modo de verificação do certificado SSL para usar ao se conectar ao Amazon Redshift. Os seguintes valores são possíveis:

- `verify-full`: Conectar somente usando SSL, uma autoridade de certificação confiável e um nome de servidor que corresponda ao certificado.
- `verify-ca`: Conectar somente usando SSL e uma autoridade de certificação confiável.
- `require`: Conectar somente usando SSL.
- `prefer`: Conectar usando SSL, se disponível. Caso contrário, conectar sem usar SSL.
- `allow`: por padrão, conectar sem usar SSL. Se o servidor exigir conexões SSL, use SSL.
- `disable`: Conectar sem usar SSL.

Esse parâmetro é opcional.

StsConnectionTimeout

- Valor padrão: 0
- Tipo de dados — Inteiro

O tempo máximo de espera para conexões do IAM, em segundos. Se definido como 0 ou não especificado, o driver espera 60 segundos para cada chamada AWS STS.

Esse parâmetro é opcional.

StsEndpointUrl

- Valor padrão – Nenhum
- Tipo de dados – String

Essa opção especifica o endpoint de substituição usado para se comunicar com o AWS Security Token Service (AWS STS).

Esse parâmetro é opcional.

UID | Usuário | LogonID

- Valor padrão – Nenhum
- Tipo de dados – String

O nome de usuário que você usa para acessar o servidor do Amazon Redshift.

Esse parâmetro será necessário se você usar autenticação de banco de dados.

web_identity_token

- Valor padrão – Nenhum
- Tipo de dados – String

O token OAUTH fornecido pelo provedor de identidades. Ele é usado no plugin JWT.

Esse parâmetro será necessário se você definir o parâmetro plugin_name como BasicJwtCredentialsProvider.

Versões anteriores do driver ODBC

Baixe uma versão anterior do driver ODBC versão 2.x do Amazon Redshift somente se sua ferramenta exigir uma versão específica do driver.

Usar versões anteriores do driver ODBC para o Microsoft Windows

A seguir estão as versões 2.x anteriores do driver ODBC do Amazon Redshift para Microsoft Windows:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/AmazonRedshiftODBC64-2.0.1.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/AmazonRedshiftODBC64-2.0.0.11.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/AmazonRedshiftODBC64-2.0.0.9.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/AmazonRedshiftODBC64-2.0.0.8.msi

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/AmazonRedshiftODBC64-2.0.0.7.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/AmazonRedshiftODBC64-2.0.0.6.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/AmazonRedshiftODBC64-2.0.0.5.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/AmazonRedshiftODBC64-2.0.0.3.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/AmazonRedshiftODBC64-2.0.0.1.msi

Usar versões anteriores do driver ODBC para Linux

A seguir estão as versões 2.x anteriores do driver ODBC do Amazon Redshift para Linux:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/AmazonRedshiftODBC-64-bit-2.0.1.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/AmazonRedshiftODBC-64-bit-2.0.0.11.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/AmazonRedshiftODBC-64-bit-2.0.0.9.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/AmazonRedshiftODBC-64-bit-2.0.0.8.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/AmazonRedshiftODBC-64-bit-2.0.0.7.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/AmazonRedshiftODBC-64-bit-2.0.0.6.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/AmazonRedshiftODBC-64-bit-2.0.0.5.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/AmazonRedshiftODBC-64-bit-2.0.0.3.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/AmazonRedshiftODBC-64-bit-2.0.0.1.x86_64.rpm

# Configurar uma conexão ODBC

Você pode usar uma conexão ODBC para se conectar ao seu cluster Amazon Redshift a partir de muitas ferramentas e aplicações de cliente SQL de terceiros. Para fazer isso, configure a conexão em seu computador cliente ou instância do Amazon EC2. Se sua ferramenta cliente oferece suporte ao JDBC, você pode optar por usar esse tipo de conexão em vez de usar o ODBC, devido à facilidade de configuração que o JDBC oferece. Contudo, se sua ferramenta cliente não oferece suporte ao JDBC, siga as etapas nesta seção para configurar uma conexão ODBC.

O Amazon Redshift fornece drivers ODBC 64 bits para sistemas operacionais Linux, Windows e macOS X. Os drivers ODBC de 32 bits foram descontinuados. Outras atualizações não serão lançadas, exceto para patches de segurança urgentes.

Para obter as informações mais recentes sobre a funcionalidade e os pré-requisitos do driver ODBC, consulte as Notas de release do driver ODBC do Amazon Redshift.

Para obter informações sobre a instalação e a configuração de drivers ODBC do Amazon Redshift, consulte Guia de instalação e configuração do conector ODBC do Amazon Redshift.

Se quiser usar uma conexão ODBC, siga as etapas a seguir.

Tópicos


- Obtenção do URL do ODBC para o cluster
- Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows
- Instalar o driver ODBC do Amazon Redshift no Linux
- Instalar o driver ODBC do Amazon Redshift no macOS X
- Use um gerenciador de driver ODBC para configurar o driver nos sistemas operacionais Linux e macOS X
- Configurar as opções do driver ODBC
- Versões anteriores do driver ODBC


## Obtenção do URL do ODBC para o cluster

O Amazon Redshift exibe o URL do ODBC para o cluster no console do Amazon Redshift. Este URL contém as informações para a configuração da conexão entre o computador cliente e o banco de dados.

O URL do ODBC tem o seguinte formato:
`Driver={driver};Server=endpoint;Database=database_name;UID=user_name;PWD=passwor`

Os campos do formato mostrado anteriormente têm os seguintes valores.

| Campo | Valor |
|---|---|
| `Driver` | O nome do driver ODBC de 64 bits a ser usado: Amazon Redshift (x64).<br><br>O nome do driver ODBC de 32 bits a ser usado: Amazon Redshift (x86). |
| `Server` | O endpoint do cluster Amazon Redshift. |
| `Database` | O banco de dados que você criou para o cluster. |
| `UID` | O nome do usuário de uma conta de usuário que tem a permissão para se conectar ao banco de dados. Este valor é uma permissão do banco de dados, não uma permissão do Amazon Redshift, embora você possa usar a conta de usuário administrador que você configurou quando iniciou o cluster. |
| `PWD` | A senha da conta de usuário para se conectar ao banco de dados. |
| `Port` | O número da porta usado quando você iniciou o cluster. Se você tem um firewall, certifique-se de que essa porta está aberta para uso. |

Os campos nas tabelas anteriores podem conter os seguintes caracteres especiais:

```
[]{}(),;?*=!@
```

Se você usar esses caracteres especiais, deverá colocar o valor entre chaves. Por exemplo, o valor de senha `Your;password123` em uma string de conexão é representado como `PWD={Your;password123};`.

Como os pares `Field=value` são separados por ponto e vírgula, a combinação de `}` e `;` com qualquer número de espaços entre eles é considerada o fim de um par `Field={value};`. Recomendamos que você evite a sequência `};` nos valores de campo. Por exemplo, se você definir o valor da senha como `PWD={This is a passwor} ;d};`, sua senha será `This is a passwor} ;` e o URL apresentará um erro.

Veja a seguir um exemplo de URL de 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
```

Para obter informações sobre como obter sua conexão ODBC, consulte Encontrar a string de conexão do cluster.

Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows

Requisitos do sistema

Você instala o driver ODBC do Amazon Redshift em computadores clientes que acessam um data warehouse do Amazon Redshift. Cada computador onde o driver é instalado deve atender a uma lista de requisitos mínimos do sistema. Para obter informações sobre os requisitos mínimos do sistema, consulte o Guia de instalação e configuração do conector ODBC do Amazon Redshift.

Instalação do driver do Amazon Redshift em sistemas operacionais Windows

Use o procedimento a seguir para baixar os drivers ODBC do Amazon Redshift para sistemas operacionais Windows. Use apenas um driver diferente desses se estiver executando uma aplicação de terceiros certificado para uso com o Amazon Redshift e que requer um driver específico.

Para instalar o driver ODBC do

1. Baixe uma das versões a seguir, dependendo da arquitetura de sistema usada pela aplicação ou pela ferramenta do cliente SQL:

   - Driver ODBC de 64 bits versão 1.5.9

     O nome deste driver é Amazon Redshift (x64).
   - Driver ODBC de 32 bits versão 1.4.52

     O nome deste driver é Amazon Redshift (x86). Os drivers ODBC de 32 bits foram descontinuados. Outras atualizações não serão lançadas, exceto para patches de segurança urgentes.

> **Note**
>
> Baixe o pacote MSI que correspondente à arquitetura de sistema da ferramenta do cliente ou do aplicativo SQL. Por exemplo, se a ferramenta do cliente SQL é de 64 bits, instale o driver de 64 bits.

Depois, baixe e revise o Acordo de licença do driver ODBC e JDBC do Amazon Redshift.

2. Clique duas vezes no arquivo .msi e, em seguida, siga os passos do assistente para instalar o driver.

Criação de uma entrada de DSN do sistema para uma conexão ODBC no Microsoft Windows

Depois de baixar e instalar o driver ODBC, adicione uma entrada de nome de origem dos dados (DSN) ao computador cliente ou instância do Amazon EC2. As ferramentas de cliente SQL usam essa origem dos dados para se conectar ao banco de dados do Amazon Redshift.

Recomendamos a criação de um DSN de sistema em vez de um DSN de usuário. Alguns aplicativos carregam os dados usando uma conta de usuário diferente. Esses aplicativos podem não conseguir detectar DSNs de usuário criados em outra conta de usuário.

> **Note**
>
> Para realizar a autenticação usando as credenciais do AWS Identity and Access Management (IAM) ou do provedor de identidades (IdP), serão necessárias etapas adicionais. Para obter mais informações, consulte Configurar uma conexão JDBC ou ODBC para usar credenciais do IAM.

Para obter informações sobre como criar uma entrada DSN do sistema, consulte o Guia de instalação e configuração do conector ODBC do Amazon Redshift.

Como criar uma entrada de DSN de sistema para uma conexão ODBC no Windows

1. No menu Iniciar, abra Fontes de dados ODBC.

Certifique-se de escolher o Administrador de origem dos dados ODBC que tem a mesma quantidade de bits da aplicação cliente que você está usando para se conectar ao Amazon Redshift.

2. Em ODBC Data Source Administrator (Administrador de origem dos dados ODBC), escolha a guia Drivers e localize a pasta do driver:

   - Driver ODBC do Amazon Redshift (64 bits)
   - Driver ODBC do Amazon Redshift (32 bits)

3. Selecione a guia DSN de Sistema a fim de configurar o driver para todos os usuários no computador, ou a guia DSN de Usuário a fim de configurar o driver apenas para sua conta de usuário.
4. Escolha Add. A janela Create New Data Source é exibida.
5. Escolha o driver ODBC do Amazon Redshift e, em seguida, escolha Concluir. A janela Configuração de DSN do driver ODBC do Amazon Redshift é exibida.
6. Em Connection Settings, insira as seguintes informações:

   Nome da fonte de dados

   Insira um nome para a fonte de dados. Use um nome qualquer para identificar a fonte de dados posteriormente, quando você criar a conexão com o cluster. Por exemplo, se você seguiu o Guia de conceitos básicos do Amazon Redshift, pode digitar `examplecluserdsn` para facilitar a lembrança do cluster que associa a este DSN.

   Servidor

   Especifique o endpoint do cluster do Amazon Redshift. Você pode encontrar essas informações no console do Amazon Redshift na página de detalhes do cluster. Para obter mais informações, consulte Configurar conexões no Amazon Redshift.

   Porta

   Insira o número da porta que o banco de dados usa. Use a porta que foi configurada para o cluster quando ele foi iniciado ou modificado.

   Banco de dados

   Insira o nome do banco de dados do Amazon Redshift. Se você iniciou o cluster sem especificar um nome de banco de dados, insira *dev*. Caso contrário, use o nome escolhido durante o

processo de inicialização. Se você seguiu o Guia de conceitos básicos do Amazon Redshift, insira *dev*.

7. Em Autenticação, especifique as opções de configuração para definir autenticação padrão ou do IAM. Para obter informações sobre as opções de autenticação, consulte “Configurar a autenticação no Windows” no Guia de instalação e configuração do conector ODBC Amazon Redshift.
8. Em SSL Settings, especifique um valor para:

   Autenticação SSL

   Escolha um modo para tratar o Secure Sockets Layer (SSL). Em um ambiente de teste, você pode usar `prefer`. No entanto, para ambientes de produção e quando um intercâmbio de dados seguro for necessário, use `verify-ca` ou `verify-full`. Para obter mais informações sobre como usar SSL no Windows, consulte "Configurando a verificação SSL no Windows" no Guia de instalação e configuração do conector ODBC Amazon Redshift.
9. Em Opções Adicionais, especifique opções sobre como retornar os resultados de consultas ao aplicativo ou ferramenta do cliente SQL. Para obter mais informações, consulte "Configurando opções adicionais no Windows" no Guia de instalação e configuração do conector ODBC Amazon Redshift.
10. Em Opções de Log, especifique valores para a opção de registro em log. Para obter mais informações, consulte "Configurando opções de registro em log no Windows" no Guia de instalação e configuração do conector ODBC Amazon Redshift.

    Escolha OK.
11. Em Opções de Tipo de Dados, especifique valores para os tipos de dados. Para obter mais informações, consulte "Configurando opções de tipo de dados no Windows" no Guia de instalação e configuração do conector ODBC Amazon Redshift.

    Escolha OK.
12. Escolha Testar. Se o computador cliente puder se conectar ao banco de dados Amazon Redshift, você verá a seguinte mensagem: Conexão bem-sucedida.

    Se a conexão do computador cliente com o banco de dados falhar, você pode tentar solucionar os possíveis problemas. Para obter mais informações, consulte Solução de problemas de conexão no Amazon Redshift.

13. Configure manutenções de atividade de TCP no Windows para impedir que as conexões atinjam o tempo limite. Para obter informações sobre como configurar keepalives TCP no Windows, consulte o Guia de instalação e configuração do conector ODBC Amazon Redshift.
14. Para ajudar na solução de problemas, configure o registro em log. Para obter informações sobre como configurar o registro em log no Windows, consulte o Guia de instalação e configuração do conector ODBC Amazon Redshift.

### Instalar o driver ODBC do Amazon Redshift no Linux

#### Requisitos do sistema

Você instala o driver ODBC do Amazon Redshift em computadores clientes que acessam um data warehouse do Amazon Redshift. Cada computador onde o driver é instalado deve atender a uma lista de requisitos mínimos do sistema. Para obter informações sobre os requisitos mínimos do sistema, consulte o Guia de instalação e configuração do conector ODBC do Amazon Redshift.

#### Instalação do driver do Amazon Redshift em sistemas operacionais Linux

Siga as etapas nesta seção para baixar e instalar os drivers ODBC do Amazon Redshift em uma distribuição Linux compatível. O processo de instalação instala os arquivos de driver nos seguintes diretórios:

- `/opt/amazon/redshiftodbc/lib/64` (para o driver de 64 bits)
- `/opt/amazon/redshiftodbc/ErrorMessages`
- `/opt/amazon/redshiftodbc/Setup`
- `/opt/amazon/redshiftodbc/lib/32` (para o driver de 32 bits)

#### Para instalar o driver ODBC do Amazon Redshift

1. Baixe uma das versões a seguir, dependendo da arquitetura de sistema usada pela aplicação ou pela ferramenta do cliente SQL:
   - Driver RPM de 64 bits versão 1.5.9
   - Driver Debian de 64 bits versão 1.5.9
   - Driver RPM de 32 bits versão 1.4.52
   - Driver Debian de 32 bits versão 1.4.52

O nome de cada um desses drivers é driver ODBC do Amazon Redshift. Os drivers ODBC de 32 bits foram descontinuados. Outras atualizações não serão lançadas, exceto para patches de segurança urgentes.

> **Note**
>
> Baixe o pacote que correspondente à arquitetura de sistema da ferramenta do cliente ou do aplicativo SQL. Por exemplo, se a ferramenta do cliente é de 64 bits, instale um driver de 64 bits.

Depois, baixe e revise o Acordo de licença do driver ODBC e JDBC do Amazon Redshift.

2. Navegue até o local onde você salvou o download do pacote e execute um dos comandos a seguir. Use o comando que corresponde a sua distribuição do Linux.

   - Em sistemas operacionais RHEL e CentOS , execute o comando a seguir.

     ```
     yum --nogpgcheck localinstall RPMFileName
     ```

     Substitua *RPMFileName* pelo nome do arquivo de pacote do RPM. Por exemplo, o comando a seguir demonstra a instalação do driver de 64 bits.

     ```
     yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-1.x.xx.xxxx-x.x86_64.rpm
     ```

   - Em SLES, execute o comando a seguir.

     ```
     zypper install RPMFileName
     ```

     Substitua *RPMFileName* pelo nome do arquivo de pacote do RPM. Por exemplo, o comando a seguir demonstra a instalação do driver de 64 bits.

     ```
     zypper install AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.rpm
     ```

   - Em Debian, execute o comando a seguir.

     ```
     sudo apt install ./DEBFileName.deb
     ```

Substitua *DEBFileName.deb* pelo nome do arquivo de pacote do Debian. Por exemplo, o comando a seguir demonstra a instalação do driver de 64 bits.

```
sudo apt install ./AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.deb
```

> **Important**
>
> Quando você tiver concluído a instalação dos drivers, configure-os para usar no sistema. Para obter mais informações sobre a configuração de drivers, consulte Use um gerenciador de driver ODBC para configurar o driver nos sistemas operacionais Linux e macOS X.

## Instalar o driver ODBC do Amazon Redshift no macOS X

### Requisitos do sistema

Você instala o driver em computadores clientes que acessam um data warehouse do Amazon Redshift. Cada computador onde o driver é instalado deve atender a uma lista de requisitos mínimos do sistema. Para obter informações sobre os requisitos mínimos do sistema, consulte o Guia de instalação e configuração do conector ODBC do Amazon Redshift.

### Instalar o driver ODBC do Amazon Redshift no macOS X

Siga as etapas nesta seção para baixar e instalar o driver ODBC do Amazon Redshift em uma versão compatível do macOS X. O processo de instalação instala os arquivos do driver nos seguintes diretórios:

- `/opt/amazon/redshift/lib/universal`
- `/opt/amazon/redshift/ErrorMessages`
- `/opt/amazon/redshift/Setup`

### Para instalar o driver ODBC do Amazon Redshift no macOS X

1. Se o sistema macOS X usa arquitetura Intel, baixe o driver Intel para macOS X versão 1.5.9. Se o sistema usa arquitetura ARM, baixe o driver ARM para macOS X versão 1.5.9. Em ambos os casos, o nome desse driver é driver ODBC do Amazon Redshift.

Depois, baixe e revise o Acordo de licença do driver ODBC e JDBC do Amazon Redshift.

2. Clique duas vezes em AmazonRedshiftODBC.dmg para montar a imagem do disco.
3. Clique duas vezes em AmazonRedshiftODBC.pkg para executar o instalador.
4. Siga as etapas no instalador para concluir o processo de instalação do driver. Para executar a instalação, aceite os termos do acordo de licença.

> **Important**
>
> Quando você tiver concluído a instalação do driver, configure-o para usar no sistema. Para obter mais informações sobre a configuração de drivers, consulte Use um gerenciador de driver ODBC para configurar o driver nos sistemas operacionais Linux e macOS X.

Use um gerenciador de driver ODBC para configurar o driver nos sistemas operacionais Linux e macOS X

Nos sistemas operacionais Linux e macOS X, utilize o gerenciador de driver ODBC para configurar as definições de conexão ODBC. Os gerenciadores de driver ODBC usam arquivos de configuração para definir e configurar as fontes de dados e os drivers ODBC. O gerenciador de driver ODBC que você usa depende do sistema operacional que você usa:

- Gerenciador de drivers unixODBC (para sistemas operacionais Linux)
- Gerenciador de controladores iODBC (para o sistema operacional macOS X)

Para obter mais informações sobre os gerenciadores de driver ODBC com suporte para configurar os drivers ODBC do Amazon Redshift, consulte Requisitos do sistema para sistemas operacionais Linux e Requisitos do sistema para sistemas operacionais macOS X. Consulte também “Especificar gerenciadores de drivers ODBC em máquinas que não utilizam Windows” no Guia de instalação e configuração do conector ODBC do Amazon Redshift. .

Três arquivos são necessários para configurar o driver ODBC do Amazon Redshift: `amazon.redshiftodbc.ini`, `odbc.ini` e `odbcinst.ini`.

Se você fez a instalação no local padrão, o arquivo de configuração `amazon.redshiftodbc.ini` estará localizado em um dos seguintes diretórios:

- /opt/amazon/redshiftodbc/lib/64 (para o driver de 64 bits em sistemas operacionais Linux)
- /opt/amazon/redshiftodbc/lib/32 (para o driver de 32 bits em sistemas operacionais Linux)
- /opt/amazon/redshift/lib (para o driver em macOS X)

Além disso, em /opt/amazon/redshiftodbc/Setup no Linux ou /opt/amazon/redshift/Setup no macOS X, há arquivos odbc.ini e odbcinst.ini de exemplo. Você pode usar esses arquivos como exemplos para configurar o driver ODBC do Amazon Redshift e o nome da origem dos dados (DSN).

Não é recomendado o uso do diretório de instalação do driver ODBC do Amazon Redshift para os arquivos de configuração. Os arquivos de exemplo do diretório Setup devem ser usados somente para servir de modelo. Se você reinstalar o driver ODBC do Amazon Redshift posteriormente ou atualizar para uma versão mais recente, o diretório de instalação será substituído. Você perderá todas as alterações que fez nesses arquivos.

Para evitar isso, copie o arquivo amazon.redshiftodbc.ini para um diretório diferente do diretório de instalação. Se você copiar esse arquivo no diretório base do usuário, adicione um ponto (.) ao início do nome do arquivo para torná-lo um arquivo oculto.

Para os arquivos odbc.ini e odbcinst.ini, use os arquivos de configuração do diretório inicial do usuário ou crie versões em um outro diretório. Por padrão, os sistemas operacionais Linux e macOS X devem ter um arquivo odbc.ini e um odbcinst.ini no diretório inicial do usuário (/home/$USER ou ~/). Esses arquivos padrão são arquivos ocultos, o que é indicado pelo ponto (.) na frente do nome de cada arquivo. Esses arquivos são exibidos somente ao usar o sinalizador -a para listar o conteúdo do diretório.

Qualquer que seja a opção escolhida para os arquivos odbc.ini e odbcinst.ini, modifique os arquivos para adicionar as informações do driver e da configuração de DSN. Se você criar arquivos, também precisará definir as variáveis do ambiente para especificar onde esses arquivos de configuração estão localizados.

Por padrão, os gerenciadores de driver ODBC são configurados para usar versões ocultas dos arquivos de configuração odbc.ini e odbcinst.ini (chamados odbc.ini e odbcinst.ini) localizadas no diretório inicial. Eles também são configurados para usar o arquivo amazon.redshiftodbc.ini na subpasta /lib do diretório de instalação do driver. Se você armazenar esses arquivos de configuração em outro lugar, defina as variáveis de ambiente descritas

a seguir para que o gerenciador de driver possa localizar os arquivos. Para obter mais informações, consulte “Especificar os locais dos arquivos de configuração do driver” no Guia de instalação e configuração do conector ODBC do Amazon Redshift. .

Criar um nome da fonte de dados em sistemas operacionais Linux e macOS X

Ao conectar-se ao armazenamento de dados usando um nome da fonte de dados (DSN), configure o arquivo `odbc.ini` para definir DSNs. Defina as propriedades no arquivo `odbc.ini` para criar um DSN que especifique as informações de conexão para o armazenamento de dados.

Para obter informações sobre como configurar o arquivo `odbc.ini`, consulte “Criar um nome da fonte de dados em uma máquina que não usa Windows” no Guia de instalação e configuração do conector ODBC do Amazon Redshift .

Use o formato a seguir em sistemas operacionais 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
```

O exemplo a seguir mostra a configuração do odbc.ini com driver ODBC de 64 bits em sistemas operacionais Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift (x64)

[Amazon Redshift (x64)]
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

O exemplo a seguir mostra a configuração do odbc.ini com driver ODBC de 32 bits em sistemas operacionais 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
```

Use o formato a seguir em sistemas operacionais 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
```

O exemplo a seguir mostra a configuração do `odbc.ini` em sistemas operacionais 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
```

Configurar uma conexão sem DSN em sistemas operacionais Linux e macOS X

Para se conectar ao armazenamento de dados por meio de uma conexão que não tenha um DSN, defina o driver no arquivo `odbcinst.ini`. Depois, forneça uma string de conexão sem DSN no aplicativo.

Para obter informações sobre como configurar o arquivo `odbcinst.ini` nesse caso, consulte "Configurar uma conexão sem DSN em uma máquina que não usa Windows" no Guia de instalação e configuração do conector ODBC do Amazon Redshift. .

Use o formato a seguir em sistemas operacionais Linux.

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

O exemplo a seguir mostra a configuração do `odbcinst.ini` para o driver de 64 bits instalados em diretórios padrão em sistemas operacionais 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
```

O exemplo a seguir mostra a configuração do `odbcinst.ini` para o driver de 32 bits instalados em diretórios padrão em sistemas operacionais 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
```

Use o formato a seguir em sistemas operacionais macOS X.

```
[ODBC Drivers]
driver_name=Installed
```

```
...

[driver_name]
Description=driver_description
Driver=path/lib/amazonredshiftodbc.dylib

...
```

O exemplo a seguir mostra a configuração do `odbcinst.ini` para o driver instalado no diretório padrão em sistemas operacionais 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
```

Configurar variáveis de ambiente

Use o gerenciador de driver ODBC correto para carregar o driver correto. Para isso, defina a variável de ambiente do caminho da biblioteca. Para obter mais informações, consulte “Especificar gerenciadores de driver ODBC em máquinas que não usam Windows” no Guia de instalação e configuração do conector ODBC do Amazon Redshift. .

Por padrão, os gerenciadores de driver ODBC são configurados para usar versões ocultas dos arquivos de configuração `odbc.ini` e `odbcinst.ini` (chamados `odbc.ini` e `odbcinst.ini`) localizadas no diretório inicial. Eles também são configurados para usar o arquivo `amazon.redshiftodbc.ini` na subpasta `/lib` do diretório de instalação do driver. Se você armazenar esses arquivos de configuração em outro lugar, defina as variáveis de ambiente para que o gerenciador de driver possa localizar os arquivos. Para obter mais informações, consulte "Especificando os locais dos arquivos de configuração do driver" no Guia de instalação e configuração do conector ODBC Amazon Redshift.

Configurar recursos de conexão

Você pode configurar os seguintes recursos de conexão para a configuração ODBC:

- Configure o driver ODBC para fornecer credenciais e autenticar a conexão com o banco de dados do Amazon Redshift.

- Configure o driver ODBC para se conectar a um soquete habilitado com Secure Sockets Layer (SSL), se você estiver se conectando a um servidor Amazon Redshift que tenha SSL habilitado.
- Configure o driver ODBC para se conectar ao Amazon Redshift por meio de um servidor proxy.
- Configure o driver ODBC para usar um modo de processamento de consultas a fim de impedir que as consultas consumam muita memória.
- Configure o driver ODBC para transmitir processos de autenticação do IAM por meio de um servidor de proxy.
- Configure o driver ODBC para usar manutenções de atividade de TCP a fim de impedir que as conexões atinjam o tempo limite.

Para obter informações sobre esses recursos de conexão, consulte o Guia de instalação e configuração do conector ODBC do Amazon Redshift.

Configurar as opções do driver ODBC

Você pode usar opções de configuração para controlar o comportamento do driver ODBC Amazon Redshift.

No Microsoft Windows, você normalmente define as opções de driver ao configurar um nome de fonte de dados (DSN). Também é possível definir as opções de driver na string de conexão estabelecendo a conexão de forma programática ou adicionando/alterando as chaves de registro em `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\`*`your_DSN`*. Para obter mais informações sobre a configuração de um DSN, consulte Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows.

No Linux e no macOS X, defina as opções de configuração do driver nos arquivos `odbc.ini` e `amazon.redshiftodbc.ini`, conforme descrito em Use um gerenciador de driver ODBC para configurar o driver nos sistemas operacionais Linux e macOS X. As opções de configuração definidas em um arquivo `amazon.redshiftodbc.ini` aplicam-se a todas as conexões. Em contrapartida, as opções de configuração definidas em um arquivo `odbc.ini` são específicas de uma conexão. As opções de configuração definidas em `odbc.ini` têm precedência sobre as opções de configuração definidas em `amazon.redshiftodbc.ini`.

Para obter informações sobre como definir as opções de configuração do driver ODBC, consulte o Guia de instalação e configuração do conector ODBC do Amazon Redshift.

Versões anteriores do driver ODBC

Baixe uma versão anterior do driver ODBC do Amazon Redshift apenas se sua ferramenta exigir uma versão específica do driver.

Usar versões anteriores do driver ODBC para Windows

Estes são os drivers de 64 bits:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC64-1.5.7.1007.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC64-1.4.65.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC64-1.4.62.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC64-1.4.59.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC64-1.4.56.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.53.1000/AmazonRedshiftODBC64-1.4.53.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC64-1.4.52.1000.msi

Os drivers de 32 bits são descontinuados e as versões anteriores não são compatíveis.

Usar versões anteriores do driver ODBC para Linux

Estas são as versões do driver de 64 bits:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC-64-bit-1.5.7.1007-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC-64-bit-1.4.65.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC-64-bit-1.4.62.1000-1.x86_64.rpm

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-64-bit-1.4.59.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-64-bit-1.4.59.1000-1.x86_64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-64-bit-1.4.56.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-64-bit-1.4.56.1000-1.x86_64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-64-bit-1.4.52.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-64-bit-1.4.52.1000-1.x86_64.deb

Os drivers de 32 bits são descontinuados e as versões anteriores não são compatíveis.

Usar versões anteriores do driver ODBC para macOS X

A seguir estão as versões do driver ODBC do Amazon Redshift para macOS X:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC-1.5.7.1007.x86_64.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC-1.4.65.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC-1.4.62.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-1.4.59.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-1.4.56.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-1.4.52.1000.dmg

# Configurar as opções de segurança para conexões

O Amazon Redshift oferece suporte a conexões Secure Sockets Layer (SSL) para criptografar dados e certificados do servidor para validar o certificado do servidor ao qual o cliente se conecta.

## Conexão usando SSL

Para oferecer suporte a conexões SSL, o Amazon Redshift cria e instala um certificado SSL emitido AWS Certificate Manager (ACM) em cada cluster. Os certificados ACM são publicamente confiáveis pela maioria dos sistemas operacionais, navegadores da Web e clientes. Poderá ser necessário baixar um pacote de certificados, caso seus clientes ou aplicações SQL se conectarem ao Amazon Redshift usando SSL com a opção de conexão `sslmode` definida como `require`, `verify-ca` ou `verify-full`. Se o cliente precisar de um certificado, o Amazon Redshift fornecerá um certificado de pacote da seguinte forma:

- Baixe o pacote em https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt.
  - O número de soma de verificação MD5 esperado é 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - O número da soma de verificação sha256 é 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  Não use o pacote de certificados anterior localizado em `https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt`.
- Na Região da AWS da China, baixe o pacote de https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt.
  - O número de soma de verificação MD5 esperado é 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - O número da soma de verificação sha256 é 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  Não use os pacotes de certificados anteriores localizados em `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` e `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem`

> **Important**
>
> O Amazon Redshift mudou a maneira como os certificados SSL são gerenciados. Talvez seja necessário atualizar os certificados CA raiz confiáveis atuais para continuar se conectando

aos clusters por meio de SSL. Para obter mais informações, consulte Transição para certificados ACM das conexões SSL.

Por padrão, os bancos de dados de cluster aceitam tanto as conexões SSL quanto as que não utilizam SSL. Para configurar seu cluster para solicitar uma conexão SSL, configure o parâmetro `require_SSL` como `true` no parameter group que está associado ao cluster.

O Amazon Redshift oferece suporte a um modo SSL compatível com Federal Information Processing Standard (FIPS) 140-2. O modo SSL compatível com a FIPS está desativado por padrão.

> **Important**
>
> Habilite o modo SSL compatível com FIPS somente se o sistema precisar ser compatível com FIPS.

Para habilitar o modo SSL compatível com a FIPS, defina os parâmetros `use_fips_ssl` e `require_SSL` como `true` no grupo de parâmetros que está associado ao cluster. Para obter informações sobre como modificar um parameter group, consulte Grupos de parâmetros do Amazon Redshift.

O Amazon Redshift oferece suporte ao protocolo de acordo de chave Elliptic Curve Diffie—Hellman Ephemeral (ECDHE). Com o ECDHE, o cliente e o servidor têm, cada um, um par de chaves públicas/privadas de curva elíptica que é usado para estabelecer um segredo compartilhado através de um canal inseguro. Não é necessário configurar nada no Amazon Redshift para habilitar o ECDHE. Se você se conectar a partir de uma ferramenta de cliente SQL que usa ECDHE para criptografar a comunicação entre o cliente e o servidor, o Amazon Redshift usa a lista de cifras fornecida para fazer a conexão apropriada. Para obter mais informações, consulte Elliptic curve diffie—hellman na Wikipedia e Cifras no site do OpenSSL.

### Uso do SSL e dos certificados CA confiáveis no ODBC

Se você estabelecer a conexão usando os drivers ODBC mais recentes do Amazon Redshift (versão 1.3.7.1000 ou posterior), ignore esta seção. Para baixar os drivers mais recentes, consulte Configurar uma conexão ODBC.

Talvez seja necessário atualizar os certificados CA raiz confiáveis atuais para continuar se conectando aos clusters por meio de SSL. Para obter mais informações, consulte Conexão usando SSL.

Você pode verificar se o certificado baixado corresponde ao número de checksum MD5 esperado. Para isso, você pode usar o programa Md5sum em sistemas operacionais Linux ou outra ferramenta em sistemas operacionais Windows e macOS X.

Os DSNs do ODBC contêm uma configuração `sslmode` que determina como lidar com a criptografia para conexões de cliente e verificação de certificado de servidor. O Amazon Redshift oferece suporte ao seguinte valores `sslmode` da conexão do cliente:

- `disable`

  O SSL é desabilitado e a conexão não é criptografada.
- `allow`

  O SSL será usado se o servidor exigir.
- `prefer`

  O SSL será usado se o servidor for compatível. O Amazon Redshift oferece suporte ao SSL, portanto, o SSL é usado quando você define `sslmode` como `prefer`.
- `require`

  O SSL é necessário.
- `verify-ca`

  O SSL deve ser usado e o certificado de servidor deve ser verificado.
- `verify-full`

  O SSL deve ser usado. O certificado de servidor deve ser verificado, e o nome do host do servidor deve corresponder ao nome do host atribuído no certificado.

É possível determinar se o SSL é usado, e se os certificados do servidor são verificados em uma conexão entre o cliente e o servidor. Para fazer isso, você precisa revisar a configuração `sslmode` do ODBC DSN no cliente e a configuração `require_SSL` do cluster do Amazon Redshift no servidor. A tabela a seguir descreve o resultado da criptografia para várias combinações de configuração de clientes e servidores:

| sslmode (cliente) | require_SSL (servidor) | Resultado |
|---|---|---|
| `disable` | `false` | A conexão não é criptografada. |
| `disable` | `true` | A conexão não pode ser estabelecida porque o servidor exige SSL e o cliente está com o SSL desabilitado para esta conexão. |
| `allow` | `true` | A conexão é criptografada. |
| `allow` | `false` | A conexão não é criptografada. |
| `prefer` ou `require` | `true` | A conexão é criptografada. |
| `prefer` ou `require` | `false` | A conexão é criptografada. |
| `verify-ca` | `true` | A conexão é criptografada e o certificado do servidor foi verificado. |
| `verify-ca` | `false` | A conexão é criptografada e o certificado do servidor foi verificado. |
| `verify-full` | `true` | A conexão é criptografada e o certificado do servidor e o nome do host foram verificados. |
| `verify-full` | `false` | A conexão é criptografada e o certificado do servidor e o nome do host foram verificados. |

Conexão usando o certificado de servidor com o ODBC no Microsoft Windows

Se você deseja se conectar ao seu cluster usando SSL e o certificado do servidor, primeiro baixe o certificado para o seu computador cliente ou instância do Amazon EC2. Depois, configure o DSN do ODBC.

1. Baixe o pacote de autoridade de certificação do Amazon Redshift para o seu computador cliente na pasta `lib` no diretório de instalação do driver e salve o arquivo como `root.crt`. Para baixar as informações, consulte Conexão usando SSL.

2. Abra ODBC Data Source Administrator e adicione ou edite a entrada de DSN do sistema para a conexão ODBC. Em SSL Mode, selecione `verify-full`, a menos que você use um alias DNS. Se você usa um alias DNS, selecione `verify-ca`. Em seguida, escolha Salvar.

   Para obter mais informações sobre a configuração do DSN do ODBC, consulte Configurar uma conexão ODBC.

## Utilização de SSL e dos certificados de servidor em Java

O SSL fornece uma camada de segurança criptografando os dados transferidos entre o cliente e o cluster. Usar um certificado de servidor fornece uma camada extra de segurança, validando que o cluster é um cluster do Amazon Redshift. Para isso, ele verifica o certificado de servidor que é instalado automaticamente em todos os clusters provisionados. Para obter mais informações sobre como usar certificados de servidor com o JDBC, acesse Configuração do cliente na documentação do PostgreSQL.

Conexão por meio de certificados CA confiáveis em Java

> **Important**
>
> O Amazon Redshift mudou a maneira como os certificados SSL são gerenciados. Talvez seja necessário atualizar os certificados CA raiz confiáveis atuais para continuar se conectando aos clusters por meio de SSL. Para obter mais informações, consulte Conexão usando SSL.

Para se conectar por meio de certificados CA confiáveis

Você pode usar o arquivo `redshift-keytool.jar` para importar certificados CA no pacote de autoridade de certificação do Amazon Redshift para um Java TrustStore ou seu TrustStore privado.

1. Se você usa a opção `-Djavax.net.ssl.trustStore` de linha de comando Java, remova-a da linha de comando, se possível.
2. Baixe o redshift-keytool.jar.
3. Execute um destes procedimentos:

   - Para importar o pacote de autoridade de certificação do Amazon Redshift para um Java TrustStore, execute o comando a seguir.

```
java -jar redshift-keytool.jar -s
```

- Para importar o pacote de autoridade de certificação do Amazon Redshift para o seu TrustStore privado, execute o seguinte comando:

```
java -jar redshift-keytool.jar -k <your_private_trust_store> -
p <keystore_password>
```

## Transição para certificados ACM das conexões SSL

O Amazon Redshift está substituindo os certificados SSL em seus clusters por certificados AWS Certificate Manager (ACM) emitidos. O ACM é uma autoridade de certificação pública confiável pela maioria dos sistemas atuais. Talvez seja necessário atualizar os certificados CA raiz confiáveis atuais para continuar se conectando aos clusters por meio de SSL.

Essa alteração afetará você somente se todas as condições a seguir forem aplicáveis:

- Os clientes ou os aplicativos SQL se conectam aos clusters do Amazon Redshift usando o SSL com a opção de conexão `sslMode` definida como a opção de configuração `require`, `verify-ca` ou `verify-full`.
- Você não está usando os drivers ODBC ou JDBC do Amazon Redshift ou usa os drivers do Amazon Redshift anteriores ao ODBC versão 1.3.7.1000 ou JDBC versão 1.2.8.1005.

Se essa mudança afetar você nas regiões comerciais do Amazon Redshift, você deverá atualizar seus certificados CA raiz de confiança atuais antes de 23 de outubro de 2017. O Amazon Redshift fará a transição dos clusters para que usem certificados ACM até 23 de outubro de 2017. A alteração afetará muito pouco ou não afetará a performance ou a disponibilidade do cluster.

Se essa mudança afetar você nas regiões AWS GovCloud (US) (EUA), você deverá atualizar seus certificados CA raiz de confiança atuais antes de 1° de abril de 2020 para evitar a interrupção do serviço. A partir desta data, os clientes que se conectam a clusters Amazon Redshift usando conexões criptografadas SSL precisam de uma autoridade de certificação (CA) confiável adicional. Os clientes usam autoridades de certificação confiáveis para confirmar a identidade do cluster Amazon Redshift quando se conectam a ele. É necessário que você atualize os clientes e aplicativos SQL para usar um pacote de certificados atualizado que inclui a nova CA confiável.

> **Important**
>
> Nas regiões da China em 5 de janeiro de 2021, o Amazon Redshift substituirá os certificados SSL nos clusters pelos certificados AWS Certificate Manager (ACM) emitidos. Se essa alteração afetar você na região China (Pequim) ou China (Ningxia), será necessário atualizar os certificados CA raiz de confiança atuais antes de 5 de janeiro de 2021 para evitar a interrupção do serviço. A partir desta data, os clientes que se conectam a clusters Amazon Redshift usando conexões criptografadas SSL precisam de uma autoridade de certificação (CA) confiável adicional. Os clientes usam autoridades de certificação confiáveis para confirmar a identidade do cluster Amazon Redshift quando se conectam a ele. É necessário que você atualize os clientes e aplicativos SQL para usar um pacote de certificados atualizado que inclui a nova CA confiável.

- Uso dos drivers ODBC ou JDBC mais recentes do Amazon Redshift
- Uso dos drivers ODBC ou JDBC mais antigos do Amazon Redshift
- Uso de outros tipos de conexão SSL

Uso dos drivers ODBC ou JDBC mais recentes do Amazon Redshift

O método preferencial é usar os drivers ODBC ou JDBC mais recentes do Amazon Redshift. Os drivers do Amazon Redshift a partir da versão ODBC 1.3.7.1000 e da versão JDBC 1.2.8.1005 gerenciam automaticamente a transição de um certificado autoassinado do Amazon Redshift para um certificado ACM. Para baixar os drivers mais recentes, consulte Configurar uma conexão ODBC ou Configurar uma conexão para o driver JDBC versão 2.1 para o Amazon Redshift.

Se você usar o driver JDBC mais recente do Amazon Redshift, é recomendável não usar `-Djavax.net.ssl.trustStore` nas opções da JVM. Se você precisar usar `-Djavax.net.ssl.trustStore`, importe o pacote da autoridade de certificação do Redshift para a truststore indicada. Para baixar as informações, consulte Conexão usando SSL. Para obter mais informações, consulte Importar o pacote de autoridade de certificação do Amazon Redshift para um TrustStore.

Uso dos drivers ODBC ou JDBC mais antigos do Amazon Redshift

- Se o DSN ODBC for configurado com `SSLCertPath`, substitua o arquivo de certificado no caminho especificado.

- Se `SSLCertPath` não for definido, substitua o arquivo de certificado `root.crt` no local da DLL do driver.

Se você deve usar um driver JDBC do Amazon Redshift antes da versão 1.2.8.1005, siga um destes procedimentos:

- Se a string de conexão JDBC usar a opção `sslCert`, remova a opção `sslCert`. Depois, importe o pacote da autoridade de certificação do Redshift para a Java TrustStore. Para baixar as informações, consulte Conexão usando SSL. Para obter mais informações, consulte Importar o pacote de autoridade de certificação do Amazon Redshift para um TrustStore.
- Se você usa a opção `-Djavax.net.ssl.trustStore` de linha de comando Java, remova-a da linha de comando, se possível. Depois, importe o pacote da autoridade de certificação do Redshift para a Java TrustStore. Para baixar as informações, consulte Conexão usando SSL. Para obter mais informações, consulte Importar o pacote de autoridade de certificação do Amazon Redshift para um TrustStore.

Importar o pacote de autoridade de certificação do Amazon Redshift para um TrustStore

Você pode usar `redshift-keytool.jar` para importar certificados CA no pacote de autoridade de certificação do Amazon Redshift para um Java TrustStore ou seu truststore privado.

Para importar o pacote de autoridade de certificação do Amazon Redshift para um TrustStore

1. Baixe o redshift-keytool.jar.
2. Execute um destes procedimentos:

   - Para importar o pacote de autoridade de certificação do Amazon Redshift para um Java TrustStore, execute o comando a seguir.

     ```
     java -jar redshift-keytool.jar -s
     ```

   - Para importar o pacote de autoridade de certificação do Amazon Redshift para o seu TrustStore privado, execute o seguinte comando:

     ```
     java -jar redshift-keytool.jar -k <your_private_trust_store> -
     p <keystore_password>
     ```

Uso de outros tipos de conexão SSL

Siga as etapas nesta seção se você se conectar usando um dos itens a seguir:

- Driver ODBC de código aberto
- Driver JDBC de código aberto
- A interface de linha de comando Amazon Redshift RSQL
- Qualquer vinculação de linguagem baseada em libpq, como psycopg2 (Python) e ruby-pg (Ruby)

Para usar certificados ACM com outros tipos de conexão SSL:

1. Baixe o pacote de autoridade de certificação do Amazon Redshift. Para baixar as informações, consulte Conexão usando SSL.
2. Insira os certificados do pacote em seu arquivo `root.crt`.
   - Nos sistemas operacionais Linux e macOS X, o arquivo é `~/.postgresql/root.crt`.
   - No Microsoft Windows, o arquivo é `%APPDATA%\postgresql\root.crt`.

## Conexão de código e ferramentas clientes

O Amazon Redshift fornece o editor de consultas v2 do Amazon Redshift para conexão a clusters e grupos de trabalho. Para ter mais informações, consulte Consultar um banco de dados usando o editor de consultas v2 do Amazon Redshift.

Esta seção fornece algumas opções de ferramentas de terceiros para conexão. Além disso, ela descreve como estabelecer a conexão com o cluster por meio de programação.

Tópicos

- Conectar-se com o Amazon Redshift RSQL
- Conectar-se a um cluster com o Amazon Redshift RSQL
- Metacomandos do Amazon Redshift RSQL
- Variáveis do Amazon Redshift RSQL
- Códigos de erro Amazon Redshift RSQL
- Variáveis de ambiente do Amazon Redshift RSQL

# Conectar-se com o Amazon Redshift RSQL

O Amazon Redshift RSQL é um cliente de linha de comando para interagir com clusters e bancos de dados do Amazon Redshift. Você pode se conectar a um cluster do Amazon Redshift, descrever objetos de banco de dados, consultar dados e visualizar resultados de consulta em vários formatos de saída.

O Amazon Redshift RSQL oferece suporte aos recursos da ferramenta da linha de comando psql PostgreSQL com um conjunto adicional de recursos específicos para o Amazon Redshift. Incluindo o seguinte:

- É possível usar autenticação única utilizando ADFS, PingIdentity, Okta, Azure ADm ou outros provedores de identidades baseados em SAML/JWT. Você também pode usar provedores de identidade SAML baseados em navegador para autenticação multifator (MFA).
- É possível descrever propriedades ou atributos de objetos do Amazon Redshift, como chaves de distribuição de tabela, chaves de classificação de tabela, visualizações de vinculação tardia (LBVs) e views materializadas. Você também pode descrever propriedades ou atributos de tabelas externas em um catálogo do AWS Glue ou Apache Hive Metastore, bancos de dados externos no Amazon RDS for PostgreSQL, Amazon Aurora edição compatível com PostgreSQL, RDS para MySQL (pré-visualização) e Amazon Aurora edição compatível com MySQL (pré-visualização) e tabelas compartilhadas usando o compartilhamento de dados do Amazon Redshift.
- Você também pode usar comandos de fluxo de controle aprimorados, como `IF` (`\ELSEIF`, `\ELSE, \ENDIF`), `\GOTO` e `\LABEL`.

Com o modo em lote do Amazon Redshift RSQL, que executa um script passado como um parâmetro de entrada, é póssível executar scripts que contenham SQL e lógica de negócios complexa. Se você tiver data warehouses on-premises autogerenciados, poderá usar o Amazon Redshift RSQL para substituir scripts existentes de extração, transformação, carregamento (ETL) e automação, como scripts Teradata BTEQ. Usar o RSQL ajuda você a evitar a reimplementação manual de scripts em uma linguagem processual.

O Amazon Redshift RSQL está disponível para sistemas operacionais Linux, Windows e macOS X.

Para relatar problemas com o Amazon Redshift RSQL, escreva para `<redshift-rsql-support@amazon.com>`.

Tópicos

- Conceitos básicos do Amazon Redshift RSQL

- Log de alterações do Amazon Redshift RSQL

### Conceitos básicos do Amazon Redshift RSQL

Instale o Amazon Redshift RSQL em um computador com sistema operacional Linux, macOS ou Microsoft Windows.

#### Baixar o RSQL

- RPM de 64 bits do Linux: RSQL versão 1.0.8
- DMG de 64 bits do Mac OS: RSQL versão 1.0.8
- MSI de 64 bits do Windows: RSQL versão 1.0.8

Veja o log de alterações e os downloads das versões anteriores em Log de alterações do Amazon Redshift RSQL.

#### Instalar o RSQL para Linux

Siga as etapas abaixo para instalar o RSQL para Linux.

1. Instale o driver com o seguinte comando:

   ```
   sudo yum install unixODBC openssl
   ```

   O OpenSSL é necessário para as distribuições do Linux. A biblioteca OpenSSL fica localizada no repositório Linux OpenSSL do Github. Para obter mais informações sobre openssl, consulte OpenSSL.
2. Instale o driver ODBC: Instalação do driver do Amazon Redshift em sistemas operacionais Linux.
3. Copie o arquivo ini para o diretório inicial:

   ```
   cp /opt/amazon/redshiftodbc/Setup/odbc.ini ~/.odbc.ini
   ```
4. Defina as variáveis de ambiente para apontar ao local do arquivo:

   ```
   export ODBCINI=~/.odbc.ini
       export ODBCSYSINI=/opt/amazon/redshiftodbc/Setup
   ```

```
    export AMAZONREDSHIFTODBCINI=/opt/amazon/redshiftodbc/lib/64/
amazon.redshiftodbc.ini
```

Para obter mais informações sobre como configurar as variáveis de ambiente do ODBC, consulte Configurar variáveis de ambiente.

5. Agora é possível instalar o RSQL executando o comando a seguir.

```
sudo rpm -i AmazonRedshiftRsql-<version>-1.x86_64.rpm
```

Instalar o RSQL para Mac

Siga as etapas abaixo para instalar o RQL para Mac OSX.

1. Instale o driver com o seguinte comando:

```
brew install unixodbc openssl@1.1 --build-from-source
```

2. Instale o driver ODBC: Instalar o driver ODBC do Amazon Redshift no macOS X.
3. Copie o arquivo ini para o diretório inicial:

```
cp /opt/amazon/redshift/Setup/odbc.ini ~/.odbc.ini
```

4. Defina as variáveis de ambiente para apontar ao local do arquivo:

```
export ODBCINI=~/.odbc.ini
export ODBCSYSINI=/opt/amazon/redshift/Setup
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshift/lib/amazon.redshiftodbc.ini
```

Para obter mais informações sobre como configurar as variáveis de ambiente do ODBC, consulte Configurar variáveis de ambiente.

5. Defina `DYLD_LIBRARY_PATH` para a localização do seu libodbc.dylib se não estiver em `/usr/local/lib`.

```
export DYLD_LIBRARY_PATH=$DYLD_LIBRARY_PATH:/usr/local/lib
```

6. Clique duas vezes no arquivo dmg para montar a imagem do disco.
7. Clique duas vezes no arquivo pkg para executar o instalador.

8. Siga as etapas do instalador para concluir a instalação. Concorde com os termos do contrato de licença.

### Instalar o RSQL para Windows

Siga as instruções em Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows para instalar o driver. O Windows não requer um gerenciador de drivers.

O OpenSSL é necessário para o Amazon Redshift RSQL no Windows. A biblioteca OpenSSL do Windows fica localizada no repositório Linux OpenSSL do Github. Para obter mais informações sobre openssl, consulte OpenSSL.

Clique duas vezes no arquivo de download do RSQL para executar o instalador e siga as solicitações para concluir a instalação.

### Log de alterações do Amazon Redshift RSQL

#### 1.0.8 (2023-06-19)

Correções de bugs

- Corrigido um problema em que a saída era truncada com os comandos SHOW.
- Adicionado suporte a \de para descrever fluxos externos do Kinesis e tópicos do Kafka.

#### 1.0.7 (22/03/2023)

Correções de bugs

- Correção de um problema em que o RSQL não conseguia descrever visões materializadas.
- Correção do erro de permissão negada em stl_connection_log ao usar o Amazon Redshift sem servidor.
- Correção de um problema em que o RSQL processava rótulos \GOTO incorretamente.
- Correção de um problema em que mensagens SSL eram impressas no modo silencioso.
- Correção de um problema de exibição de caracteres aleatórios ao descrever procedimentos armazenados.
- Correção de um problema de impressão de mensagens ERROR/INFO duplicadas.

Novo

- O RSQL agora recebe informações de SSL diretamente do driver ODBC.

1.0.6 (21/02/2023)

Correções de bugs

- Correção de um problema em que \d gerava um erro (sintaxe de entrada inválida para inteiro: “xid”) no patch 1.0.46086 (P173) do Redshift.

Novo

- Renomeação dos arquivos de instalação para refletir a arquitetura compatível.

1.0.5 (2022-06-27)

Correções de bugs

- Envia mensagens de erro SQL para erro padrão (stderr).
- Corrigido o problema com os códigos de saída ao usar ON_ERROR_STOP. Os scripts agora terminam depois de encontrar um erro e retornam os códigos de saída corretos.
- Maxerror agora não diferencia maiúsculas de minúsculas.

Novo

- Inclusão de suporte ao driver ODBC 2.x.

1.0.4 (19-03-2022)

- Adicione suporte para a variável de ambiente RSPASSWORD. Defina uma senha para se conectar ao Amazon Redshift. Por exemplo, `.export RSPASSW0RD=TestPassw0rd`

1.0.3 (2021-12-08)

Correções de bugs

- Caixa de diálogo pop-up corrigida ao usar `\c` ou `\logon` para alternar entre bancos de dados no sistema operacional Windows.
- Corrigida a falha ao verificar informações ssl.

### Versões anteriores do Amazon Redshift RSQL

Escolha um dos links para baixar a versão do Amazon Redshift RSQL de que você precisa, com base em seu sistema operacional.

#### RPM de 64 bits do Linux

- RSQL versão 1.0.7
- RSQL versão 1.0.6
- RSQL versão 1.0.5
- RSQL versão 1.0.4
- RSQL versão 1.0.3
- RSQL versão 1.0.1

#### DMG de 64 bits do Mac

- RSQL versão 1.0.7
- RSQL versão 1.0.6
- RSQL versão 1.0.5
- RSQL versão 1.0.4
- RSQL versão 1.0.3
- RSQL versão 1.0.1

#### MSI de 64 bits do Windows

- RSQL versão 1.0.7
- RSQL versão 1.0.6
- RSQL versão 1.0.5
- RSQL versão 1.0.4

- RSQL versão 1.0.3
- RSQL versão 1.0.1

## Conectar-se a um cluster com o Amazon Redshift RSQL

Conectar-se sem um DSN

1. No console do Amazon Redshift, escolha o cluster ao qual você deseja se conectar e anote o endpoint, o banco de dados e a porta.
2. No prompt de comando, especifique as informações de conexão usando os parâmetros de linha de comando.

   ```
   rsql -h <endpoint> -U <username> -d <databasename> -p <port>
   ```

   Aqui, o seguinte se aplica:

   - *<endpoint>* é o Endpoint que você registrou na etapa anterior.
   - *<username>* é o nome do usuário com as permissões para a conexão com o cluster.
   - *<databasename>* é o Nome do banco de dados que você registrou na etapa anterior.
   - *<port>* é a porta que você registrou na etapa anterior. *<port>* é um parâmetro opcional.

   Veja a seguir um exemplo.

   ```
   rsql -h testcluster.example.amazonaws.com -U user1 -d dev -p 5439
   ```

3. No prompt da senha, digite a senha do usuário *<username>*.

   Uma resposta de conexão bem-sucedida tem a aparência a seguir.

   ```
   % 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=#
```

O comando para conectar tem os mesmos parâmetros no Linux, Mac OS e Windows.

Conectar-se usando um DSN

É possível conectar o RSQL ao Amazon Redshift usando um nome da origem dos dados (DSN) para simplificar a organização das propriedades de conexão. Para obter mais informações, consulte Configurar recursos de conexão. Este tópico inclui instruções para instalação do driver ODBC e descrições para propriedades DSN. Por exemplo, a seção Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows a seguir mostra como se conectar a um DSN usando o Windows.

Usar uma conexão DSN com uma senha

Veja a seguir um exemplo de uma configuração de conexão DSN que usa uma senha.
O padrão `<path to driver>` para Mac OSX é `/opt/amazon/redshift/lib/libamazonredshiftodbc.dylib` e para Linux é `/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
```

A saída a seguir é resultado de uma conexão bem-sucedida.

```
% 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=#
```

Usar o DSN de autenticação única

Você pode configurar um DSN para autenticação única. Veja a seguir um exemplo de configuração de conexão DSN que usa autenticação única do 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>
```

Exemplo de saída de uma conexão bem-sucedida.

```
% 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=#
```

Veja a seguir o exemplo de uma configuração de conexão DSN que usa autenticação única do 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>
```

Usar uma conexão DSN com um perfil do IAM

Você pode se conectar ao Amazon Redshift usando seu perfil do IAM configurado. O perfil do IAM deve ter privilégios para chamar `GetClusterCredentials`. O exemplo a seguir mostra as propriedades DSN a serem usadas. Os parâmetros `ClusterID` e `Region` são obrigatórios somente se o `Host` não for um endpoint fornecido pela Amazon, como `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
```

O valor da chave `Profile` é o perfil nomeado que você escolhe a partir de suas credenciais AWS da CLI. Esse exemplo mostra as credenciais do perfil chamado `default`.

```
$ cat .aws/credentials
[default]
aws_access_key_id = ASIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

Veja a seguir a resposta da conexão.

```
$ 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=>
```

Usar uma conexão DSN com um perfil da instância

Você pode se conectar ao Amazon Redshift usando seu perfil de instância do Amazon EC2. O perfil da instância deve ter privilégios para chamar `GetClusterCredentials`. Veja o exemplo abaixo para saber quais propriedades DSN serão usadas. Os parâmetros `ClusterID` e `Region` são obrigatórios somente se o `Host` não for um endpoint fornecido pela Amazon, como `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
```

Veja a seguir a resposta da conexão.

```
$ 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=>
```

Uso de uma conexão DSN com a cadeia de fornecedores de credenciais padrão

Para se conectar usando a cadeia de provedores de credenciais padrão, especifique apenas a propriedade do IAM, e o Amazon Redshift RSQL tentará adquirir credenciais na ordem descrita em Trabalho com credenciais da AWS no SDK da AWS para Java. Pelo menos um dos provedores da cadeia deve ter a permissão `GetClusterCredentials`. Isso é útil para se conectar a partir de contêineres ECS, por exemplo.

```
[iamcredentials]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
```

## Metacomandos do Amazon Redshift RSQL

Os metacomandos do Amazon Redshift RSQL retornam registros informativos sobre bancos de dados ou sobre objetos específicos do banco de dados. Os resultados podem incluir várias colunas e metadados. Outros comandos executam ações específicas. Esses comandos são precedidos por uma barra invertida.

\d[S+]

Lista tabelas criadas pelo usuário local, visualizações regulares, visualizações de vinculação tardia e visualizações materializadas.`\dS` também lista tabelas e visualizações, como `\d`, mas os objetos do sistema são incluídos nos registros retornados. O + resulta na coluna de metadados adicionais `description` para todos os objetos listados. A seguir, veja exemplos de registros retornados como resultado do comando.

```
List of relations
```

```
 schema |   name    | type  |  owner
--------+-----------+-------+---------
 public | category  | table | awsuser
 public | date      | table | awsuser
 public | event     | table | awsuser
 public | listing   | table | awsuser
 public | sales     | table | awsuser
 public | users     | table | awsuser
 public | venue     | table | awsuser
(7 rows)
```

\d[S+] NAME

Descreve uma tabela, uma visualização ou um índice. Inclui os nomes e tipos de colunas. Fornece também o diststyle, a configuração de backup, a data de criação (tabelas criadas após outubro de 2018) e restrições. Por exemplo, `\dS+ sample` retorna propriedades do objeto. Anexar S+ resulta em colunas adicionais incluídas nos registros retornados.

```
Table "public.sample"
 Column |            Type             |   Collation    | Nullable | Default Value |
 Encoding  | DistKey | SortKey
--------+-----------------------------+----------------+----------+---------------
+-----------+---------+---------
 col1   | smallint                    |                | NO       |               |
 none      | t       | 1
 col2   | character(100)              | case_sensitive | YES      |               |
 none      | f       | 2
 col3   | character varying(100)      | case_sensitive | YES      |               |
 text32k   | f       | 3
 col4   | timestamp without time zone |                | YES      |               |
 runlength | f       | 0
 col5   | super                       |                | YES      |               |
 zstd      | f       | 0
 col6   | bigint                      |                | YES      |               |
 az64      | f       | 0

Diststyle: KEY
Backup: YES
Created: 2021-07-20 19:47:27.997045
Unique Constraints:
    "sample_pkey" PRIMARY KEY (col1)
    "sample_col2_key" UNIQUE (col2)
Foreign-key constraints:
```

```
    "sample_col2_fkey" FOREIGN KEY (col2) REFERENCES lineitem(l_orderkey)
```

O estilo de distribuição, ou Diststyle, da tabela pode ser KEY, AUTO, EVEN ou ALL.

Backup indica se o backup da tabela é feito quando se obtém um snapshot. Os valores válidos são YES ou NO.

Created (Criado) é o carimbo de data/hora para quando a tabela é criada. A data de criação não está disponível para tabelas do Amazon Redshift criadas antes de novembro de 2018. As tabelas criadas antes desta data exibem n/a (não disponível).

Unique Constraints (Restrições exclusivas) lista restrições de chave exclusivas e primárias na tabela.

Foreign-key constraints (Restrições de chave estrangeira) lista restrições de chave estrangeira na tabela.

\dC[+] [PATTERN]

Lista conversões. Inclui o tipo de origem, o tipo de destino e se a conversão está implícita.

Veja a seguir um subconjunto de resultados de \dC+.

```
List of casts
         source type         |         target type         |      function       |
 implicit?   | description
-----------------------------+-----------------------------+---------------------
+---------------+-------------
 "char"                      | character                   | bpchar              | in
 assignment |
 "char"                      | character varying           | text                | in
 assignment |
 "char"                      | integer                     | int4                | no
          |
 "char"                      | text                        | text                | yes
          |
 "path"                      | point                       | point               | no
          |
 "path"                      | polygon                     | polygon             | in
 assignment |
 abstime                     | date                        | date                | in
 assignment |
 abstime                     | integer                     | (binary coercible)  | no
          |
```

```
abstime                     | time without time zone      | time                | in
assignment |
abstime                     | timestamp with time zone    | timestamptz         | yes
        |
abstime                     | timestamp without time zone | timestamp           | yes
        |
bigint                      | bit                         | bit                 | no
        |
bigint                      | boolean                     | bool                | yes
        |
bigint                      | character                   | bpchar              | in
assignment |
bigint                      | character varying           | text                | in
assignment |
bigint                      | double precision            | float8              | yes
        |
bigint                      | integer                     | int4                | in
assignment |
bigint                      | numeric                     | numeric             | yes
        |
bigint                      | oid                         | oid                 | yes
        |
bigint                      | real                        | float4              | yes
        |
bigint                      | regclass                    | oid                 | yes
        |
bigint                      | regoper                     | oid                 | yes
        |
bigint                      | regoperator                 | oid                 | yes
        |
bigint                      | regproc                     | oid                 | yes
        |
bigint                      | regprocedure                | oid                 | yes
        |
bigint                      | regtype                     | oid                 | yes
        |
bigint                      | smallint                    | int2                | in
assignment |
bigint                      | super                       | int8_partiql        | in
assignment |
```

\dd[S] [PATTERN]

Mostra descrições de objetos que não são exibidas em outro lugar.

\de

Lista tabelas externas. Inclui tabelas no catálogo de dados do AWS Glue, no Hive Metastore e tabelas federadas de tabelas de unidade de compartilhamento de dados do Amazon RDS/Aurora MySQL, Amazon RDS/Aurora PostgreSQL e Amazon Redshift.

\de NAME

Descreve uma tabela externa.

A consulta de exemplo a seguir mostra uma tabela externa do AWS Glue.

```
# \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"}
```

Uma tabela Hive Metastore.

```
# \de emr.lineitem
                    Hive Metastore External Table "emr.lineitem"
     Column      | External Type | Redshift Type | Position | Partition Key | Nullable
-----------------+---------------+---------------+----------+---------------+----------
 l_orderkey      | bigint        | bigint        | 1        | 0             |
 l_partkey       | bigint        | bigint        | 2        | 0             |
 l_suppkey       | int           | int           | 3        | 0             |
 l_linenumber    | int           | int           | 4        | 0             |
 l_quantity      | decimal(12,2) | decimal(12,2) | 5        | 0             |
 l_extendedprice | decimal(12,2) | decimal(12,2) | 6        | 0             |
 l_discount      | decimal(12,2) | decimal(12,2) | 7        | 0             |
 l_tax           | decimal(12,2) | decimal(12,2) | 8        | 0             |
 l_returnflag    | char(1)       | char(1)       | 9        | 0             |
 l_linestatus    | char(1)       | char(1)       | 10       | 0             |
 l_commitdate    | date          | date          | 11       | 0             |
 l_receiptdate   | date          | date          | 12       | 0             |
 l_shipinstruct  | char(25)      | char(25)      | 13       | 0             |
 l_shipmode      | char(10)      | char(10)      | 14       | 0             |
 l_comment       | varchar(44)   | varchar(44)   | 15       | 0             |
 l_shipdate      | date          | date          | 16       | 1             |

Location: s3://redshiftbucket/cetas
Input_format: org.apache.hadoop.hive.ql.io.parquet.MapredParquetInputFormat
Output_format: org.apache.hadoop.hive.ql.io.parquet.MapredParquetOutputFormat
Serialization_lib: org.apache.hadoop.hive.ql.io.parquet.serde.ParquetHiveSerDe
Serde_parameters: {"serialization.format":"1"}
Parameters: {"EXTERNAL":"TRUE", "numRows":"4307207",
 "transient_lastDdlTime":"1626990007"}
```

Tabela externa do PostgreSQL.

```
# \de pgrsql.alltypes
                                Postgres Federated Table "pgrsql.alltypes"
 Column |        External Type        |        Redshift Type        | Position |
 Partition Key | Nullable
```

```
--------+----------------------------+----------------------------+----------
+---------------+----------
 col1   | bigint                     | bigint                     | 1        | 0
        |
 col2   | bigint                     | bigint                     | 2        | 0
        |
 col5   | boolean                    | boolean                    | 3        | 0
        |
 col6   | box                        | varchar(65535)             | 4        | 0
        |
 col7   | bytea                      | varchar(65535)             | 5        | 0
        |
 col8   | character(10)              | character(10)              | 6        | 0
        |
 col9   | character varying(10)      | character varying(10)      | 7        | 0
        |
 col10  | cidr                       | varchar(65535)             | 8        | 0
        |
 col11  | circle                     | varchar(65535)             | 9        | 0
        |
 col12  | date                       | date                       | 10       | 0
        |
 col13  | double precision           | double precision           | 11       | 0
        |
 col14  | inet                       | varchar(65535)             | 12       | 0
        |
 col15  | integer                    | integer                    | 13       | 0
        |
 col16  | interval                   | varchar(65535)             | 14       | 0
        |
 col17  | json                       | varchar(65535)             | 15       | 0
        |
 col18  | jsonb                      | varchar(65535)             | 16       | 0
        |
 col19  | line                       | varchar(65535)             | 17       | 0
        |
 col20  | lseg                       | varchar(65535)             | 18       | 0
        |
 col21  | macaddr                    | varchar(65535)             | 19       | 0
        |
 col22  | macaddr8                   | varchar(65535)             | 20       | 0
        |
 col23  | money                      | varchar(65535)             | 21       | 0
        |
```

```
col24  | numeric                     | numeric(38,20)              | 22       | 0
       |
col25  | path                        | varchar(65535)              | 23       | 0
       |
col26  | pg_lsn                      | varchar(65535)              | 24       | 0
       |
col28  | point                       | varchar(65535)              | 25       | 0
       |
col29  | polygon                     | varchar(65535)              | 26       | 0
       |
col30  | real                        | real                        | 27       | 0
       |
col31  | smallint                    | smallint                    | 28       | 0
       |
col32  | smallint                    | smallint                    | 29       | 0
       |
col33  | integer                     | integer                     | 30       | 0
       |
col34  | text                        | varchar(65535)              | 31       | 0
       |
col35  | time without time zone      | varchar(65535)              | 32       | 0
       |
col36  | time with time zone         | varchar(65535)              | 33       | 0
       |
col37  | timestamp without time zone | timestamp without time zone | 34       | 0
       |
col38  | timestamp with time zone    | timestamp with time zone    | 35       | 0
       |
col39  | tsquery                     | varchar(65535)              | 36       | 0
       |
col40  | tsvector                    | varchar(65535)              | 37       | 0
       |
col41  | txid_snapshot               | varchar(65535)              | 38       | 0
       |
col42  | uuid                        | varchar(65535)              | 39       | 0
       |
col43  | xml                         | varchar(65535)              | 40       | 0
       |
```

\df[anptw][S+] [PATTERN]

Lista funções de vários tipos. O comando `\df`, por exemplo, retorna uma lista de funções. Os resultados incluem propriedades como nome, tipo de dados retornado, privilégios de acesso e outros metadados. Os tipos de função podem incluir acionadores, procedimentos armazenados, funções da janela e outros tipos. Quando você acrescenta `S+` ao comando, por exemplo `\dfantS+`, colunas de metadados adicionais são incluídas, como `owner`, `security` e `access privileges`.

\dL[S+] [PATTERN]

Lista dados sobre linguagens processuais associadas ao banco de dados. As informações incluem o nome, como plpgsql, e outros metadados, que incluem confiabilidade, privilégios de acesso e descrição. A chamada de amostra é, por exemplo, `\dLS+`, que lista linguagens e suas propriedades. Quando você acrescenta `S+` ao comando, colunas de metadados adicionais são incluídas, como `call handler` e `access privileges`.

Exemplos de resultados:

```
List of languages
   name    | trusted | internal language |      call handler       |
      validator                         | access privileges |          description

-----------+---------+-------------------+-------------------------
+-------------------------------------------------------------+-------------------
+--------------------------------
 c         | f       | t                 | -                       |
 fmgr_c_validator(oid)                                         |                 |
 Dynamically-loaded C functions
 exfunc    | f       | f                 | exfunc_call_handler()   | -
                                         | rdsdb=U/rdsdb     |
 internal  | f       | t                 | -                       |
 fmgr_internal_validator(oid)                                  |                 |
 Built-in functions
 mlfunc    | f       | f                 | mlfunc_call_handler()   | -
                                         | rdsdb=U/rdsdb     |
 plpgsql   | t       | f                 | plpgsql_call_handler()  |
 plpgsql_validator(oid)                                        |                 |
 plpythonu | f       | f                 | plpython_call_handler() |
 plpython_compiler(cstring,cstring,cstring,cstring,cstring) | rdsdb=U/rdsdb     |
 sql       | t       | t                 | -                       |
 fmgr_sql_validator(oid)                                       | =U/rdsdb          | SQL-
language functions
```

\dm[S+] [PATTERN]

Lista visualizações materializadas. Por exemplo, `\dmS+` lista visualizações materializadas e suas propriedades. Quando você acrescenta `S+` ao comando, colunas de metadados adicionais são incluídas.

\dn[S+] [PATTERN]

Lista os esquemas. Quando você acrescenta `S+` ao comando, por exemplo `\dnS+`, colunas de metadados adicionais são incluídas, como `description` e `access privileges`.

\dp [PATTERN]

Lista os privilégios de acesso à tabela, visualização e sequência.

\dt[S+] [PATTERN]

Lista tabelas. Quando você acrescenta `S+` ao comando, por exemplo `\dtS+`, colunas de metadados adicionais são incluídas, como `description`, neste caso.

\du

Lista os usuários do banco de dados. Inclui o nome e suas funções, como superusuário, e atributos.

\dv[S+] [PATTERN]

Lista as visualizações. Inclui esquema, tipo e proprietário dos dados. Quando você acrescenta `S+` ao comando, por exemplo `\dvS+`, colunas de metadados adicionais são incluídas.

\H

Ativa a saída HTML. Isso é útil para retornar rapidamente resultados formatados. Por exemplo, `select * from sales; \H` retorna resultados da tabela de vendas, em HTML. Para voltar aos resultados tabulares, use `\q` ou quiet.

\i

Executa comandos de um arquivo. Por exemplo, supondo que você tenha rsql_steps.sql em seu diretório de trabalho, o seguinte executa os comandos no arquivo: `\i rsql_steps.sql`.

\l[+] [PATTERN]

Lista bancos de dados. Inclui proprietário, codificação e outras informações.

\q

O encerramento, ou comando \q, faz logoff das sessões do banco de dados e fecha o RSQL.

\sv[+] VIEWNAME

Exibe a definição de uma visualização.

\timing

Mostra o tempo de execução, de uma consulta, por exemplo.

\z [PATTERN]

A mesma saída que \dp.

\?

Exibe informações de ajuda. O parâmetro opcional especifica o item a ser explicado.

\EXIT

Faz logoff de todas as sessões de banco de dados e fecha o Amazon Redshift RSQL. Além disso, é possível especificar um código de saída opcional. Por exemplo, `\EXIT 15` fechará o terminal RSQL do Amazon Redshift e retornará o código de saída 15.

O exemplo a seguir mostra a saída de uma conexão e saída do RSQL.

```
% rsql -D testuser
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.34.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=# \exit 15
```

```
% echo $?
15
```

\EXPORT

Especifica o nome de um arquivo de exportação que o RSQL usa para armazenar informações de banco de dados retornadas por uma instrução SQL SELECT subsequente.

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
```

Resultado no console

```
Rformat is off.
Target width is 1500.
Heading is set to: General Title
Titledashes is on.
(exported 40 rows)
```

\LOGON

Conecta-se a um banco de dados. É possível especificar parâmetros de conexão usando a sintaxe posicional ou como uma cadeia de conexão.

A sintaxe de comando é a seguinte: `\logon {[DBNAME|- USERNAME|- HOST|- PORT|- [PASSWORD]] | conninfo}`

`DBNAME` é o nome do banco de dados ao qual se conectar. `USERNAME` é nome de usuário ao qual se conectar. O `HOST` padrão é `localhost`. O `PORT` padrão é `5439`.

Quando um nome de host é especificado em um comando `\LOGON`, ele se torna o nome de host padrão para outros comandos `\LOGON`. Para alterar o nome do host padrão, especifique um novo `HOST` em outro comando `\LOGON`.

A seguir, veja um exemplo de saída do comando \LOGON para user1.

```
(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=#
```

Exemplo de saída para user2.

```
(testcluster) user1@dev=# \logon dev user2 testcluster2.example.com
Password for user user2:
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
You are now connected to database "dev" as user "user2" on host
 "testcluster2.example.com" at port "5439".
(testcluster2) user2@dev=#
```

\REMARK

Uma extensão do comando \echo. \REMARK imprime a string especificada no fluxo de saída. \REMARK estende \echo adicionando a capacidade de dividir a saída em linhas separadas.

O exemplo a seguir mostra a saída do comando.

```
(testcluster) user1@dev=# \remark 'hello//world'
hello
world
```

\RSET

O comando \rset define parâmetros e variáveis de comando. O \rset tem um modo interativo e um modo em lote. Ele não é compatível com opções como opções bash, por exemplo, -x, nem com argumentos, por exemplo --<arg>.

Ele define variáveis, como as seguintes:

- ERRORLEVEL
- HEADING e RTITLE
- RFORMAT
- MAXERROR
- TITLEDASHES
- WIDTH

O exemplo a seguir especifica um cabeçalho.

```
\rset heading "Winter Sales Report"
```

Você pode encontrar mais exemplos de como usar `\rset`, nos tópicos sobre Variáveis do Amazon Redshift RSQL.

\RUN

Executa o script Amazon Redshift RSQL contido no arquivo especificado. `\RUN` estende o comando `\i` adicionando uma opção para ignorar linhas de cabeçalho de um arquivo.

Se o nome do arquivo contiver uma vírgula, ponto e vírgula ou espaço, coloque-o entre aspas simples. Além disso, se o nome do arquivo for procedido de texto, coloque-o entre aspas. Em UNIX, os nomes dos arquivos diferenciam letras maiúsculas de minúsculas. No Windows, os nomes de arquivos não diferenciam maiúsculas de minúsculas.

O exemplo a seguir mostra a saída do comando.

```
(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

Um alias para o `\!` comando. `\OS` executa o comando do sistema operacional que é passado como um parâmetro. O controle retorna ao Amazon Redshift RSQL após a execução do comando. Por exemplo, você pode executar este comando para imprimir a data e hora atual do sistema e retornar ao terminal RSQL: `\os date`.

```
(testcluster) user1@dev=# \os date
Tue Sep 7 20:47:54 UTC 2021
```

\GOTO

Um novo comando para o Amazon Redshift RSQL. `\GOTO` ignora todos os comandos intervenientes e retoma o processamento no `\LABEL` especificado. O `\LABEL` deve ser uma referência de encaminhamento. Não é possível pular para um `\LABEL` que preceda lexicamente o `\GOTO`.

Veja a seguir um exemplo de saída.

```
(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

Um novo comando para o Amazon Redshift RSQL. `\LABEL` estabelece um ponto de entrada para executar o programa, como o destino para um comando `\GOTO`.

O exemplo a seguir exibe a saída do comando.

```
(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` e comandos relacionados executam condicionalmente partes do script de entrada. Uma extensão do comando PSQL `\if` (`\elif`, `\else`, `\endif`). `\IF` e `\ELSEIF` oferecem suporte a expressões boolianas, inclusive condições `AND`, `OR` e `NOT`.

O exemplo a seguir exibe a saída dos comandos.

```
(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
```

Use `ERRORCODE` em sua lógica de ramificação.

```
\if :'ERRORCODE' = '00000'
    \remark 'The statement was executed without error'
\else
    \remark :LAST_ERROR_MESSAGE
\endif
```

Use `\GOTO` dentro de um bloco `\IF` para controlar como o código será executado.

## Variáveis do Amazon Redshift RSQL

Algumas palavras-chave funcionam como variáveis no RSQL. Você pode definir cada uma delas para um valor específico ou redefinir o valor. A maioria está definida com `\rset`, que tem um modo interativo e um modo em lote. Os comandos podem ser definidos em minúsculas ou maiúsculas.

ACTIVITYCOUNT

Indica o número de linhas afetadas pela última solicitação enviada. Para uma solicitação de retorno de dados, esse é o número de linhas retornadas ao RSQL do banco de dados. O valor é 0 ou um inteiro positivo. O valor máximo é 18.446.744.073.709.551.615.

A variável especialmente tratada `ACTIVITYCOUNT` é semelhante à variável `ROW_COUNT`. Porém, `ROW_COUNT` não informa à aplicação cliente a quantidade de linhas afetadas na conclusão do comando para `SELECT`, `COPY` ou `UNLOAD`. Mas `ACTIVITYCOUNT` o faz.

activitycount_01.sql:

```
select viewname, schemaname
from pg_views
where schemaname = 'not_existing_schema';
\if :ACTIVITYCOUNT = 0
\remark 'views do not exist'
\endif
```

Resultado no console:

```
viewname | schemaname
----------+------------
(0 rows)

views do not exist
```

ERRORLEVEL

Atribui aos erros níveis de gravidade. Use os níveis de gravidade para determinar um curso de ação. Se o comando `ERRORLEVEL` não foi usado, seu valor é `ON` por padrão.

errorlevel_01.sql:

```
\rset errorlevel 42P01 severity 0
```

```
select * from tbl;

select 1 as col;

\echo exit
\quit
```

Resultado no console:

```
Errorlevel is on.
rsql: ERROR: relation "tbl" does not exist
(1 row)

col
1

exit
```

HEADING e RTITLE

Permite que os usuários especifiquem um cabeçalho que aparece no início de um relatório. O cabeçalho especificado pelo comando `RSET RTITLE` inclui automaticamente a data atual do sistema do computador cliente.

Conteúdo de rset_heading_rtitle_02.rsql:

```
\remark Starting...
\rset rtitle "Marketing Department||Confidential//Third Quarter//Chicago"
\rset width 70
\rset rformat on
select * from rsql_test.tbl_currency order by id limit 2;
\exit
\remark Finishing...
```

Resultado no console:

```
Starting...
Rtitle is set to: &DATE||Marketing Department||Confidential//Third Quarter//Chicago
 (Changes will take effect after RFORMAT is
switched ON)
Target width is 70.
Rformat is on.
```

```
09/11/20       Marketing       Department Confidential
                  Third Quarter
                     Chicago
id  | bankid  | name |      start_date
100 |       1 | USD | 2020-09-11 10:51:39.106905
110 |       1 | EUR | 2020-09-11 10:51:39.106905
(2 rows)

Press any key to continue . . .
```

MAXERROR

designa um nível máximo de gravidade de erro além do qual o RSQL termina o processamento do trabalho. Os códigos de retorno são valores inteiros que o RSQL retorna ao sistema operacional cliente após a conclusão de cada trabalho ou tarefa. O valor do código de retorno indica o status de conclusão do trabalho ou tarefa. Se um script contiver uma instrução que produza um nível de gravidade de erro maior que o valor `maxerror` designado, o RSQL sai imediatamente. Portanto, para que o RSQL saia em um nível de gravidade de erro 8, use `RSET MAXERROR 7`.

Conteúdo de maxerror_01.sql:

```
\rset maxerror 0

select 1 as col;

\quit
```

Resultado no console:

```
Maxerror is default.
(1 row)

col
1
```

RFORMAT

Permite que os usuários especifiquem se as configurações serão aplicadas para os comandos de formatação.

Conteúdo rset_rformat.rsql:

```
\remark Starting...
\pset border 2
\pset format wrapped
\pset expanded on
\pset title 'Great Title'
select * from rsql_test.tbl_long where id = 500;
\rset rformat
select * from rsql_test.tbl_long where id = 500;
\rset rformat off
select * from rsql_test.tbl_long where id = 500;
\rset rformat on
select * from rsql_test.tbl_long where id = 500;
\exit
\remark Finishing...
```

Resultado no console:

```
Starting...
Border style is 2. (Changes will take effect after RFORMAT is switched ON)
Output format is wrapped. (Changes will take effect after RFORMAT is switched ON)
Expanded display is on. (Changes will take effect after RFORMAT is switched ON)
Title is "Great Title". (Changes will take effect after RFORMAT is switched ON)
id  |                                                                  long_string
500 | In general, the higher the number the more borders and lines the tables will
 have, but details depend on the particular
format.
(1 row)

Rformat is on.
Great Title
+-[ RECORD
 1 ]+-------------------------------------------------------------------------------------------------
-----------+
| id          | 500
|
| long_string | In general, the higher the number the more borders and lines the tables
 will have, but details depend on the
particular format. |
+-------------
+-------------------------------------------------------------------------------------------------
-----------+

Rformat is off.
```

```
id  |                                                                long_string
500 | In general, the higher the number the more borders and lines the tables will
 have, but details depend on the particular format.
(1 row)

Rformat is on.
Great Title
+-[ RECORD
 1 ]+-------------------------------------------------------------------------------------------
-----------+
| id           | 500
|
| long_string | In general, the higher the number the more borders and lines the tables
 will have, but details depend on the
particular format. |
+-------------
+-------------------------------------------------------------------------------------------
-----------+
Press any key to continue . . .
```

ROW_COUNT

Obtém o número de registros afetados pela consulta anterior. Geralmente é usado para conferir um resultado, como no seguinte fragmento de código:

```
SET result = ROW_COUNT;

IF result = 0
...
```

TITLEDASHES

Esse controle permite que os usuários especifiquem se uma linha de caracteres de traço deve ser impressa acima dos dados de colunas retornados para instruções SQL.

Exemplo:

```
\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;
```

Resultado no console:

```
dept_no      emp_no          salary
------------ ----------- --------------------
100          1000346        1300.00
100          1000245        5000.00
100          1000262        2450.00

dept_no     emp_no          salary
100          1000346        1300.00
100          1000245        5000.00
100          1000262        2450.00
```

WIDTH

Define o formato de saída como empacotado e especifica a largura de destino para cada linha em um relatório. Sem um parâmetro, ele retorna as configurações atuais para o formato e a largura do destino.

Conteúdo rset_width_01.rsql:

```
\echo Starting...
\rset width
\rset width 50
\rset width
\quit
\echo Finishing...
```

Resultado no console:

```
Starting...
Target width is 75.
Target width is 50.
Target width is 50.
Press any key to continue . . .
```

Exemplo com parâmetro:

```
\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...
```

Resultado no console:

```
Starting...
Rformat is on.
Output format is wrapped.
id  |                                          long_string
500 | In general, the higher the number the more borders and lines the ta.
    |.bles will have, but details depend on the particular format.
(1 row)

Target width is 50.
id  |                                          long_string
500 | In general, the higher the number the more.
    |. borders and lines the tables will have, b.
    |.ut details depend on the particular format.
    |..
(1 row)
Press any key to continue . . .
```

## Códigos de erro Amazon Redshift RSQL

Mensagens de sucesso, avisos e exceções:

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 00000 | Classe 00 - Conclusão bem-sucedida | successful_completion |
| 01000 | Classe 01 - Aviso | aviso |
| 0100C | Classe 01 - Aviso | dynamic_result_sets_returned |
| 01008 | Classe 01 - Aviso | implicit_zero_bit_padding |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 01003 | Classe 01 - Aviso | null_value_eliminated_in_set_function |
| 01007 | Classe 01 - Aviso | privilege_not_granted |
| 01006 | Classe 01 - Aviso | privilege_not_revoked |
| 01004 | Classe 01 - Aviso | string_data_right_truncation |
| 01P01 | Classe 01 - Aviso | deprecated_feature |
| 02000 | Classe 02 - Sem dados | no_data |
| 02001 | Classe 02 - Sem dados | no_additional_dynamic_result_sets_returned |
| 03000 | Classe 03 - Instrução SQL ainda não concluída | sql_statement_not_yet_complete |
| 08000 | Classe 08 - Exceção de conexão | connection_exception |
| 08003 | Classe 08 - Exceção de conexão | connection_does_not_exist |
| 08006 | Classe 08 - Exceção de conexão | connection_failure |
| 08001 | Classe 08 - Exceção de conexão | sqlclient_unable_to_establish_sqlconnection |
| 08004 | Classe 08 - Exceção de conexão | sqlserver_rejected_establishment_of_sqlconnection |
| 08007 | Classe 08 - Exceção de conexão | transaction_resolution_unknown |
| 08P01 | Classe 08 - Exceção de conexão | protocol_violation |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 09000 | Classe 09 - Exceção de ação acionada | triggered_action_exception |
| 0A000 | Classe 0A - Recurso incompatível | feature_not_supported |
| 0A000 | Classe 0A - Recurso incompatível | feature_not_supported |
| 0B000 | Classe 0B - Iniciação de transação inválida | invalid_transaction_initiation |
| 0F000 | Classe 0F - Exceção do localizador | locator_exception |
| 0F001 | Classe 0F - Exceção do localizador | invalid_locator_specification |
| 0L000 | Classe 0L - Concedente inválido | invalid_grantor |
| 0LP01 | Classe 0L - Concedente inválido | invalid_grant_operation |
| 0P000 | Classe 0P - Especificação de função inválida | invalid_role_specification |
| 0Z000 | Classe 0Z - Exceção de diagnóstico | diagnostics_exception |
| 0Z002 | Classe 0Z - Exceção de diagnóstico | stacked_diagnostics_accessed_without_active_handler |
| 20000 | Classe 20 - Caso não encontrado | case_not_found |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 21000 | Classe 21 - Violação de cardinalidade | cardinality_violation |

Exceções de dados:

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 22000 | Classe 22 - Exceção de dados | data_exception |
| 2202E | Classe 22 - Exceção de dados | array_subscript_error |
| 22021 | Classe 22 - Exceção de dados | character_not_in_repertoire |
| 22008 | Classe 22 - Exceção de dados | datetime_field_overflow |
| 22012 | Classe 22 - Exceção de dados | division_by_zero |
| 22005 | Classe 01 - Aviso | error_in_assignment |
| 2200B | Classe 01 - Aviso | escape_character_conflict |
| 22022 | Classe 01 - Aviso | indicator_overflow |
| 22015 | Classe 01 - Aviso | interval_field_overflow |
| 2201E | Classe 01 - Aviso | invalid_argument_for_logarithm |
| 2201F | Classe 01 - Aviso | invalid_argument_for_power_function |
| 2201G | Classe 01 - Aviso | invalid_argument_for_width_bucket_function |
| 22018 | Classe 01 - Aviso | invalid_character_value_for_cast |
| 22007 | Classe 01 - Aviso | invalid_datetime_format |
| 22019 | Classe 01 - Aviso | invalid_escape_character |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 2200D | Classe 01 - Aviso | invalid_escape_octet |
| 22025 | Classe 01 - Aviso | invalid_escape_sequence |
| 22P06 | Classe 01 - Aviso | nonstandard_use_of_escape_character |
| 22010 | Classe 01 - Aviso | invalid_indicator_parameter_value |
| 22023 | Classe 01 - Aviso | invalid_parameter_value |
| 2201B | Classe 01 - Aviso | invalid_regular_expression |
| 22009 | Classe 01 - Aviso | invalid_time_zone_displacement_value |
| 2200C | Classe 01 - Aviso | invalid_use_of_escape_character |
| 2200G | Classe 01 - Aviso | most_specific_type_mismatch |
| 22004 | Classe 01 - Aviso | null_value_not_allowed |
| 22002 | Classe 01 - Aviso | null_value_no_indicator_parameter |
| 22003 | Classe 01 - Aviso | numeric_value_out_of_range |
| 22026 | Classe 01 - Aviso | string_data_length_mismatch |
| 22001 | Classe 01 - Aviso | string_data_right_truncation |
| 22011 | Classe 01 - Aviso | substring_error |
| 22027 | Classe 01 - Aviso | trim_error |
| 22024 | Classe 01 - Aviso | unterminated_c_string |
| 2200F | Classe 01 - Aviso | zero_length_character_string |
| 22P01 | Classe 01 - Aviso | floating_point_exception |
| 22P02 | Classe 01 - Aviso | invalid_text_representation |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 22P03 | Classe 01 - Aviso | invalid_binary_representation |
| 22P04 | Classe 01 - Aviso | bad_copy_file_format |
| 22P05 | Classe 01 - Aviso | untranslatable_character |

Violações de restrição de integridade:

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 23000 | Classe 23 - Violação de restrição de integridade | integrity_constraint_violation |
| 23001 | Classe 23 - Violação de restrição de integridade | restrict_violation |
| 23502 | Classe 23 - Violação de restrição de integridade | not_null_violation |
| 23503 | Classe 23 - Violação de restrição de integridade | foreign_key_violation |
| 23505 | Classe 23 - Violação de restrição de integridade | unique_violation |
| 23514 | Classe 23 - Violação de restrição de integridade | check_violation |
| 24000 | Classe 24 - Estado do cursor inválido | invalid_cursor_state |
| 01004 | Classe 01 - Aviso | string_data_right_truncation |
| 25000 | Classe 25 - Estado de transação inválido | invalid_transaction_state |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 25001 | Classe 25 - Estado de transação inválido | active_sql_transaction |
| 25002 | Classe 25 - Estado de transação inválido | invalid_transaction_state |
| 25008 | Classe 25 - Estado de transação inválido | held_cursor_requires_same_isolation_level |
| 25003 | Classe 25 - Estado de transação inválido | inappropriate_access_mode_for_branch_transaction |
| 25004 | Classe 25 - Estado de transação inválido | inappropriate_isolation_level_for_branch_transaction |
| 25005 | Classe 25 - Estado de transação inválido | no_active_sql_transaction_for_branch_transaction |
| 25006 | Classe 25 - Estado de transação inválido | read_only_sql_transaction |
| 25007 | Classe 25 - Estado de transação inválido | no_active_sql_transaction_for_branch_transaction |
| 25P01 | Classe 25 - Estado de transação inválido | no_active_sql_transaction |
| 25P02 | Classe 25 - Estado de transação inválido | in_failed_sql_transaction |
| 26000 | Classe 26 - Nome de instrução SQL inválido | invalid_sql_statement_name |
| 28000 | Classe 28 - Especificação de autorização inválida | invalid_authorization_specification |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 2B000 | Classe 2B - Descritores de privilégios dependentes ainda existem | dependent_privilege_descriptors_still_exist |
| 2BP01 | Classe 2B - Descritores de privilégios dependentes ainda existem | dependent_objects_still_exist |
| 2D000 | Classe 2D - Encerramento de transação inválida | invalid_transaction_termination |
| 2F000 | Classe 2F - Exceção de rotina SQL | sql_routine_exception |
| 2F005 | Classe 2F - Exceção de rotina SQL | function_executed_no_return_statement |
| 2F002 | Classe 2F - Exceção de rotina SQL | modifying_sql_data_not_permitted |
| 2F003 | Classe 2F - Exceção de rotina SQL | prohibited_sql_statement_attempted |
| 2F004 | Classe 2F - Exceção de rotina SQL | reading_sql_data_not_permitted |
| 34000 | Classe 34 - Nome do cursor inválido | invalid_cursor_name |
| 38000 | Classe 38 - Exceção de rotina externa | external_routine_exception |
| 38001 | Classe 38 - Exceção de rotina externa | containing_sql_not_permitted |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 38002 | Classe 38 - Exceção de rotina externa | modifying_sql_data_not_permitted |
| 38003 | Classe 38 - Exceção de rotina externa | prohibited_sql_statement_attempted |
| 38004 | Classe 38 - Exceção de rotina externa | reading_sql_data_not_permitted |
| 39000 | Classe 39 - Exceção de invocação de rotina externa | external_routine_invocation_exception |
| 39001 | Classe 39 - Exceção de invocação de rotina externa | invalid_sqlstate_returned |
| 39004 | Classe 39 - Exceção de invocação de rotina externa | null_value_not_allowed |
| 39P01 | Classe 39 - Exceção de invocação de rotina externa | trigger_protocol_violated |
| 39P02 | Classe 39 - Exceção de invocação de rotina externa | srf_protocol_violated |
| 3D000 | Classe 3D - Nome de catálogo inválido | invalid_catalog_name |
| 3F000 | Classe 3F - Nome de esquema inválido | invalid_schema_name |
| 42000 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | syntax_error_or_access_rule_violation |
| 42601 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | syntax_error |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 42501 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | insuficient_privilege |
| 42846 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | cannot_coerce |
| 42803 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | grouping_error |
| 42830 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_foreign_key |
| 42602 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_name |
| 42622 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | name_too_long |
| 42939 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | reserved_name |
| 42804 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | datatype_mismatch |
| 42P18 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | indeterminate_datatype |
| 42809 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | wrong_object_type |
| 42703 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | undefined_column |
| 42883 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | undefined_function |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 42P01 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | undefined_table |
| 42P02 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | undefined_parameter |
| 42704 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | undefined_object |
| 42701 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | duplicate_column |
| 42P03 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | duplicate_cursor |
| 42P04 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | duplicate_database |
| 42723 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | duplicate_function |
| 42P05 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | duplicate_prepared_statement |
| 42P06 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | duplicate_schema |
| 42P07 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | duplicate_table |
| 42712 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | duplicate_alias |
| 42710 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | duplicate_object |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 42702 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | ambiguous_column |
| 42725 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | ambiguous_function |
| 42P08 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | ambiguous_parameter |
| 42P09 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | ambiguous_alias |
| 42P10 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_column_reference |
| 42611 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_column_definition |
| 42P11 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_cursor_definition |
| 42P12 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_database_definition |
| 42P13 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_function_definition |
| 42P14 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_prepared_statement_definition |
| 42P15 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_schema_definition |
| 42P16 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_table_definition |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 42P17 | Classe 42 - Erro de sintaxe ou violação de regra de acesso | invalid_object_definition |
| 44000 | Classe 44 - Violação WITH CHECK OPTION | with_check_option_violation |
| 53000 | Classe 53 - Recursos insuficientes | insuficiente_resources |
| 53100 | Classe 53 - Recursos insuficientes | disk_full |
| 53200 | Classe 53 - Recursos insuficientes | out_of_memory |
| 53300 | Classe 53 - Recursos insuficientes | too_many_connections |
| 54000 | Classe 54 - Limite do programa excedido | program_limit_exceeded |
| 54001 | Classe 54 - Limite do programa excedido | statement_too_complex |
| 54011 | Classe 54 - Limite do programa excedido | too_many_columns |
| 54023 | Classe 54 - Limite do programa excedido | too_many_arguments |
| 55000 | Classe 55 - O objeto não está no estado de pré-requisito | object_not_in_prerequisite_state |
| 55006 | Classe 55 - O objeto não está no estado de pré-requisito | object_in_use |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| 55P02 | Classe 55 - O objeto não está no estado de pré-requisito | cant_change_runtime_param |
| 55P03 | Classe 55 - O objeto não está no estado de pré-requisito | lock_not_available |
| 57000 | Classe 57 - Intervenção do Operador | operator_intervention |
| 57014 | Classe 57 - Intervenção do Operador | query_canceled |
| 57P01 | Classe 57 - Intervenção do Operador | admin_shutdown |
| 57P02 | Classe 57 - Intervenção do Operador | crash_shutdown |
| 57P03 | Classe 57 - Intervenção do Operador | cannot_connect_now |
| 58000 | Classe 58 - Erro do sistema (erros externos ao PostgreSQL) | system_error |
| 58030 | Classe 58 - Erro do sistema (erros externos ao PostgreSQL) | io_error |
| 58P01 | Classe 58 - Erro do sistema (erros externos ao PostgreSQL) | undefined_file |
| 58P02 | Classe 58 - Erro do sistema (erros externos ao PostgreSQL) | duplicate_file |

| Código de erro | Classe de erro | Nome da condição |
|---|---|---|
| F0000 | Classe F0 - Erro no arquivo de configuração | duplicate_file |
| F0001 | Classe F0 - Erro no arquivo de configuração | lock_file_exists |
| P0000 | Classe P0 - Erro PL/pgSQL | plpgsql_error |
| P0001 | Classe P0 - Erro PL/pgSQL | raise_exception |
| P0002 | Classe P0 - Erro PL/pgSQL | no_data_found |
| P0003 | Classe P0 - Erro PL/pgSQL | too_many_rows |
| XX000 | Classe XX - Erro interno | internal_error |
| XX001 | Classe XX - Erro interno | data_corrupted |
| XX002 | Classe XX - Erro interno | index_corrupted |

## Variáveis de ambiente do Amazon Redshift RSQL

O Amazon Redshift RSQL pode usar variáveis de ambiente para selecionar valores de parâmetros padrão.

RSPASSWORD

> **Important**
>
> Não recomendamos usar essa variável de ambiente por motivos de segurança, pois alguns sistemas operacionais permitem que usuários não administrativos vejam variáveis de ambiente de processo.

Define a senha do Amazon Redshift RSQL para usar na conexão com o Amazon Redshift. Essa variável de ambiente requer o Amazon Redshift RSQL 1.0.4 ou posterior.

O RSQL prioriza o RSPASSWORD caso esteja definido. Se o RSPASSWORD não estiver definido e você estiver se conectando usando um DSN, o RSQL usará a senha dos parâmetros do arquivo DSN. Por fim, se o RSPASSWORD não estiver definido e você não estiver usando um DSN, o RSQL exibirá uma solicitação de senha depois de tentar se conectar.

Veja a seguir um exemplo de como definir um RSPASSWORD:

```
export RSPASSWORD=TestPassw0rd
```

## Conectar-se com SQL Workbench/J

Você pode se conectar a um banco de dados usando o SQL Workbench/J, uma ferramenta de consulta SQL gratuita, independente do DBMS e multiplataforma.

O Amazon Redshift não fornece nem instala nenhuma ferramenta ou biblioteca de cliente SQL de terceiros, portanto você deve instalar qualquer uma que queira usar com seu banco de dados. Para instalar o SQL Workbench/J, siga as instruções na documentação do SQL Workbench/J (SQL Workbench/J). Em geral, para usar o SQL Workbench/J, faça o seguinte:

- Consulte a licença de software do SQL Workbench/J.
- Baixe o pacote Using a custom domain name for client connections apropriado para seu sistema operacional no computador cliente ou na instância do Amazon EC2.
- Instale o SQL Workbench/J no sistema.

  Tenha o Ambiente de Execução Java (JRE) instalado no sistema. Certifique-se de que você está usando a versão correta do JRE exigida pelo cliente SQL Workbench/J.
- Conecte-se ao banco de dados por meio de uma conexão JDBC no SQL Workbench/J

  Verifique se o seu computador cliente ou instância do Amazon EC2 tem o driver JDBC do Amazon Redshift recomendado. Para obter os links de download dos drivers mais recentes, consulte Baixe o driver JDBC do Amazon Redshift, versão 2.1. Além disso, certifique-se de ter definido as configurações do firewall para permitir o acesso ao banco de dados. Para obter mais informações, consulte Etapa 4: Autorizar o acesso ao cluster no Guia de conceitos básicos do Amazon Redshift.
- Crie um perfil de conexão no SQL Workbench/J que use o driver do Amazon Redshift.

## Conectar-se ao data warehouse de forma programática

Para obter informações sobre ferramentas a fim de compilar aplicações para se conectar ao data warehouse, consulte Tools to Build on AWS.

## Usar um perfil de autenticação para se conectar ao Amazon Redshift

Se você tiver muitas conexões com o Amazon Redshift, poderá ser difícil gerenciar as configurações para todas elas. Muitas vezes, cada conexão JDBC ou ODBC usa opções de configuração específicas. Com um perfil de autenticação, você pode armazenar opções de conexão juntas. Dessa forma, seus usuários podem escolher um perfil para se conectar e evitar o gerenciamento de configurações para opções individuais. Os perfis podem ser aplicados a vários cenários e tipos de usuário.

Depois de criar um perfil de autenticação, os usuários podem adicionar o perfil pronto para uso a uma cadeia de conexão. Com isso, eles podem se conectar ao Amazon Redshift com as configurações corretas para cada função e caso de uso.

Para obter informações de API do Amazon Redshift, consulte CreateAuthenticationProfile.

### Criar um perfil de autenticação

Com o AWS CLI, você cria um perfil de autenticação com o comando `create-authentication-profile`. Isso pressupõe que você tenha um cluster do Amazon Redshift existente e um banco de dados existente. Suas credenciais devem ter permissão para se conectar ao banco de dados do Amazon Redshift e direitos para buscar o perfil de autenticação. Forneça as opções de configuração como uma string JSON ou referencie um arquivo que contenha sua string JSON.

```
create-authentication-profile --authentication-profile-name<value: String> --
authentication-profile-content<value: String>
```

O exemplo a seguir cria um perfil chamado `ExampleProfileName`. Aqui, você pode adicionar chaves e valores que definem o nome do cluster e outras configurações de opção, como uma 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}"
}
```

Esse comando cria o perfil com as configurações JSON especificadas. Retorna-se o seguinte resultado, indicando que o perfil foi criado.

```
{"AuthenticationProfileName": "ExampleProfileName",
"AuthenticationProfileContent": "{\"AllowDBUserOverride\":\"1\",
\"Client_ID\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID\",
\"AutoCreate\":false,\"enableFetchRingBuffer\":true,
\"databaseMetadataCurrentDbOnly\":true}" }
```

Limitações e cotas para criar um perfil de autenticação

Cada cliente tem uma cota de dez (10) perfis de autenticação.

Podem ocorrer alguns erros com perfis de autenticação. Por exemplo, se você criar um novo perfil com um nome existente ou se exceder sua cota de perfil. Para obter mais informações, consulte CreateAuthenticationProfile.

Não é possível armazenar determinadas chaves e valores de opção para cadeias de conexão JDBC, ODBC e Python no repositório de perfis de autenticação:

- `AccessKeyID`
- `access_key_id`
- `SecretAccessKey`
- `secret_access_key_id`
- `PWD`
- `Password`
- `password`

Não é possível armazenar a chave ou o valor `AuthProfile` no repositório de perfis, para cadeias de conexão JDBC ou ODBC. Para conexões Python, não é possível armazenar `auth_profile`.

Os perfis de autenticação são armazenados no Amazon DynamoDB e gerenciados pela AWS.

## Trabalhar com perfis de autenticação

Depois de criar um perfil de autenticação, é possível incluir o nome do perfil como uma opção de conexão para o JDBC versão 2.0 `AuthProfile`. Usar essa opção de conexão recupera as configurações armazenadas.

```
jdbc:redshift:iam://endpoint:port/database?AuthProfile=<Profile-
Name>&AccessKeyID=<Caller-Access-Key>&SecretAccessKey=<Caller-Secret-Key>
```

Este é um exemplo de string URL do JDBC.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
AuthProfile="ExampleProfile"&AccessKeyID="AKIAIOSFODNN7EXAMPLE"&SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

Especifique `AccessKeyID` e `SecretAccessKey` na URL do JDBC, juntamente com o nome do perfil de autenticação.

Também é possível separar as opções de configuração com delimitadores de ponto e vírgula, como no exemplo a seguir, que inclui opções para registro em log.

```
jdbc:redshift:iam://my_redshift_end_point:5439/dev?LogLevel=6;LogPath=/
tmp;AuthProfile=my_profile;AccessKeyID="AKIAIOSFODNN7EXAMPLE";SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

> **Note**
>
> Não acrescente informações confidenciais ao perfil de autenticação. Por exemplo, não armazene um valor `AccessKeyID` ou `SecretAccessKey` em um perfil de autenticação. O repositório de perfis de autenticação tem regras para proibir o armazenamento de chaves secretas. Você receberá um erro, caso tente armazenar uma chave e um valor associados a informações confidenciais.

## Obter perfis de autenticação

Para listar perfis de autenticação existentes, chame o comando a seguir.

```
describe-authentication-profiles --authentication-profile-name <value: String>
```

O exemplo a seguir mostra dois perfis recuperados. Se você não especificar um nome de perfil, todos os perfis serão retornados.

```
{ "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}" } ] }
```

## Solução de problemas de conexão no Amazon Redshift

Se você está com problemas na conexão de uma ferramenta do cliente SQL com o seu cluster, existem várias coisas que pode verificar para reduzir o número de possibilidades para o motivo do problema. Se você estiver usando o SSL ou certificados de servidor, remova essa complexidade antes de tentar solucionar o problema de conexão. Você poderá adicioná-los de volta quando tiver encontrado uma solução. Para obter mais informações, consulte Configurar as opções de segurança para conexões.

> **Important**
>
> O Amazon Redshift mudou a maneira como os certificados SSL são gerenciados. Se você tiver problemas para se conectar usando o SSL, talvez seja necessário atualizar os certificados CA raiz confiáveis. Para obter mais informações, consulte Transição para certificados ACM das conexões SSL.

A seção a seguir apresenta algumas mensagens de erro de exemplo e possíveis soluções para os problemas de conexão. Como diferentes ferramentas do cliente SQL geram diferentes mensagens de erro, essa não é uma lista completa, mas deve ser um bom ponto de partida para a solução de problemas.

Tópicos

- Conexão de fora do Amazon EC2 - problema de tempo limite do firewall
- A conexão é recusada ou falha
- O cliente e o driver são incompatíveis
- As consultas parecem travar e, às vezes, não se comunicam com o cluster
- Como configurar o parâmetro JDBC para o tamanho da busca

## Conexão de fora do Amazon EC2 - problema de tempo limite do firewall

Exemplo do problema

A conexão do cliente com o banco de dados parece estar travada ou ter expirado por exceder o tempo limite ao executar consultas longas, como um comando de COPY. Nesse caso, você pode observar que o console do Amazon Redshift exibe que a consulta foi concluída, mas a própria ferramenta do cliente ainda parece estar executando a consulta. Os resultados da consulta podem estar ausentes ou incompletos, dependendo de quando a conexão foi interrompida.

Soluções possíveis:

Esse problema ocorre quando você se conecta ao Amazon Redshift de uma máquina que não seja uma instância do Amazon EC2. Nesse caso, as conexões são encerradas por um componente intermediário de rede, como um firewall, após um período de inatividade. Esse é um comportamento típico que ocorre ao fazer logon em uma rede virtual privada (VPN) ou na rede local.

Para evitar essas limitações de tempo, recomendamos as seguintes alterações:

- Aumente os valores do sistema no cliente que controlam os tempos limite de TCP/IP. Faça essas alterações no computador que está sendo usado para se conectar ao cluster. O período limite deve ser ajustado para o cliente e a rede. Para obter mais informações, consulte Alteração das configurações de tempo limite de TCP/IP.
- Opcionalmente, defina o comportamento de manutenção de atividade no nível do DSN. Para obter mais informações, consulte Alteração das configurações de tempo limite do DSN.

Alteração das configurações de tempo limite de TCP/IP

Para alterar as configurações de tempo limite de TCP/IP, configure essas definições de acordo com o sistema operacional usado para a conexão com o cluster.

- Linux - Se o seu cliente estiver executando no Linux, execute o seguinte comando como usuário root para alterar as configurações de tempo limite da sessão atual:

  ```
  /sbin/sysctl -w net.ipv4.tcp_keepalive_time=200 net.ipv4.tcp_keepalive_intvl=200
   net.ipv4.tcp_keepalive_probes=5
  ```

  Para manter as configurações, crie ou altere o arquivo `/etc/sysctl.conf` com os seguintes valores e, em seguida, reinicialize o sistema.

```
net.ipv4.tcp_keepalive_time=200
net.ipv4.tcp_keepalive_intvl=200
net.ipv4.tcp_keepalive_probes=5
```

- Windows - Se o seu cliente for executado no Windows, edite os valores para as seguintes configurações de registro em HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\:
  - KeepAliveTime: 30000
  - KeepAliveInterval: 1000
  - TcpMaxDataRetransmissions: 10

  Essas configurações usam o tipo de dados DWORD. Se elas não existem no caminho do registro, você pode criar as configurações e especificar esses valores recomendados. Para obter mais informações sobre como editar o registro do Windows, consulte a documentação do Windows.

  Após configurar esses valores, reinicie seu computador para que as alterações sejam implementadas.

- Mac - Se o seu cliente estiver sendo executado em um Mac, execute os seguintes comandos para alterar as configurações de tempo limite da sessão atual:

  ```
  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
  ```

  Para manter as configurações, crie ou altere o arquivo `/etc/sysctl.conf` com os seguintes valores:

  ```
  net.inet.tcp.keepidle=200000
  net.inet.tcp.keepintvl=200000
  net.inet.tcp.keepinit=200000
  net.inet.tcp.always_keepalive=1
  ```

Reinicie seu computador e, em seguida, execute os seguintes comandos para verificar se os valores estão definidos.

```
sysctl net.inet.tcp.keepidle
sysctl net.inet.tcp.keepintvl
sysctl net.inet.tcp.keepinit
sysctl net.inet.tcp.always_keepalive
```

Alteração das configurações de tempo limite do DSN

Você pode definir o comportamento de manutenção de atividade no nível do DSN, se desejar. Para isso, adicione ou modifique os seguintes parâmetros no arquivo odbc.ini:

KeepAlivesCount

O número de pacotes de keepalive de TCP que podem ser perdidos antes que a conexão seja considerada interrompida.

KeepAlivesIdle

O número de segundos de inatividade antes que o driver envie um pacote de manutenções de atividade de TCP.

KeepAlivesInterval

O número de segundos entre cada retransmissão de keepalive de TCP.

No Windows, modifique esses parâmetros no registro adicionando ou alterando as chaves em HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI*your_DSN*. No Linux e no macOS, adicione ou modifique esses parâmetros na entrada do DSN de destino diretamente no arquivo odbc.ini. Para obter mais informações sobre como modificar o arquivo odbc.ini em computadores com Linux e macOS, consulte Use um gerenciador de driver ODBC para configurar o driver nos sistemas operacionais Linux e macOS X.

Se esses parâmetros não existem, ou se estão com o valor 0, o sistema usa os parâmetros de manutenção de atividade especificados para TCP/IP a fim de determinar o comportamento de manutenção de atividade do DSN. No Windows, os parâmetros de TCP/IP podem ser encontrados no registro em `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\`. No Linux e no macOS, os parâmetros de TCP/IP podem ser encontrados no arquivo sysctl.conf.

## A conexão é recusada ou falha

Exemplos de erros:

- "Falha ao estabelecer uma conexão com *<endpoint>*."
- “Não foi possível conectar-se ao servidor: a conexão expirou por exceder o tempo limite. O servidor está sendo executado no host *'<endpoint>'* e aceitando as conexões TCP/IP na porta *'<port>'*?"
- "A conexão foi recusada. Certifique-se de que o nome do host e da porta estão corretos e o postmaster está aceitando conexões de TCP/IP.”

Soluções possíveis:

Geralmente, quando você recebe uma mensagem de erro indicando que não foi possível estabelecer uma conexão, o problema é relacionado à permissão de acesso ao cluster ou ao tráfego de rede que está chegando ao cluster.

Para se conectar ao cluster de uma ferramenta de cliente fora da rede em que o cluster está, adicione uma regra de entrada ao grupo de segurança do cluster. A configuração da regra depende da criação do cluster do Amazon Redshift em uma nuvem privada virtual (VPC):

- Se você criou o cluster do Amazon Redshift em uma nuvem privada virtual (VPC) com base no Amazon VPC, adicione uma regra de entrada ao grupo de segurança da VPC no endereço CIDR/IP no Amazon VPC. Para obter mais informações sobre a configuração de grupos de segurança da VPC para o cluster e opções acessíveis ao público geral, consulte Gerenciamento de clusters em uma VPC.
- Se você criou seu cluster do Amazon Redshift fora de um VPC, adicione o endereço CIDR/endereço IP ao grupo de segurança do cluster no Amazon Redshift. Para obter mais informações sobre a configuração de grupos de segurança de clusters, consulte Grupos de segurança de clusters do Amazon Redshift.

Se você tentar se conectar ao cluster de uma ferramenta cliente que executa uma instância do Amazon EC2, deverá também adicionar uma regra de entrada. Nesse caso, adicione uma regra ao grupo de segurança do cluster. A regra deve especificar o grupo de segurança do Amazon EC2 associado à instância do Amazon EC2 da ferramenta cliente.

Em alguns casos, pode haver uma camada entre o cliente e o servidor, como um firewall. Nesses casos, verifique se o firewall aceita conexões de entrada pela porta que foi configurada para o cluster.

## O cliente e o driver são incompatíveis

### Exemplo de erro

"O DSN especificado apresenta uma incompatibilidade de arquiteturas entre o driver e o aplicativo."

### Solução possível

Quando você recebe uma mensagem de erro de incompatibilidade de arquiteturas ao tentar estabelecer uma conexão, isso significa que a ferramenta do cliente e o driver são incompatíveis. Isso ocorre porque as arquiteturas de sistema não correspondem. Por exemplo, isso pode ocorrer se você tiver uma ferramenta do cliente de 32 bits mas instalou uma versão do driver para 64 bits. Em algumas ocasiões, as ferramentas do cliente de 64 bits podem usar drivers de 32 bits, mas não é possível usar aplicativos de 32 bits com drivers de 64 bits. Certifique-se de que o driver e a ferramenta do cliente estão usando a mesma versão de arquitetura de sistema.

## As consultas parecem travar e, às vezes, não se comunicam com o cluster

### Exemplo do problema

Você está tendo um problema com a conclusão das consultas, onde as consultas parecem estar em execução mas travam na ferramenta do cliente SQL. Às vezes, as consultas não aparecem no cluster, como nas tabelas do sistema ou no console do Amazon Redshift.

### Solução possível

Esse problema pode ocorrer devido à perda de pacotes. Nesse caso, há uma diferença no tamanho da unidade de transmissão máxima (MTU) no caminho da rede entre dois hosts de IP (Internet Protocol). O tamanho de MTU determina o tamanho máximo, em bytes, de um pacote que pode ser transferido em um quadro Ethernet através de uma conexão de rede. Na AWS, alguns tipos de instância do Amazon EC2 oferecem suporte a um MTU de 1500 (frames Ethernet v2) e outros tipos de instância oferecem suporte a um MTU de 9001 (frames jumbo TCP/IP).

Para evitar problemas que podem ocorrer com as diferenças de tamanho de MTU, recomendamos a execução de uma das ações a seguir:

- Se o seu cluster usa a plataforma EC2-VPC, configure o grupo de segurança Amazon VPC com uma regra de entrada personalizada de protocolo de mensagem de controle da Internet (ICMP) que retorna `Destination Unreachable`. Assim, a mensagem instrui o host de origem a usar o menor tamanho de MTU no caminho de rede. Para obter mais detalhes sobre essa abordagem, consulte Configuração de grupos de segurança para permitir o "destino inacessível" do ICMP.
- Se o cluster usa a plataforma EC2-Classic, ou se você não pode permitir a regra de entrada do ICMP, desabilite os quadros jumbo de TCP/IP para que os quadros de Ethernet v2 sejam usados. Para obter mais detalhes sobre essa abordagem, consulte Configuração da MTU de uma instância.

Configuração de grupos de segurança para permitir o "destino inacessível" do ICMP

Quando há alguma diferença no tamanho de MTU da rede entre dois hosts, em primeiro lugar certifique-se de que suas configurações de rede não estão obstruindo a descoberta de MTU do caminho (PMTUD). A PMTUD permite que o host de recepção responda ao host de origem com a seguinte mensagem de ICMP: `Destination Unreachable: fragmentation needed and DF set (ICMP Type 3, Code 4)`. Essa mensagem instrui o host de origem a usar o menor tamanho de MTU no caminho de rede para enviar novamente a solicitação. Sem essa negociação, a perda de pacotes pode ocorrer porque a solicitação é muito grande para o host aceitar. Para obter mais informações sobre a mensagem do ICMP, acesse RFC792 no website Internet Engineering Task Force (IETF).

Se você não configurar explicitamente esta regra de entrada ICMP para seu grupo de segurança do Amazon VPC, PMTUD será bloqueado. Na AWS, grupos de segurança são firewalls virtuais que especificam regras para o tráfego de entrada e saída de uma instância. Para obter informações sobre o grupo de segurança de cluster do Amazon Redshift, consulte Grupos de segurança de clusters do Amazon Redshift. Para clusters que usam a plataforma EC2-VPC, o Amazon Redshift usa grupos de segurança da VPC para permitir ou negar o tráfego para o cluster. Por padrão, os grupos de segurança são bloqueados e negam todo o tráfego de entrada. Para obter informações sobre como definir regras de entrada e saída para instâncias EC2-Classic ou EC2-VPC, consulte Diferenças entre instâncias em EC2-Classic e VPC no Manual do usuário do Amazon EC2 para instâncias do Linux.

Para obter mais informações sobre como adicionar regras aos grupos de segurança da VPC, consulte Gerenciar grupos de segurança da VPC de um cluster. Para obter mais informações sobre configurações específicas de PMTUD exigidas nesta regra, consulte Descoberta do MTU de caminho no Manual do usuário do Amazon EC2 para instâncias do Linux.

### Configuração da MTU de uma instância

Em alguns casos, o cluster pode usar a plataforma EC2-Classic ou você não pode permitir a regra ICMP personalizada para tráfego de entrada. Nesses casos, é recomendado que você ajuste o MTU para 1500 na interface de rede (NIC) das instâncias do EC2 a partir das quais você se conecta ao cluster do Amazon Redshift. Esse ajuste desabilita os quadros enormes de TCP/IP para garantir que as conexões usem consistentemente o mesmo tamanho de pacote. No entanto, essa opção reduz totalmente o throughput máximo da rede para a instância, não apenas para conexões com o Amazon Redshift. Para obter mais informações, consulte os procedimentos a seguir.

#### Para definir a MTU em um sistema operacional Microsoft Windows

Se o cliente é executado em um sistema operacional Microsoft Windows, você pode revisar e definir o valor da MTU para o adaptador de Ethernet usando o comando `netsh`.

1. Execute o comando a seguir para determinar o valor atual da MTU:

   ```
   netsh interface ipv4 show subinterfaces
   ```

2. Revise o valor `MTU` para o adaptador `Ethernet` na saída.
3. Se o valor não for `1500`, execute o seguinte comando para defini-lo:

   ```
   netsh interface ipv4 set subinterface "Ethernet" mtu=1500 store=persistent
   ```

   Após configurar esse valor, reinicie seu computador para que as alterações sejam implementadas.

#### Para definir a MTU em um sistema operacional Linux

Se o cliente é executado em um sistema operacional Linux, você pode revisar e definir o valor da MTU usando o comando `ip`.

1. Execute o comando a seguir para determinar o valor atual da MTU:

   ```
   $ ip link show eth0
   ```

2. Revise o valor da `mtu` na saída.
3. Se o valor não for `1500`, execute o seguinte comando para defini-lo:

```
$ sudo ip link set dev eth0 mtu 1500
```

Para definir a MTU em um sistema operacional Mac

- Siga as instruções no site de suporte do macOS sobre `How to change the MTU for troubleshooting purposes`. Para obter mais informações, pesquise o site de suporte.

## Como configurar o parâmetro JDBC para o tamanho da busca

Por padrão, o driver JDBC coleta todos os resultados de uma consulta ao mesmo tempo. Como resultado, quando você tenta recuperar um grande conjunto de resultados por meio de uma conexão JDBC, pode encontrar um erro de falta de memória por parte do cliente. Para habilitar seu cliente para recuperar conjuntos de resultados em lotes em vez de em uma única busca tudo ou nada, configure o parâmetro JDBC para o tamanho de busca em seu aplicativo cliente.

> **Note**
>
> O tamanho de busca não é compatível com ODBC.

Para obter uma melhor performance, defina o tamanho de busca como o maior valor que não resulte em erros de falta de memória. Um valor menor de tamanho de busca resulta em mais viagens do servidor, o que prolonga os tempos de execução. O servidor reserva recursos, incluindo a vaga de consulta WLM e memória associada, até que o cliente recupere todo o conjunto de resultados ou até que a consulta seja cancelada. Quando você ajusta o tamanho de busca adequadamente, esses recursos são liberados mais rapidamente, disponibilizando-os para outras consultas.

> **Note**
>
> Se você precisar extrair grandes conjuntos de dados, recomendamos o uso de uma instrução UNLOAD para transferir os dados ao Amazon S3. Quando você usa UNLOAD, os nós de computação funcionam em paralelo para acelerar a transferência de dados.

Para obter mais informações sobre a configuração do parâmetro JDBC para o tamanho de busca, acesse Obtenção de resultados com base em um cursor na documentação do PostgreSQL.

# Usar a API de dados Amazon Redshift

Você pode acessar seu banco de dados do Amazon Redshift usando a API interna de dados do Amazon Redshift. Usando essa API, você pode acessar dados do Amazon Redshift com aplicativos baseados em serviços da web, incluindo o AWS Lambda, notebooks do Amazon SageMaker e AWS Cloud9. Para obter mais informações sobre essas aplicações, consulte AWS Lambda, Amazon SageMaker, e AWS Cloud9.

A API de dados não requer uma conexão persistente com o banco de dados. Em vez disso, ela oferece um endpoint HTTP seguro e uma integração com SDKs da AWS. Você pode usar o endpoint para executar instruções SQL sem gerenciar conexões. Chamadas para a API de dados são assíncronas.

A API de dados usa as credenciais armazenadas no AWS Secrets Manager ou credenciais temporárias do banco de dados. Você não precisa passar senhas nas chamadas de API com nenhum dos métodos de autorização. Para obter informações sobre o AWS Secrets Manager, consulte O que é AWS Secrets Manager? no Manual do usuário do AWS Secrets Manager.

Para obter mais informações sobre as operações da API de dados, consulte a Referência da API de dados do Amazon Redshift.

## Trabalhar com a API de dados do Amazon Redshift

Antes de usar a API de dados do Amazon Redshift, revise as seguintes etapas:

1. Determine se você, como autor da chamada da API de dados, está autorizado. Para obter mais informações sobre a autorização, consulte Autorizar acesso à API de dados do Amazon Redshift.
2. Determine se você planeja chamar a API de dados com credenciais de autenticação do Secrets Manager ou credenciais temporárias. Para ter mais informações, consulte Escolher credenciais de autenticação de banco de dados ao chamar a API de dados do Amazon Redshift.
3. Configure um segredo se você usar o Secrets Manager para credenciais de autenticação. Para ter mais informações, consulte Armazenar credenciais de banco de dados no AWS Secrets Manager.
4. Revise as considerações e limitações ao chamar a API de dados. Para ter mais informações, consulte Considerações ao chamar a API de dados do Amazon Redshift.
5. Ligue para a API de dados a partir da AWS Command Line Interface(AWS CLI), a partir de seu próprio código ou usando o editor de consulta no console do Amazon Redshift. Para obter exemplos de chamadas a partir da AWS CLI, consulteChamar a API de dados.

# Considerações ao chamar a API de dados do Amazon Redshift

Considere o seguinte ao chamar a API de dados:

- A API de dados do Amazon Redshift pode acessar bancos de dados em clusters provisionados do Amazon Redshift e grupos de trabalho do Redshift sem servidor. Para obter uma lista de Regiões da AWS onde a API de dados do Redshift está disponível, consulte os endpoints listados para a API de dados do Redshift na Referência geral da Amazon Web Services.
- A duração máxima de uma consulta é de 24 horas.
- O número máximo de consultas ativas (`STARTED` e `SUBMITTED`) por cluster do Amazon Redshift é 200.
- O tamanho máximo do resultado da consulta é 100 MB (após a compactação gzip). Se uma chamada retornar mais de 100 MB de dados de resposta, a chamada será encerrada.
- O tempo máximo de retenção para resultados da consulta é de 24 horas.
- O tamanho máximo da instrução de consulta é de 100 KB.
- A API de dados está disponível para consultar clusters de nó único e de vários nós dos seguintes tipos de nó:
  - dc2.large
  - dc2.8xlarge
  - ds2.xlarge
  - ds2.8xlarge
  - ra3.xlplus
  - ra3.4xlarge
  - ra3.16xlarge
- O cluster deve estar em uma Virtual Private Cloud (VPC) baseada no serviço Amazon VPC.
- Por padrão, os usuários com o mesmo perfil do IAM ou permissões do IAM que o executor de uma operação da API `ExecuteStatement` ou `BatchExecuteStatement` podem atuar na mesma instrução com as operações da API `CancelStatement`, `DescribeStatement`, `GetStatementResult` e `ListStatements`. Para agir na mesma instrução SQL de outro usuário, o usuário deve ser capaz de assumir o perfil do IAM do usuário que executou a instrução SQL. Para obter mais informações sobre como assumir uma função, consulte Autorizar acesso à API de dados do Amazon Redshift.
- As instruções SQL no parâmetro `Sqls` da operação da API `BatchExecuteStatement` são executadas como uma única transação. Eles são executados em série na ordem da matriz. As

instruções SQL subsequentes não são iniciadas enquanto a instrução anterior na matriz não for concluída. Se alguma instrução SQL falhar, como ela é executada como uma transação, todo o trabalho será revertido.

- O tempo máximo de retenção de um token de cliente usado na operação de API `ExecuteStatement` ou `BatchExecuteStatement` é de 8 horas.
- Cada API na API do Redshift Data tem uma cota de transações por segundo antes do controle de utilização das solicitações. Para a cota, consulte Cotas da API de dados do Amazon Redshift. Se a taxa de solicitação exceder a cota, um `ThrottlingException` com o código de status HTTP: 400 será retornado. Para responder ao controle de utilização, use uma estratégia de repetição conforme descrito em Comportamento de nova tentativa no Guia de referência de SDKs e ferramentas da AWS. Essa estratégia é implementada automaticamente para erros no controle de utilização em alguns SDKs da AWS.

> **Note**
>
> Por padrão, no AWS Step Functions, as novas tentativas não permanecem habilitadas. Se você precisar chamar uma API do Redshift Data em uma máquina de estado Step Functions, inclua o parâmetro de idempotência `ClientToken` na chamada de API do Redshift Data. O valor de `ClientToken` precisa persistir entre as novas tentativas. No trecho de exemplo a seguir de uma solicitação para a API `ExecuteStatement`, a expressão `States.ArrayGetItem(States.StringSplit($$.Execution.Id, ':'), 7)` usa uma função intrínseca para extrair a parte UUID de `$$.Execution.Id`, que é exclusiva de cada execução da máquina de estado. Para obter mais informações, consulte Intrinsic functions no Guia de desenvolvedor do AWS Step Functions.
>
> ```
> {
>   "Database": "dev",
>   "Sql": "select 1;",
>   "ClusterIdentifier": "MyCluster",
>   "ClientToken.$": "States.ArrayGetItem(States.StringSplit($$.Execution.Id,
>  ':'), 7)"
> }
> ```

## Escolher credenciais de autenticação de banco de dados ao chamar a API de dados do Amazon Redshift

Quando você chama a API de dados, você usa um dos métodos de autenticação a seguir para algumas operações de API. Cada método requer uma combinação diferente de parâmetros.

AWS Secrets Manager

Com esse método, forneça o `secret-arn` de um segredo armazenado no AWS Secrets Manager que tenha `username` e `password`. O segredo especificado contém credenciais para se conectar ao `database` que você especificar. Quando está se conectando a um cluster, você também fornece o nome do banco de dados. Se você fornecer um identificador do cluster (`dbClusterIdentifier`), ele deverá corresponder ao identificar de cluster armazenado no segredo. Ao se conectar a um grupo de trabalho com a tecnologia sem servidor, você também fornece o nome do banco de dados. Para ter mais informações, consulte Armazenar credenciais de banco de dados no AWS Secrets Manager.

Credenciais temporárias

Com esse método, escolha uma das seguintes opções:

- Ao se conectar a um grupo de trabalho com tecnologia sem servidor, especifique o nome do grupo de trabalho e o nome do banco de dados. O nome de usuário do banco de dados é derivado da identidade do IAM. Por exemplo, `arn:iam::123456789012:user:foo` tem o nome de usuário de banco de dados `IAM:foo`. Além disso, é necessário ter uma permissão para chamar a operação `redshift-serverless:GetCredentials`.
- Ao se conectar a um cluster como uma identidade do IAM, especifique o identificador do cluster e o nome do banco de dados. O nome de usuário do banco de dados é derivado da identidade do IAM. Por exemplo, `arn:iam::123456789012:user:foo` tem o nome de usuário de banco de dados `IAM:foo`. Além disso, é necessário ter uma permissão para chamar a operação `redshift:GetClusterCredentialsWithIAM`.
- Ao se conectar a um cluster como um usuário do banco de dados, especifique o identificador do cluster, o nome do banco de dados e o nome de usuário do banco de dados. Além disso, é necessário ter uma permissão para chamar a operação `redshift:GetClusterCredentials`. Para obter informações sobre como ingressar em grupos de banco de dados ao se conectar com esse método, consulte Unir grupos de banco de dados ao se conectar a um cluster.

Com esses métodos, você também pode fornecer um valor de `region` que especifica a Região da AWS em que os dados estão localizados.

## Mapear tipos de dados JDBC ao chamar a API de dados do Amazon Redshift

A tabela a seguir mapeia tipos de dados Java Database Connectivity (JDBC) para os tipos de dados especificados nas chamadas da API Data.

| Tipo de dados JDBC | Tipo de dados da API de dados |
|---|---|
| `INTEGER, SMALLINT, BIGINT` | `LONG` |
| `FLOAT, REAL, DOUBLE` | `DOUBLE` |
| `DECIMAL` | `STRING` |
| `BOOLEAN, BIT` | `BOOLEAN` |
| `BLOB, BINARY, LONGVARBINARY, VARBINARY` | `BLOB` |
| `VARBINARY` | `STRING` |
| `CLOB` | `STRING` |
| Outros tipos (incluindo tipos relacionados a data e hora) | `STRING` |

Os valores de string são passados ao banco de dados do Amazon Redshift e convertidos implicitamente em um tipo de dados de banco de dados.

> **Note**
>
> Atualmente, a API de dados não oferece suporte a arrays de identificadores exclusivos universais (UUIDs).

## Executar instruções SQL com parâmetros ao chamar a API de dados do Amazon Redshift

Você pode controlar o texto SQL submetido ao mecanismo de banco de dados chamando a operação API de dados usando parâmetros para partes da instrução SQL. Parâmetros nomeados fornecem uma maneira flexível de transmitir parâmetros sem codificá-los no texto SQL. Eles ajudam você a reutilizar o texto SQL e evitar problemas de injeção SQL.

O exemplo a seguir mostra os parâmetros nomeados de um campo `parameters` de um comando `execute-statement` da AWS CLI.

```
--parameters "[{\"name\": \"id\", \"value\": \"1\"},{\"name\": \"address\", \"value\":
 \"Seattle\"}]"
```

Considere o seguinte ao usar parâmetros nomeados:

- Parâmetros nomeados só podem ser usados para substituir valores em instruções SQL.
  - Você pode substituir os valores em uma instrução INSERT, como `INSERT INTO mytable VALUES(:val1)`.

    Os parâmetros nomeados podem estar em qualquer ordem e os parâmetros podem ser usados mais de uma vez no texto SQL. Na opção de parâmetros mostrada em um exemplo anterior, os valores `1` e `Seattle` são inseridos nas colunas da tabela `id` e `address`. No texto SQL, você especifica os parâmetros nomeados da seguinte forma:

    ```
    --sql "insert into mytable values (:id, :address)"
    ```
  - Você pode substituir os valores em uma cláusula de condições, como `WHERE attr >= :val1`, `WHERE attr BETWEEN :val1 AND :val2` e `HAVING COUNT(attr) > :val`.
  - Você não pode substituir nomes de colunas em uma instrução SQL, como `SELECT column-name`, `ORDER BY column-name` ou `GROUP BY column-name`.

    Por exemplo, a instrução SELECT a seguir falha com sintaxe inválida.

    ```
    --sql "SELECT :colname, FROM event" --parameters "[{\"name\": \"colname\", \"value
    \": \"eventname\"}]"
    ```

    Se você descrever (operação `describe-statement`) a instrução com o erro de sintaxe, a `QueryString` retornada não substituirá o nome da coluna pelo parâmetro (`"QueryString":`

`"SELECT :colname, FROM event"`) e um erro será relatado (ERRO: erro de sintaxe em ou próximo a \"FROM\"\n Posição: 12).

  - Não é possível substituir nomes de colunas em uma função agregada, como `COUNT(column-name)`, `AVG(column-name)` ou `SUM(column-name)`.
  - Não é possível substituir nomes de colunas em uma cláusula JOIN.
- Quando o SQL é executado, os dados são implicitamente convertidos em um tipo de dados. Para obter mais informações sobre a conversão do tipo de dados do, consulte Tipos de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- Não é possível definir um valor como NULL. A API de dados a interpreta como a string literal `NULL`. O exemplo a seguir substitui `id` com a string literal `null`. Não o valor NULL SQL.

```
--parameters "[{\"name\": \"id\", \"value\": \"null\"}]"
```

- Não é possível definir um valor de comprimento zero. Falha na instrução SQL da API de dados. O exemplo a seguir tenta definir `id` com um valor de comprimento zero e resulta em uma falha da instrução SQL.

```
--parameters "[{\"name\": \"id\", \"value\": \"\"}]"
```

- Você não pode definir um nome de tabela na instrução SQL com um parâmetro. A API de dados segue a regra do JDBC `PreparedStatement`.
- A saída da operação `describe-statement` retorna os parâmetros de consulta de uma instrução SQL.
- Somente a operação `execute-statement` suporta instruções SQL com parâmetros.

## Executar instruções SQL com um token de idempotência ao chamar a API de dados do Amazon Redshift

Quando você faz uma solicitação de API de mutação, a solicitação normalmente retorna um resultado antes da conclusão dos fluxos de trabalho assíncronos da operação. As operações também podem expirar ou encontrar outros problemas no servidor antes de serem concluídas, mesmo que a solicitação já tenha retornado um resultado. Isso pode dificultar na hora de determinar se a solicitação foi bem-sucedida ou não, e pode levar a várias novas tentativas para garantir que a operação seja concluída com êxito. No entanto, se a solicitação original e as tentativas subsequentes forem bem-sucedidas, a operação será concluída várias vezes. Isso significa que você pode atualizar mais recursos do que pretendia.

A idempotência garante que uma solicitação de API seja concluída no máximo uma vez. Com uma solicitação idempotente, se a solicitação original for concluída com êxito, todas as novas tentativas subsequentes serão concluídas com êxito sem realizar nenhuma ação. As operações `ExecuteStatement` e `BatchExecuteStatement` da API de dados têm um parâmetro idempotente `ClientToken` opcional. O `ClientToken` expira após 8 horas.

> **Important**
>
> Se você chamar as operações `ExecuteStatement` e `BatchExecuteStatement` usando um AWS SDK, um token de cliente será gerado automaticamente para ser usado em uma nova tentativa. Nesse caso, não recomendamos usar o parâmetro `client-token` com as operações `ExecuteStatement` e `BatchExecuteStatement`. Veja o log do CloudTrail para ver o `ClientToken`. Para obter um exemplo de log do CloudTrail, consulte Exemplos de API de dados do Amazon Redshift.

O comando `execute-statement` da AWS CLI a seguir ilustra o parâmetro `client-token` opcional para idempotência.

```
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
```

A tabela a seguir mostra algumas respostas comuns que você pode obter para solicitações de API idempotentes e fornece recomendações para novas tentativas.

| Resposta | Recomendação | Comentários |
| --- | --- | --- |
| 200 (OK) | Não repetir | A solicitação original foi concluída com êxito. Qualquer repetição subsequente é retornada com êxito. |
| Códigos de resposta da série 400 | Não repetir | Há um dos seguintes problemas com a solicitação: |

| Resposta | Recomendação | Comentários |
| --- | --- | --- |
| | | • Ela inclui um parâmetro ou uma combinação de parâmetros que não é válido.<br>• Ela usa uma ação ou um recurso para o qual você não tem permissões.<br>• Ela usa um recurso que está em processo de mudança de estado.<br><br>Se a solicitação envolver um recurso em processo de mudança de estado, a repetição da solicitação poderá ser bem-sucedida. |
| Códigos de resposta da série 500 | Tentar novamente | O erro é causado por um problema no servidor da AWS e geralmente é transitório. Repita a solicitação com uma estratégia de recuo apropriada. |

Para obter informações sobre os códigos de resposta do Amazon Redshift, consulte Erros comuns na Referência de API do Amazon Redshift.

## Autorizar acesso à API de dados do Amazon Redshift

Para acessar a API de dados, um usuário deve ser autorizado. Você pode autorizar um usuário a acessar a API de dados adicionando uma política gerenciada, que é uma política do AWS Identity and Access Management (IAM) predefinida para esse usuário. Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift. Para ver as permissões permitidas e negadas pelas políticas gerenciadas, consulte o console do IAM (https://console.aws.amazon.com/iam/).

O Amazon Redshift fornece a política gerenciada `AmazonRedshiftDataFullAccess`. Esta política fornece acesso total às operações da API de dados do Amazon Redshift. Esta política também permite acesso com escopo específico ao Amazon Redshift, ao AWS Secrets Manager e às operações de API do IAM necessárias para autenticar e acessar um cluster do Amazon Redshift ou um grupo de trabalho do Redshift sem servidor.

Você também pode criar sua própria política do IAM que permite acesso a recursos específicos. Para criar sua política, use a política `AmazonRedshiftDataFullAccess` como seu modelo inicial. Depois de criar sua política, adicione-a a cada usuário que requer acesso à API de dados.

Considere os seguintes requisitos da política do IAM associada ao usuário:

- Se você usar o AWS Secrets Manager para autenticar, confirme se a política permite o uso da ação `secretsmanager:GetSecretValue` para recuperar o segredo marcado com a chave `RedshiftDataFullAccess`.
- Se você usar credenciais temporárias a fim de autenticar em um cluster, confirme se a política permitirá o uso da ação `redshift:GetClusterCredentials` para o nome do usuário do banco de dados `redshift_data_api_user` a qualquer banco de dados no cluster. Esse nome de usuário já deve ter sido criado no banco de dados.
- Se você usar credenciais temporárias para autenticar em um grupo de trabalho com a tecnologia sem servidor, confirme se a política permite o uso da ação `redshift-serverless:GetCredentials` para recuperar o grupo de trabalho marcado com a chave `RedshiftDataFullAccess`. O usuário do banco de dados é mapeado 1:1 para a identidade de origem do AWS Identity and Access Management (IAM). Por exemplo, o usuário usuário_amostra é mapeado para o usuário do banco de dados `IAM:sample_user` e o perfil do IAM perfil_amostra é mapeado para `IAMR:sample_role`. Para obter mais informações sobre as identidades do IAM, consulte Identidades do IAM (usuários, grupos de usuários e perfis) no Guia do usuário do IAM.

Para executar uma consulta em um cluster que pertence a outra conta, a conta proprietária deve fornecer uma função do IAM que a API de dados pode assumir na conta de chamada. Por exemplo, suponha que a Conta B possui um cluster que a Conta A precisa acessar. A Conta B pode anexar a política gerenciada pela AWS `AmazonRedshiftDataFullAccess` para a função do IAM da Conta B. Em seguida, a Conta B confia na Conta A utilizando uma política fidedigna como a seguinte:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::accountID-of-account-A:role/someRoleA"
        ]
```

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Finalmente, a função do IAM da conta A precisa ser capaz de assumir a função do IAM da conta B.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::accountID-of-account-B:role/someRoleB"
  }
}
```

Os links a seguir fornecem informações adicionais sobre o AWS Identity and Access Management no Manual do usuário do IAM.

- Para obter informações sobre como criar funções de IAM, consulte Criar funções do IAM.
- Para obter informações sobre como criar uma política do IAM, consulte Criar políticas do IAM.
- Para obter informações sobre como adicionar uma política do IAM a um usuário, consulte Adicionando e removendo permissões de identidade do IAM.

## Armazenar credenciais de banco de dados no AWS Secrets Manager

Ao chamar a API de dados, você pode passar credenciais para o cluster ou um grupo de trabalho com a tecnologia sem servidor usando um segredo no AWS Secrets Manager. Para passar credenciais dessa maneira, especifique o nome do segredo ou o nome de recurso da Amazon (ARN) do segredo.

Para armazenar credenciais com o Secrets Manager, você precisa da permissão de política gerenciada `SecretManagerReadWrite`. Para obter mais informações sobre as permissões mínimas, consulte Criar e gerenciar segredos com o AWSSecrets Manager no Manual do usuário do AWS Secrets Manager.

Para armazenar suas credenciais em um segredo para um cluster do Amazon Redshift

1. Use o console do AWS Secrets Manager a fim de criar um segredo que contenha credenciais para o cluster:

   - Quando você escolher Armazenar um novo segredo, escolha Credenciais do cluster Redshift.
   - Armazene seus valores para Nome de usuário (usuário do banco de dados), Senha eCluster de banco de dados (identificador de cluster) em seu segredo.
   - Etiquete o segredo com a chave `RedshiftDataFullAccess`. A política gerenciada pelo AWS `AmazonRedshiftDataFullAccess` permite apenas a ação `secretsmanager:GetSecretValue` para segredos marcados com a chave `RedshiftDataFullAccess`.

   Para obter instruções, consulte Criar um segredo básico no Manual do usuário do AWS Secrets Manager.
2. Use o console do AWS Secrets Manager para visualizar os detalhes do segredo criado ou execute o comando `aws secretsmanager describe-secret` da AWS CLI.

   Anote o nome e o ARN do segredo. Você pode usá-los em chamadas para a API de dados.

Para armazenar suas credenciais em um segredo para um grupo de trabalho com a tecnologia sem servidor

1. Use os comandos da AWS CLI do AWS Secrets Manager para armazenar um segredo que contenha as credenciais para o grupo de trabalho com a tecnologia sem servidor:

   - Crie o segredo em um arquivo, por exemplo, um arquivo JSON denominado `mycreds.json`. Forneça os valores para User name (Nome de usuário) (usuário do banco de dados) e Password (Senha) no arquivo.

     ```
     {
           "username": "myusername",
           "password": "mypassword"
     }
     ```
   - Armazene seus valores no segredo e marque-o com a chave `RedshiftDataFullAccess`.

```
aws secretsmanager create-secret --name MyRedshiftSecret  --tags
 Key="RedshiftDataFullAccess",Value="serverless" --secret-string file://
mycreds.json
```

A seguir, é mostrada a saída.

```
{
    "ARN":
 "arn:aws:secretsmanager:region:accountId:secret:MyRedshiftSecret-mvLHxf",
    "Name": "MyRedshiftSecret",
    "VersionId": "a1603925-e8ea-4739-9ae9-e509eEXAMPLE"
}
```

Para obter mais informações, consulte Criar um segredo básico com a AWS CLI no Guia do usuário do AWS Secrets Manager.

2. Use o console do AWS Secrets Manager para visualizar os detalhes do segredo criado ou execute o comando `aws secretsmanager describe-secret` da AWS CLI.

   Anote o nome e o ARN do segredo. Você pode usá-los em chamadas para a API de dados.

## Criar um endpoint da Amazon VPC (AWS PrivateLink) para a API de dados

O Amazon Virtual Private Cloud (Amazon VPC) permite que você inicie recursos da AWS, como clusters e aplicações do Amazon Redshift, em uma nuvem privada virtual (VPC). O AWS PrivateLink fornece conectividade privada entre nuvens privadas virtuais (VPCs) e serviços da AWS com segurança na rede Amazon. Usando AWS PrivateLink, você pode criar endpoints da VPC, que você pode usar para se conectar a serviços em diferentes contas e VPCs com base no Amazon VPC. Para obter mais informações sobre AWS PrivateLink, consulte Serviços de endpoint da VPC (AWS PrivateLink) no Manual do usuário do Amazon Virtual Private Cloud.

Você pode chamar a API de dados com endpoints da Amazon VPC. O uso de um endpoint da Amazon VPC mantém o tráfego entre aplicações em sua Amazon VPC e a API de dados na AWS sem usar endereços IP públicos. Os endpoints do Amazon VPC podem ajudá-lo a atender aos requisitos normativos e de compatibilidade relacionados à limitação da conectividade pública com a Internet. Por exemplo, ao usar um endpoint da Amazon VPC, você pode manter o tráfego entre uma aplicação em execução em uma instância do Amazon EC2 e a API de dados nas VPCs que API contêm.

Depois de criar o Amazon VPC endpoint, você pode começar a usá-lo sem fazer alterações no código ou na configuração de sua aplicação.

Como criar um Amazon VPC endpoint para a API de dados

1. Faça login no AWS Management Console e abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Escolha Endpoints e Create Endpoint (Criar endpoint).
3. Na página Criar endpoint, para a Categoria de serviço, escolha Serviços da AWS. Para o Nome do serviço, escolha redshift-data (`com.amazonaws.region.redshift-data`).
4. Em VPC, escolha a VPC na qual criar o endpoint.

   Escolha a VPC que contém a aplicação que faz chamadas da API de dados.
5. Em Sub-redes, escolha a sub-rede de cada zona de disponibilidade (AZ) usada pelo serviço da AWS que está executando a aplicação.

   Para criar um endpoint do Amazon VPC, especifique o intervalo de endereços IP privados no qual o endpoint está acessível. Para fazer isso, escolha a sub-rede de cada zona de disponibilidade. Isso restringe o VPC endpoint ao intervalo de endereços IP privados específico para cada zona de disponibilidade e também cria um Amazon VPC endpoint em cada zona de disponibilidade.
6. Em Enable DNS Name (Habilitar nome DNS), selecione Enable for this endpoint (Habilitar para este endpoint).

   O DNS privado resolve o nome de host DNS da API de dados padrão (`https://redshift-data.region.amazonaws.com`) para os endereços IP privados associados ao nome de host DNS específico a seu Amazon VPC endpoint. Como resultado, é possível acessar o endpoint da VPC endpoint da API de dados usando a AWS CLI ou os SDKs da AWS sem fazer alterações no código ou na configuração para atualizar o URL do endpoint da API de dados.
7. Em Security group (Grupo de segurança), escolha um grupo de segurança para associar ao Amazon VPC endpoint.

   Escolha o grupo de segurança que permite o acesso ao serviço da AWS que está executando sua aplicação. Por exemplo, se uma instância do Amazon EC2 estiver executando sua aplicação, escolha o grupo de segurança que permite o acesso à instância do Amazon EC2. O grupo de segurança permite que você controle o tráfego para o Amazon VPC endpoint nos recursos em sua VPC.

8. Escolha Create endpoint (Criar endpoint).

Depois que o endpoint for criado, escolha o link no AWS Management Console para visualizar os detalhes do endpoint.

A guia Details (Detalhes) do endpoint mostra os nomes de host de DNS que foram gerados durante a criação do Amazon VPC endpoint.

Você pode usar o endpoint padrão (`redshift-data.region.amazonaws.com`) ou um dos endpoints específicos da VPC para chamar a API de dados dentro da Amazon VPC. O endpoint padrão da API de dados roteia automaticamente para o Amazon VPC endpoint. Esse roteamento ocorre porque o nome de host DNS privado foi habilitado quando o Amazon VPC endpoint foi criado.

Quando você usa um Amazon VPC endpoint em uma chamada da API de dados, todo tráfego entre sua aplicação e a API de dados permanece nas Amazon VPCs que o contêm. Você pode usar um Amazon VPC endpoint para qualquer tipo de chamada da API de dados. Para obter informações sobre como chamar a API de dados, consulte Considerações ao chamar a API de dados do Amazon Redshift.

## Unir grupos de banco de dados ao se conectar a um cluster

Grupos de banco de dados são coleções de usuários do banco de dados. Os privilégios do banco de dados podem ser concedidos a grupos. Um administrador pode configurar um perfil do IAM de forma que esses grupos de banco de dados sejam levados em consideração quando o SQL for executado com a API de dados. Para obter informações sobre grupos de banco de dados, consulte Grupos no Guia do desenvolvedor de banco de dados do Amazon Redshift.

É possível configurar o perfil do IAM de um chamador da API de dados para que o usuário do banco de dados especificado na chamada se junte a grupos de banco de dados quando a API de dados se conectar a um cluster. Esse recurso só é compatível com a conexão com clusters provisionados. Não é compatível com a conexão com grupos de trabalho do Redshift sem servidor. O perfil do IAM do chamador da API de dados também deve permitir a ação `redshift:JoinGroup`.

Configure isso adicionando tags aos perfis do IAM. O administrador do perfil do IAM do chamador adiciona tags com a chave `RedshiftDbGroups` e um valor de chave de uma lista de grupos de banco de dados. O valor é uma lista de nomes separados por dois-pontos (:) de grupos de banco de dados com uma extensão total de até 256 caracteres. Os grupos do banco de dados devem ser definidos previamente no banco de dados conectado. Se algum grupo especificado não for encontrado no banco de dados, ele será ignorado. Por exemplo, para grupos de banco de

dados `accounting` e `retail`, o valor da chave é `accounting:retail`. O par chave-valor da tag `{"Key":"RedshiftDbGroups","Value":"accounting:retail"}` é usado pela API de dados para determinar quais grupos de banco de dados estão associados ao usuário do banco de dados fornecido na chamada para a API de dados.

Para adicionar grupos de banco de dados como uma tag a um perfil do IAM

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console, escolha Roles (Funções) e, em seguida, escolha o nome da função que deseja editar.
3. Escolha a guia Tags e Gerenciar tags.
4. Escolha Adicionar tag e adicione a chave RedshiftDbGroups e um valor que é uma lista de *`database-groups-colon-separated`*.
5. Escolha Salvar alterações.

   Agora, quando uma entidade principal do IAM (com esse perfil do IAM anexado) chama a API de dados, o usuário do banco de dados especificado se junta aos grupos de banco de dados especificados no perfil do IAM.

Para obter mais informações sobre como anexar uma etiqueta a uma entidade principal, inclusive funções do IAM e usuários do IAM, consulte Recursos de etiquetas do IAM no Guia do usuário do IAM.

## Chamar a API de dados

Você pode chamar a API de dados ou a AWS CLI para executar instruções SQL no cluster ou no grupo de trabalho com a tecnologia sem servidor. As principais operações para executar instruções SQL são `ExecuteStatement` e `BatchExecuteStatement` na Referência da API de dados do Amazon Redshift. A API de dados oferece suporte a linguagens de programação aceitas pelos AWS SDKs. Para obter mais informações, consulte Ferramentas para construir na AWS.

Para ver exemplos de código de chamada da API Data, consulte Conceitos básicos da API Data do Redshift no GitHub. Esse repositório tem exemplos de uso do AWS Lambda para acessar dados do Amazon Redshift pelo Amazon EC2, do AWS Glue Data Catalog e do Amazon SageMaker Runtime. Entre os exemplos de linguagens de programação estão: Python, Go, Java e Javascript.

Você pode chamar a API de dados usando a AWS CLI.

Os exemplos a seguir usam a AWS CLI para chamar a API de dados. Para executar os exemplos, edite os valores de parâmetro para corresponder ao seu ambiente. Em muitos dos exemplos, um `cluster-identifier` é fornecido para ser executado em um cluster. Ao executar em um grupo de trabalho com a tecnologia sem servidor, você fornece um `workgroup-name`. Estes exemplos demonstram algumas das operações da API de dados. Para obter mais informações, consulte Referência de comandos da AWS CLI.

Os comandos nos exemplos a seguir foram divididos e formatados para facilitar a leitura.

## Como executar uma instrução SQL

Para executar uma instrução SQL, use o comando `aws redshift-data execute-statement` da AWS CLI.

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster e retorna um identificador para obter os resultados. Este exemplo usa o método de autenticação AWS Secrets Manager.

```
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
```

Este é um exemplo da resposta.

```
{
    "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"
}
```

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster e retorna um identificador para obter os resultados. Este exemplo usa o método de autenticação de credenciais temporárias.

```
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"
```

Este é um exemplo da resposta.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

O comando a seguir da AWS CLI executa uma instrução SQL em um grupo de trabalho com a tecnologia sem servidor e retorna um identificador para obter os resultados. Este exemplo usa o método de autenticação de credenciais temporárias.

```
aws redshift-data execute-statement
    --database dev
    --workgroup-name myworkgroup
    --sql "select 1;"
```

Este é um exemplo da resposta.

```
{
 "CreatedAt": "2022-02-11T06:25:28.748000+00:00",
 "Database": "dev",
 "DbUser": "IAMR:RoleName",
 "Id": "89dd91f5-2d43-43d3-8461-f33aa093c41e",
 "WorkgroupName": "myworkgroup"
}
```

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster e retorna um identificador para obter os resultados. Este exemplo usa o método de autenticação AWS Secrets Manager e um token de idempotência.

```
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
```

Este é um exemplo da resposta.

```
{
    "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"
}
```

## Como executar uma instrução SQL com parâmetros

Para executar uma instrução SQL, use o comando `aws redshift-data execute-statement` da AWS CLI.

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster e retorna um identificador para obter os resultados. Este exemplo usa o método de autenticação AWS Secrets Manager. O texto SQL tem o parâmetro nomeado `distance`. Nesse caso, a distância usada no predicado é 5. Em uma instrução SELECT, os parâmetros nomeados para nomes de colunas só podem ser usados no predicado. Valores para parâmetros nomeados para a instrução SQL são especificados na opção `parameters`.

```
aws redshift-data execute-statement
    --region us-west-2
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
    --cluster-identifier mycluster-test
    --sql "SELECT ratecode FROM demo_table WHERE trip_distance > :distance"
    --parameters "[{\"name\": \"distance\", \"value\": \"5\"}]"
    --database dev
```

Este é um exemplo da resposta.

```
{
    "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"
}
```

O exemplo a seguir usa a tabela EVENT do banco de dados de amostra. Para obter mais informações, consulte Tabela EVENT no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Se você ainda não tem a tabela EVENT em seu banco de dados, você pode criar uma usando a API de dados da seguinte maneira:

```
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)"
```

O comando a seguir insere uma linha na tabela EVENT.

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "insert into event
 values(:eventid, :venueid::smallint, :catid, :dateid, :eventname, :starttime)"
--parameters "[{\"name\": \"eventid\", \"value\": \"1\"}, {\"name\": \"venueid\",
 \"value\": \"1\"},
              {\"name\": \"catid\", \"value\": \"1\"},
```

```
                {\"name\": \"dateid\", \"value\": \"1\"},
                {\"name\": \"eventname\", \"value\": \"event 1\"},
                {\"name\": \"starttime\", \"value\": \"2022-02-22\"}]"
```

O comando a seguir insere uma segunda linha na tabela EVENT. Este exemplo demonstra o seguinte:

- O parâmetro chamado `id` é usado quatro vezes no texto SQL.
- Conversão de tipo implícita é aplicada automaticamente ao inserir o parâmetro `starttime`.
- A coluna `venueid` é o tipo de conversão para o tipo de dados SMALLINT.
- As strings de caracteres que representam o tipo de dados DATE são implicitamente convertidas no tipo de dados TIMESTAMP.
- Os comentários podem ser usados dentro do texto 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\"}]"
```

O seguinte mostra as duas linhas inseridas:

```
 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
```

O comando a seguir usa um parâmetro nomeado em uma cláusula WHERE para recuperar a linha em que `eventid` é `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\"}]"
```

Execute o seguinte comando para obter os resultados SQL da instrução SQL anterior:

```
aws redshift-data get-statement-result --id 7529ad05-b905-4d71-9ec6-8b333836eb5a
```

Fornece os seguintes resultados:

```
{
    "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
}
```

## Para executar várias instruções SQL

Para executar várias instruções SQL com um comando, use o comando `aws redshift-data batch-execute-statement` da AWS CLI.

O comando a seguir da AWS CLI executa três instruções SQL em um cluster e retorna um identificador para obter os resultados. Este exemplo usa o método de autenticação de credenciais temporárias.

```
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"
```

Este é um exemplo da resposta.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

## Para listar metadados sobre instruções SQL

Para listar metadados sobre instruções SQL, use o comando `aws redshift-data list-statements` da AWS CLI. A autorização para executar esse comando é baseada nas permissões do IAM do autor da chamada.

O seguinte comando da AWS CLI lista as instruções SQL que foram executadas.

```
aws redshift-data list-statements
    --region us-west-2
    --status ALL
```

Este é um exemplo da resposta.

```
{
    "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
        }
    ]
}
```


## Como descrever metadados sobre uma instrução SQL

Para obter descrições de metadados para uma instrução SQL, use o comando `aws redshift-data describe-statement` da AWS CLI. A autorização para executar esse comando é baseada nas permissões do IAM do autor da chamada.

O comando da AWS CLI a seguir descreve uma instrução SQL.

```
aws redshift-data describe-statement
    --id d9b6c0c9-0747-4bf4-b142-e8883122f766
    --region us-west-2
```

Este é um exemplo da resposta.

```
{
    "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
}
```

Veja a seguir um exemplo de uma resposta `describe-statement` após a execução de um `batch-execute-statement` com várias instruções 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
}
```

## Como buscar os resultados de uma instrução SQL

Para buscar o resultado de uma instrução SQL que foi executada, use o comando `redshift-data get-statement-result` da AWS CLI. Você pode fornecer um `Id` que você recebe em resposta a `execute-statement` ou `batch-execute-statement`. O valor `Id` para uma instrução SQL executada pelo `batch-execute-statement` pode ser recuperado no resultado de `describe-statement` e recebe o sufixo de dois pontos e número de sequência, como `b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2`. Se você executar várias instruções SQL com `batch-execute-statement`, cada instrução SQL tem um `Id` como mostrado na `describe-statement`. A autorização para executar esse comando é baseada nas permissões do IAM do autor da chamada.

A instrução a seguir retorna o resultado de uma instrução SQL executada pelo `execute-statement`.

```
aws redshift-data get-statement-result
    --id d9b6c0c9-0747-4bf4-b142-e8883122f766
    --region us-west-2
```

A instrução a seguir retorna o resultado da segunda instrução SQL executada pelo `batch-execute-statement`.

```
aws redshift-data get-statement-result
    --id b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2
    --region us-west-2
```

Veja a seguir um exemplo de uma resposta a uma chamada para `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
}
```

## Para descrever uma tabela

Para obter metadados que descrevem uma tabela, use o comando `aws redshift-data describe-table` da AWS CLI.

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster e retorna metadados que descrevem uma tabela. Este exemplo usa o método de autenticação AWS Secrets Manager.

```
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
```

Este é um exemplo da resposta.

```
{
    "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"
        }
    ]
}
```

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster que descreve uma tabela. Este exemplo usa o método de autenticação de credenciais temporárias.

```
aws redshift-data describe-table
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --schema information_schema
    --table sql_features
```

Este é um exemplo da resposta.

```
{
    "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"
        }
    ]
}
```

## Para listar os bancos de dados em um cluster

Para listar os bancos de dados em um cluster, use o comando `aws redshift-data list-databases` da AWS CLI.

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster para listar bancos de dados. Este exemplo usa o método de autenticação AWS Secrets Manager.

```
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
```

Este é um exemplo da resposta.

```
{
    "Databases": [
        "dev"
    ]
}
```

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster para listar bancos de dados. Este exemplo usa o método de autenticação de credenciais temporárias.

```
aws redshift-data list-databases
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
```

Este é um exemplo da resposta.

```
{
    "Databases": [
        "dev"
    ]
}
```

## Para listar os esquemas em um banco de dados

Para listar os esquemas em um banco de dados, use o comando `aws redshift-data list-schemas` da AWS CLI.

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster para listar esquemas em um banco de dados. Este exemplo usa o método de autenticação AWS Secrets Manager.

```
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
```

Este é um exemplo da resposta.

```
{
    "Schemas": [
        "information_schema",
        "pg_catalog",
        "pg_internal",
        "public"
    ]
}
```

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster para listar esquemas em um banco de dados. Este exemplo usa o método de autenticação de credenciais temporárias.

```
aws redshift-data list-schemas
    --region us-west-2
    --db-user mysuser
    --cluster-identifier mycluster-test
    --database dev
```

Este é um exemplo da resposta.

```
{
    "Schemas": [
        "information_schema",
        "pg_catalog",
        "pg_internal",
        "public"
    ]
}
```

## Para listar as tabelas em um banco de dados

Para listar as tabelas em um banco de dados, use o comando `aws redshift-data list-tables` da AWS CLI.

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster para listar tabelas em um banco de dados. Este exemplo usa o método de autenticação AWS Secrets Manager.

```
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
```

Este é um exemplo da resposta.

```
{
    "Tables": [
        {
            "name": "sql_features",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        },
        {
            "name": "sql_implementation_info",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        }
}
```

O comando a seguir da AWS CLI executa uma instrução SQL em um cluster para listar tabelas em um banco de dados. Este exemplo usa o método de autenticação de credenciais temporárias.

```
aws redshift-data list-tables
     --region us-west-2
     --db-user myuser
     --cluster-identifier mycluster-test
     --database dev
     --schema information_schema
```

Este é um exemplo da resposta.

```
{
    "Tables": [
        {
            "name": "sql_features",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        },
        {
            "name": "sql_implementation_info",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        }
    ]
}
```

# Solução de problemas da API de dados do Amazon Redshift

Use as seções a seguir, intituladas com mensagens de erro comuns, para ajudar na solução de problemas com a Data API.

Tópicos


- O pacote para consulta é muito grande
- A resposta do banco de dados excedeu o limite de tamanho


## O pacote para consulta é muito grande

Se você vir um erro indicando que o pacote de uma consulta é muito grande, geralmente o conjunto de resultados retornado para uma linha é muito grande. O limite de tamanho da API de dados é de 64 KB por linha no conjunto de resultados obtido pelo banco de dados.

Para resolver esse problema, verifique se cada linha em um conjunto de resultados tem até 64 KB.

## A resposta do banco de dados excedeu o limite de tamanho

Se você vir um erro indicando que a resposta do banco de dados excedeu o limite de tamanho, geralmente o tamanho do conjunto de resultados retornado pelo banco de dados era muito grande. O limite da API de dados é de 100 MB no conjunto de resultados retornado pelo banco de dados.

Para resolver esse problema, certifique-se de que as chamadas para a API de dados retornem 100 MB de dados ou menos. Se você precisar retornar mais de 100 MB, poderá executar várias chamadas de instrução com a cláusula `LIMIT` em sua consulta.

## Programar operações da API de dados do Amazon Redshift com o Amazon EventBridge

Você pode criar regras que estabeleçam correspondência com eventos selecionados e os encaminhem aos destinos para ação. Você também pode usar as regras para executar uma ação em uma programação predeterminada. Para obter mais informações, consulte o Guia do Usuário do Amazon EventBridge.

Para programar operações de API de dados com o EventBridge, a função do IAM associada deve confiar na entidade principal para o CloudWatch Events (events.amazonaws.com). Essa função deve ter o equivalente à política gerenciada `AmazonEventBridgeFullAccess` anexada. Também deve ter política de permissões `AmazonRedshiftDataFullAccess` que são gerenciadas pela API de dados. Você pode criar uma função do IAM com essas permissões no console do IAM. Ao criar uma função no console do IAM, selecione a entidade confiável do para CloudWatch Events do serviço da AWS. Especifique o perfil do IAM no valor `RoleArn` JSON no destino do EventBridge. Para obter mais informações sobre como criar uma função do IAM, consulte Criando uma função para um serviço da AWS (console) no Guia do usuário do IAM.

O `name` da regra que você cria no Amazon EventBridge deve corresponder ao `StatementName` nos `RedshiftDataParameters`.

Os exemplos a seguir mostram variações da criação de regras do EventBridge com uma ou várias instruções SQL e com um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor como data warehouse.

Chamadas com cluster e uma única instrução SQL

O exemplo a seguir usa a AWS CLI para criar uma regra do EventBridge que é usada para executar uma instrução SQL em um cluster do Amazon Redshift.

```
aws events put-rule
--name test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

Em seguida, um destino EventBridge é criado para ser executado na programação especificada na regra.

```
aws events put-targets
--cli-input-json file://data.json
```

O arquivo data.json de entrada é o seguinte. A chave JSON `Sql` indica que há uma única instrução SQL. O valor JSON `Arn` contém um identificador de cluster. O valor `RoleArn` JSON contém o perfil do IAM usado para executar o SQL conforme descrito anteriormente.

```
{
    "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
            }
        }
    ]
}
```

Chamadas com grupo de trabalho e uma única instrução SQL

O exemplo a seguir usa a AWS CLI para criar uma regra do EventBridge que é usada para executar uma instrução SQL em um grupo de trabalho do Amazon Redshift sem servidor.

```
aws events put-rule
--name  test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

Em seguida, um destino EventBridge é criado para ser executado na programação especificada na regra.

```
aws events put-targets
--cli-input-json file://data.json
```

O arquivo data.json de entrada é o seguinte. A chave JSON `Sql` indica que há uma única instrução SQL. O valor JSON `Arn` contém um nome de grupo de trabalho. O valor `RoleArn` JSON contém o perfil do IAM usado para executar o SQL conforme descrito anteriormente.

```
{
    "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
            }
        }
    ]
}
```

Chamadas com cluster e várias instruções SQL

O exemplo a seguir usa a AWS CLI para criar uma regra do EventBridge que é usada para executar várias instruções SQL em um cluster do Amazon Redshift.

```
aws events put-rule
--name  test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

Em seguida, um destino EventBridge é criado para ser executado na programação especificada na regra.

```
aws events put-targets
--cli-input-json file://data.json
```

O arquivo data.json de entrada é o seguinte. A chave JSON `Sqls` indica que há várias instruções SQL. O valor JSON `Arn` contém um identificador de cluster. O valor `RoleArn` JSON contém o perfil do IAM usado para executar o SQL conforme descrito anteriormente.

```
{
    "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
            }
        }
    ]
}
```

Chamadas com grupo de trabalho e várias instruções SQL

O exemplo a seguir usa a AWS CLI para criar uma regra do EventBridge que é usada para executar várias instruções SQL em um grupo de trabalho do Amazon Redshift sem servidor.

```
aws events put-rule
--name  test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

Em seguida, um destino EventBridge é criado para ser executado na programação especificada na regra.

```
aws events put-targets
--cli-input-json file://data.json
```

O arquivo data.json de entrada é o seguinte. A chave JSON `Sqls` indica que há várias instruções SQL. O valor JSON `Arn` contém um nome de grupo de trabalho. O valor `RoleArn` JSON contém o perfil do IAM usado para executar o SQL conforme descrito anteriormente.

```
{
    "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
            }
        }
    ]
}
```

## Monitorar a API de dados

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e performance da API de dados e de suas outras soluções da AWS. A AWS fornece as seguintes ferramentas de monitoramento para observar a API de dados, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- O Amazon EventBridge pode ser usado para automatizar seus serviços da AWS e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicações ou alterações de recursos. Os eventos dos serviços da AWS são entregues ao EventBridge quase em tempo real. Você pode escrever regras simples para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Para obter mais informações, consulte o Guia do Usuário do Amazon EventBridge.
- O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por ou em nome de sua conta da AWS e entrega os arquivos de log a um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem no qual as chamadas foram feitas e quando elas ocorreram. Para saber mais sobre como o Amazon Redshift é integrado ao AWS CloudTrail, consulte “Logging with CloudTrail” (Registro em log com o CloudTrail). Para obter mais informações sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Tópicos

- Monitorar eventos para a API de dados do Amazon Redshift no Amazon EventBridge

## Monitorar eventos para a API de dados do Amazon Redshift no Amazon EventBridge

Você pode monitorar eventos de API de dados no EventBridge, que fornece um fluxo de dados em tempo real de suas próprias aplicações, aplicações de software como serviço (SaaS) e serviços da AWS. O EventBridge encaminha esses dados para destinos como AWS Lambda e o Amazon SNS. Esses eventos são iguais aos que aparecem no CloudWatch Events, que oferece um fluxo quase em tempo real de eventos do sistema que descrevem as mudanças nos recursos da AWS. Os eventos são enviados para a conta que contém o banco de dados do Amazon Redshift. Por exemplo, se você assumir uma função em outra conta, os eventos serão enviados para essa conta. Para obter mais informações, consulte Eventos do Amazon EventBridge no Guia do usuário do Amazon EventBridge.

Os eventos da API Data são enviados quando a operação da API `ExecuteStatement` ou `BatchExecuteStatement` define a opção `WithEvent` como `true`. O campo `state` do evento contém um dos seguintes valores:

- ABORTED: a execução da consulta foi interrompida pelo usuário.
- FAILED — Falha na execução da consulta.
- FINISHED — A consulta terminou de ser executada.

A entrega dos eventos é garantida. Para obter mais informações, consulte Eventos de produtos da AWS no Guia do usuário do Amazon EventBridge.

Exemplo de evento concluído da API de dados

Os exemplos a seguir mostram um evento para API Data quando a operação da API `ExecuteStatement` termina. Neste exemplo, uma instrução chamada `test.testtable` terminou de ser executada.

```
{
    "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
    }
}
```

# Grupos de parâmetros do Amazon Redshift

## Visão geral

No Amazon Redshift, você associa um grupo de parâmetros a cada cluster que você cria. Um grupo de parâmetros é um grupo de parâmetros que se aplicam a todos os bancos de dados que você cria no cluster. Esses parâmetros definem as configurações do banco de dados, como tempo limite de consulta e estilo de data.

## Sobre grupos de parâmetros

Cada parameter group tem vários parâmetros para definir configurações do banco de dados. A lista de parâmetros disponíveis depende da família do parameter group à qual o parameter group pertence. A família do grupo de parâmetros é a versão do mecanismo Amazon Redshift ao qual os parâmetros do grupo de parâmetros se aplicam. O formato do nome da família do grupo de parâmetros é `redshift-`*`version`* em que *`version`* é a versão do mecanismo. Por exemplo, a versão atual do mecanismo é `redshift-1.0`.

O Amazon Redshift fornece um grupo de parâmetros padrão para cada família de grupo de parâmetros. O parameter group padrão tem valores predefinidos para cada um dos parâmetros e não pode ser modificado. O formato do nome do parameter group padrão é `default.`*`parameter_group_family`*, em que *`parameter_group_family`* é a versão do mecanismo a que o parameter group pertence. Por exemplo, o parameter group padrão da versão `redshift-1.0` se chama `default.redshift-1.0`.

> **Note**
>
> No momento, `redshift-1.0` é a única versão do mecanismo Amazon Redshift. Consequentemente, `default.redshift-1.0` é o único parameter group padrão.

Se quiser usar valores de parâmetro diferentes do parameter group padrão, você deverá criar um parameter group personalizado e associar o cluster a ele. Inicialmente, os valores de parâmetro em um parameter group personalizado são os mesmos do parameter group padrão. A `source` inicial para todos os parâmetros é `engine-default` porque os valores são predefinidos pelo Amazon Redshift. Depois que você alterar um valor de parâmetro, o `source` mudará para `user` a fim de indicar que o valor foi modificado em relação ao valor padrão.

> **Note**
>
> O console do Amazon Redshift não exibe a `source` de cada parâmetro. É necessário usar a API do Amazon Redshift, a AWS CLI ou uma das AWS SDKs para visualizar a `source`.

Para grupos de parâmetros criados, você pode modificar um valor de parâmetro a qualquer momento, ou pode restaurar os padrões de todos os valores de parâmetro. Você também pode associar um grupo de parâmetros diferente a um cluster. Em alguns casos, poderá modificar valores de parâmetro em um grupo de parâmetros que já está associado a um cluster ou associar um grupo de parâmetros diferente a um cluster. Nesses casos, poderá ser necessário reiniciar o cluster para que os valores de parâmetro atualizados entrem em vigor. Se o cluster falhar e for reiniciado pelo Amazon Redshift, suas alterações serão aplicadas naquele momento. As alterações não serão aplicadas se o cluster for reiniciado durante a manutenção. Para obter mais informações, consulte Propriedades dinâmicas e estáticas do WLM.

## Valores de parâmetro padrão

A tabela a seguir mostra resumidamente os valores de parâmetro padrão com links para informações mais aprofundadas sobre cada parâmetro. Esses são os valores padrão da família de grupos de parâmetros `redshift-1.0`.

| Nome do parâmetro | Valor | Mais informações |
|---|---|---|
| auto_analyze | verdadeiro | auto_analyze no Guia do desenvolvedor de banco de dados do Amazon Redshift |
| auto_mv | verdadeiro | Visualizações materializadas automatizadas no Guia do desenvolvedor do banco de dados do Amazon Redshift |
| datestyle | ISO, MDY | datestyle no Guia do desenvolvedor de banco de dados do Amazon Redshift |
| enable_case_sensitive_identifier | false | enable_case_sensitive_identifier no Guia do desenvolvedor de banco de dados do Amazon Redshift |

| Nome do parâmetro | Valor | Mais informações |
| --- | --- | --- |
| enable_user_activity_logging | false | Registro em log da auditoria de banco de dados neste guia |
| extra_float_digits | 0 | extra_float_digits no Guia do desenvolvedor de banco de dados do Amazon Redshift |
| max_concurrency_scaling_clusters | 1 | max_concurrency_scaling_clusters no Guia do desenvolvedor de banco de dados do Amazon Redshift |
| query_group | default | query_group no Guia do desenvolvedor de banco de dados do Amazon Redshift |
| require_ssl | false | Configurar as opções de segurança para conexões neste guia |
| search_path | $user, public | search_path no Guia do desenvolvedor de banco de dados do Amazon Redshift |
| statement_timeout | 0 | statement_timeout no Guia do desenvolvedor de banco de dados do Amazon Redshift |
| wlm_json_configuration | [{"auto_wlm":true}] | Configurar o gerenciamento do workload neste guia |
| use_fips_ssl | false | Habilite o modo SSL compatível com FIPS somente se o sistema precisar ser compatível com FIPS. |

**Note**

O parâmetro `max_cursor_result_set_size` está obsoleto. Para obter mais informações sobre o tamanho do conjunto de resultados do cursor, consulte Restrições de cursor no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Você pode substituir temporariamente um parâmetro usando o comando SET no banco de dados. O comando SET substitui somente o parâmetro da duração da sessão atual. Além dos parâmetros listados na tabela anterior, você também pode ajustar temporariamente a contagem de slots definindo `wlm_query_slot_count` no banco de dados. O parâmetro `wlm_query_slot_count` não está disponível para configuração em grupos de parâmetros. Para obter mais informações sobre como ajustar a contagem de slots, consulte wlm_query_slot_count no Guia do desenvolvedor de banco de dados do Amazon Redshift. Para obter mais informações sobre como substituir temporariamente outros parâmetros, consulte Modificar a configuração do servidor no Guia do desenvolvedor de banco de dados do Amazon Redshift.

## Configurar valores de parâmetro usando a AWS CLI

Para configurar parâmetros do Amazon Redshift usando a AWS CLI, você usa o comando `modify-cluster-parameter-group` para um grupo de parâmetros específico. Você especifica o parameter group a ser modificado em `parameter-group-name`. Você usa o parâmetro `parameters` (do comando `modify-cluster-parameter-group`) a fim de especificar pares de nome/valor para cada parâmetro que deseja modificar no parameter group.

> **Note**
>
> Existem considerações especiais durante a configuração do parâmetro `wlm_json_configuration` usando a AWS CLI. Os exemplos nesta seção se aplicam a todos os parâmetros, exceto `wlm_json_configuration`. Para obter mais informações sobre como configurar o `wlm_json_configuration` usando a AWS CLI, consulte Configurar o gerenciamento do workload.

Depois de modificar valores de parâmetro, você deverá reinicializar todos os clusters que estejam associados ao parameter group modificado. O status do cluster exibe `applying` para `ParameterApplyStatus` enquanto os valores são aplicados e `pending-reboot` depois que os valores tiverem sido aplicados. Depois de reinicializar, os bancos de dados no cluster começarão a usar os novos valores de parâmetro. Para obter mais informações sobre como reiniciar clusters, consulte Reinicialização de um cluster.

> **Note**
>
> O parâmetro `wlm_json_configuration` contém algumas propriedades dinâmicas e não exigem que você reinicie clusters associados para que as alterações sejam aplicadas. Para

obter mais informações sobre propriedades dinâmicas e estáticas, consulte Propriedades dinâmicas e estáticas do WLM.

Sintaxe

A sintaxe a seguir mostra como usar o comando `modify-cluster-parameter-group` para configurar um parâmetro. Você especifica *`parameter_group_name`* e substitui *`parameter_name`* e *`parameter_value`* por um parâmetro real a ser modificado e um valor para esse parâmetro. Se você quiser modificar mais de um parâmetro simultaneamente, separe cada conjunto de parâmetros e valores do seguinte com um espaço.

```
aws redshift modify-cluster-parameter-group --parameter-group-name parameter_group_name
 --parameters ParameterName=parameter_name,ParameterValue=parameter_value
```

Exemplo

O exemplo a seguir mostra como configurar os parâmetros `statement_timeout` e `enable_user_activity_logging` do parameter group `myclusterparametergroup`.

> **Note**
>
> Para fins de legibilidade, o exemplo é exibido em várias linhas, mas, na AWS CLI real, tem uma linha.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name myclusterparametergroup
--parameters ParameterName=statement_timeout,ParameterValue=20000
 ParameterName=enable_user_activity_logging,ParameterValue=true
```

Você pode gerenciar grupos de parâmetros usando o console. Para obter mais informações, consulte Gerenciamento de grupos de parâmetros usando o console.

# Configurar o gerenciamento do workload

No Amazon Redshift, você usa o gerenciamento de workload (WLM) para definir o número de filas de consulta que estão disponíveis e como as consultas são roteadas para essas filas

para processamento. O WLM faz parte da configuração do parameter group. Um cluster usar a configuração do WLM especificada no parameter group associado.

Quando você cria um parameter group, a configuração do WLM padrão contém uma fila capaz de executar até cinco consultas simultaneamente. Você poderá adicionar filas e configurar propriedades do WLM em cada uma delas, se quiser mais controle sobre o processamento de consultas. Cada fila adicionada terá a mesma configuração do WLM padrão até você configurar as propriedades.

Quando você adiciona filas, a última fila na configuração é a fila padrão. A menos que seja roteada para outra fila com base em critérios na configuração do WLM, uma consulta é processada pela fila padrão. É possível especificar o modo e o nível de simultaneidade (slots de consulta) da fila padrão, mas não é possível especificar grupos de usuários ou de consultas para a fila padrão.

Assim como acontece com outros parâmetros, você não pode modificar a configuração do WLM no parameter group padrão. Os clusters associados ao parameter group padrão sempre usam a configuração do WLM padrão. Para modificar a configuração do WLM, crie um novo grupo de parâmetros e associe esse grupo de parâmetros a todos os clusters que exigirem a configuração do WLM personalizada.

## Propriedades dinâmicas e estáticas do WLM

As propriedades de configuração do WLM são dinâmicas ou estáticas. É possível aplicar propriedades dinâmicas ao banco de dados sem uma reinicialização do cluster, mas as propriedades estáticas exigem uma reinicialização do cluster para que as alterações entrem em vigor. Para obter mais informações sobre propriedades dinâmicas e estáticas, consulte Propriedades de configuração dinâmicas e estáticas do WLM.

## Propriedades para o parâmetro wlm_json_configuration

É possível configurar o WLM usando o console do Amazon Redshift, a AWS CLI, a API do Amazon Redshift ou uma das AWS SDKs. A configuração do WLM usa várias propriedades para definir o comportamento da fila, como alocação da memória entre as filas, o número de consultas que podem ser executadas simultaneamente em uma fila etc.

> **Note**
>
> As propriedades a seguir aparecem com seus nomes de console do Amazon Redshift, com os nomes de propriedade JSON correspondentes nas descrições.

A tabela a seguir resume se uma propriedade se aplica ao WLM automático ou WLM manual.

| Propriedade do WLM | WLM automático | WLM manual |
|---|---|---|
| Auto WLM (WLM automático) | Sim | Sim |
| Habilitar a aceleração de consultas breves | Sim | Sim |
| Tempo máximo de execução para consultas breves | Sim | Sim |
| Prioridade | Sim | Não |
| Tipo de fila | Sim | Sim |
| Nome da fila | Sim | Sim |
| Modo de escalabilidade da simultaneidade | Sim | Sim |
| Simultaneidade | Não | Sim |
| Grupos de usuários | Sim | Sim |
| Curinga do grupo de usuários | Sim | Sim |
| Grupos de consultas | Sim | Sim |
| Curinga do grupo de consultas | Sim | Sim |
| Perfis de usuário | Sim | Sim |
| Caractere curinga de perfil de usuário | Sim | Sim |
| Timeout (Tempo limite) | Não | Preterido |
| Memória | Não | Sim |

| Propriedade do WLM | WLM automático | WLM manual |
| --- | --- | --- |
| Regras de monitoramento de consulta | Sim | Sim |

A lista a seguir descreve as propriedades do WLM que você pode configurar.

Auto WLM (WLM automático)

Auto WLM (WLM automático) definido como `true` habilita o WLM automático. O WLM automático define os valores de Simultaneidade no principal e Memória (%) como `Auto`. O Amazon Redshift gerencia a simultaneidade de consultas e a alocação de memória. O padrão é `true`.

Propriedade JSON: `auto_wlm`

Habilitar a aceleração de consultas breves

A aceleração de consultas breves (SQA) prioriza as consultas de curta execução sobre as consultas de execução demorada. A SQA executa consultas breves em um espaço dedicado, de maneira que as consultas SQA não sejam forçadas a esperar em filas atrás de consultas mais demoradas. Com a SQA, consultas breves são iniciadas com mais rapidez e os usuários veem os resultados mais cedo. Quando você habilita a SQA, também pode especificar o tempo máximo de execução para consultas breves. Para habilitar a SQA, especifique `true`. O padrão é `false`. Essa configuração é aplicada para cada grupo de parâmetros em vez de para cada fila.

Propriedade JSON: `short_query_queue`

Tempo máximo de execução para consultas breves

Quando você habilita a SQA, pode especificar 0 para permitir que WLM defina, de forma dinâmica, o tempo máximo de execução para consultas breves. Como alternativa, você pode especificar um valor de 1 a 20 segundos, em milissegundos. O valor padrão é `0`.

Propriedade JSON: `max_execution_time`

Priority

Priority (Prioridade) define a prioridade das consultas executadas em uma fila. Para definir a prioridade, o WLM mode (Modo do WLM) deve ser definido como Auto WLM (WLM automático), ou seja, `auto_wlm` deve ser `true`. Os valores de prioridade podem ser `highest`, `high`, `normal`, `low` e `lowest`. O padrão é `normal`.

Propriedade JSON: `priority`

Tipo de fila

O tipo de fila designa uma fila como usada por Auto WLM (WLM automático) ou Manual WLM (WLM manual). Defina `queue_type` como `auto` ou `manual`. Se não especificado, o padrão será `manual`.

Propriedade JSON: `queue_type`

Nome da fila

O nome da fila do . Você pode definir o nome da fila com base nas necessidades da sua empresa. Os nomes de fila devem ser exclusivos dentro de uma configuração do WLM, ter até 64 caracteres alfanuméricos, sublinhados ou espaços, e não podem conter aspas. Por exemplo, se você tiver uma fila para as consultas de ETL, poderá chamá-la de `ETL queue`. Este nome é usado em métricas, valores de tabela do sistema e no console do Amazon Redshift para identificar a fila. Consultas e relatórios que usam o nome dessas fontes precisam ser capazes de lidar com alterações no nome. Anteriormente, os nomes das filas eram gerados pelo Amazon Redshift. Os nomes padrão das filas são `Queue 1`, `Queue 2`, até a última fila nomeada `Default queue`.

> **Important**
>
> Se você alterar um nome de fila, o valor da dimensão `QueueName` de métricas de fila do WLM (como WLMQueueLength, WLMQueueWaitTime, WLMQueriesCompletedPerSecond, WLMQueryDuration, WLMRunningQueries e assim por diante) também mudará. Portanto, se você alterar o nome de uma fila, pode ser necessário alterar os alarmes do CloudWatch que você configurou.

Propriedade JSON: `name`

Modo de escalabilidade da simultaneidade

Para habilitar a escalabilidade da simultaneidade em uma fila, defina o Concurrency Scaling mode (Modo de escalabilidade da simultaneidade) como `auto`. Quando o número de consultas roteadas para uma fila excede a simultaneidade configurada da fila, as consultas qualificadas são enviadas para o cluster de escalabilidade. Quando os slots forem disponibilizados, as consultas serão executadas no cluster principal. O padrão é `off`.

Propriedade JSON: `concurrency_scaling`

Simultaneidade

O número de consultas que podem ser executadas simultaneamente em uma fila do WLM. Esta propriedade só se aplica ao WLM manual. Se a escalabilidade de simultaneidade estiver habilitada, as consultas qualificadas serão enviadas a um cluster de escalabilidade quando uma fila atingir o nível de simultaneidade (slots de consulta). Se a escalabilidade da simultaneidade estiver desabilitada, as consultas aguardarão na fila até que um slot seja disponibilizado. O intervalo é entre 1 e 50.

Propriedade JSON: `query_concurrency`

User Groups (Grupos de usuários)

Uma lista separada por vírgulas de nomes de grupos de usuários. Quando membros do grupo de usuários executam consultas no banco de dados, as consultas são roteadas para a fila associada ao grupo de usuários.

Propriedade JSON: `user_group`

User Group Wildcard

Um valor Booliano que indica se é necessário permitir curingas para grupos de usuários. Se for 0, os curingas estarão desativados; se for 1, os curingas estarão ativados. Quando curingas são permitidos, você pode usar "*" ou "?" para especificar vários grupos de usuários ao executar consultas. Para obter mais informações, consulte Curingas.

Propriedade JSON: `user_group_wild_card`

Query Groups (Grupos de consultas)

Uma lista separada por vírgulas de grupos de consultas. Quando membros do grupo de consultas executam consultas no banco de dados, as consultas são roteadas para a fila associada ao grupo de consultas.

Propriedade JSON: `query_group`

Query Group Wildcard

Um valor Booliano que indica se é necessário permitir curingas para grupos de consultas. Se for 0, os curingas estarão desativados; se for 1, os curingas estarão ativados. Quando curingas são permitidos, você pode usar "*" ou "?" para especificar vários grupos de consultas ao executar consultas. Para obter mais informações, consulte Curingas.

Propriedade JSON: `query_group_wild_card`

Perfis de usuário

Uma lista de perfis de usuário separados por vírgulas. Quando membros com esse perfil de usuário executam consultas no banco de dados, as consultas são roteadas para a fila associada ao respectivo perfil de usuário. Para obter mais informações sobre perfis de usuário, consulte Controle de acesso com base em função (RBAC).

Propriedade JSON: `user_role`

Caractere curinga de perfis de usuário

Um valor Booliano que indica se é necessário permitir curingas para grupos de consultas. Se for 0, os curingas estarão desativados; se for 1, os curingas estarão ativados. Quando curingas são permitidos, você pode usar "*" ou "?" para especificar vários grupos de consultas ao executar consultas. Para obter mais informações, consulte Curingas.

Propriedade JSON: `user_role_wild_card`

Timeout (Tempo limite) (ms)

O tempo limite do WLM (`max_execution_time`) está obsoleto. Não está disponível ao usar o WLM automático. Em vez disso, crie uma regra de monitoramento de consulta (QMR) usando `query_execution_time` para limitar o tempo de execução decorrido para uma consulta. Para obter mais informações, consulte Regras de monitoramento de consultas do WLM.

O tempo máximo, em milissegundos, durante o qual as consultas poderão ser executadas até serem canceladas. Em alguns casos, uma consulta somente leitura, como uma declaração SELECT, poderá ser cancelada devido a um tempo limite do WLM Nesses casos, o WLM tenta rotear a consulta para a próxima fila correspondente com base nas regras de atribuição de filas do WLM. Se não corresponder a nenhuma outra definição de fila, a consulta será cancelada; ela não será atribuída à fila padrão. Para obter mais informações, consulte Salto na fila de consultas do WLM. O tempo limite do WLM não se aplica a uma consulta que tenha atingido o estado `returning`. Para exibir o estado de uma consulta, consulte a tabela de sistema STV_WLM_QUERY_STATE.

Propriedade JSON: `max_execution_time`

Memory (%) (Memória (%))

A porcentagem de memória a ser alocada à fila. Se especificar uma porcentagem de memória para pelo menos uma das filas, será necessário especificar uma porcentagem para todas as outras filas até um total de 100%. Se a sua alocação de memória for inferior a 100% entre

todas as filas, a memória não alocada será gerenciada pelo serviço. O serviço pode conceder temporariamente essa memória não alocada a uma fila que solicita memória adicional para processamento.

Propriedade JSON: `memory_percent_to_use`

Regras de monitoramento de consulta

Você pode usar as regras de monitoramento da consulta do WLM para monitorar continuamente as filas do WLM para consultas com base em critérios, ou predicados, especificados. Por exemplo, convém monitorar consultas com a tendência de consumir recursos de sistema excessivos e iniciar uma ação especificada quando uma consulta exceder os limites de performance especificados.

> **Note**
>
> Se você optar por criar regras programaticamente, será altamente recomendável usar o console para gerar o JSON incluído por você na definição do parameter group.

Você associa uma regra de monitoramento de consulta a uma fila de consultas específica. Pode haver até 25 regras por fila e o limite total para todas as filas é de 25 regras.

Propriedade JSON: `rules`

Hierarquia de propriedades JSON:

```
rules
    rule_name
    predicate
        metric_name
        operator
        value
    action
        value
```

Para cada regra, especifique as seguintes propriedades:

- `rule_name` – Os nomes de regra devem ser exclusivos na configuração do WLM. Os nomes de regra podem ter até 32 caracteres alfanuméricos ou sublinhados e não podem conter espaços ou aspas. Você pode ter até oito regras por fila, e o limite total para todas as filas é de oito regras.

  - `predicate` – Você pode ter até três predicados por regra. Para cada predicado, especifique as propriedades a seguir.
    - `metric_name` – Para obter uma lista de métricas, consulte Métricas de monitoramento da consulta no Guia do desenvolvedor de banco de dados do Amazon Redshift.
    - `operator` – Operações são =, < e >.
    - `value` – O valor limite para a métrica especificada que aciona uma ação.
- `action` – Cada regra está associada a uma única ação. As ações válidas são:
  - `log`
  - hop (disponível somente com o WLM manual)
  - `abort`
  - `change_query_priority` (disponível somente com o WLM automático)

O exemplo a seguir mostra o JSON de uma regra de monitoramento de consulta do WLM chamado `rule_1`, com dois predicados e a ação 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"
          }
        ]
```

Para obter mais informações sobre cada uma dessas propriedades e estratégias para configurar filas de consulta, consulte Implementar gerenciamento de workload no Guia do desenvolvedor de banco de dados do Amazon Redshift.

# Configurar o parâmetro wlm_json_configuration usando a AWS CLI

Para configurar o WLM, você modifica o parâmetro `wlm_json_configuration`. O tamanho máximo do valor da propriedade `wlm_json_configuration` é de 8.000 caracteres. O valor é formatado em JSON (JavaScript Object Notation). Se você configurar o WLM usando a AWS CLI, a API do Amazon Redshift ou um dos AWS SDKs, use o restante desta seção para saber como construir a estrutura JSON do parâmetro `wlm_json_configuration`.

> **Note**
>
> Se você configurar o WLM usando o console do Amazon Redshift, você não precisa entender a formatação JSON porque o console oferece uma maneira fácil de adicionar filas e configurar suas propriedades. Para obter mais informações sobre como configurar o WLM usando o console, consulte Modificar um parameter group.

Exemplo

O exemplo a seguir é a configuração do WLM padrão, que define uma fila com WLM automático.

```
{
   "auto_wlm": true
}
```

Exemplo

O exemplo a seguir é uma configuração do WLM personalizada que define uma fila do WLM com um nível de simultaneidade (slots de consulta) de cinco.

```
{
   "query_concurrency":5
}
```

Sintaxe

A configuração do WLM padrão é muito simples, somente com uma fila e uma propriedade. Você pode adicionar mais filas e configurar várias propriedades para cada fila na estrutura JSON. A seguinte sintaxe representa a estrutura JSON que você usa para configurar várias filas com várias propriedades:

```
[
   {
      "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",
                ...
             }
             ...

         ]"
   }
]
```

No exemplo anterior, as propriedades representativas que começam com q1 são objetos em uma matriz da primeira fila. Cada um desses objetos é um par de nome/valor; `name` e `value` definem juntos as propriedades do WLM da primeira fila. As propriedades representativas que começam com q2 são objetos em uma matriz da segunda fila. Se precisar de mais filas, você adicionará outra matriz para cada fila e definirá as propriedades de cada objeto.

Ao modificar a configuração do WLM, você deve incluir na estrutura completa das filas, mesmo se quiser alterar somente uma propriedade dentro de uma fila. Isso porque toda a estrutura JSON é passada como uma string do valor do parâmetro `wlm_json_configuration`.

## Formatar o comando da AWS CLI

O parâmetro `wlm_json_configuration` exige um formato específico quando você usa a AWS CLI. O formato usado por você depende do sistema operacional do cliente. Como os sistemas operacionais têm maneiras diferentes de envolver a estrutura JSON, ela é passada corretamente pela linha de comando. Para obter detalhes sobre como construir o comando apropriado nos sistemas operacionais Linux, Mac OS X e Windows, consulte as seções a seguir. Para obter mais informações sobre as diferenças nas estruturas de dados JSON na AWS CLI em geral, consulte Citando strings no Manual do usuário do AWS Command Line Interface.

Exemplos

O exemplo de comando a seguir configura o WLM manual para um grupo de parâmetros chamado `example-parameter-group`. A configuração permite a aceleração de consulta breve com um tempo máximo de execução para consultas breves definido como 0, o que instrui o WLM a definir o valor de forma dinâmica. A configuração de `ApplyType` é `dynamic`. Essa configuração significa que todas as alterações feitas em propriedades dinâmicas no parâmetro serão aplicadas automaticamente, a menos que outras alterações estáticas tenham sido feitas na configuração. A configuração define três filas com o seguinte:

- A primeira fila permite que os usuários especifiquem `report` como um rótulo (conforme especificado na propriedade `query_group`) nas consultas para ajudar a rotear consultas para essa fila. Como as pesquisas com curinga são permitidas para o rótulo `report*`, este não precisa estar exato para que consultas sejam roteadas para a fila. Por exemplo, `reports` e `reporting` correspondem a esse grupo de consultas. A fila recebe 25 por cento da memória total em todas as filas e pode executar até quatro consultas ao mesmo tempo. As consultas estão limitadas a um tempo máximo de 20.000 milissegundos (ms). O modo está definido como automático, portanto, quando os slots de consulta da fila estão lotados, as consultas qualificadas são enviadas para um cluster de escalabilidade.
- A segunda fila permite que usuários membros de grupos `admin` ou `dba` no banco de dados tenham as consultas roteadas para a fila tendo em vista o processamento. Como as pesquisas com curinga estão desabilitadas para grupos de usuários, os usuários devem corresponder exatamente a grupos no banco de dados de maneira que as consultas sejam roteadas para a fila. A fila recebe 40% da memória total em todas as filas e pode executar até cinco consultas ao mesmo tempo. O modo está definido como desativado, portanto, todas as consultas enviadas por membros nos grupos de dba e administrador são executadas no cluster principal.
- A última fila na configuração é a padrão. Essa fila recebe 35% da memória total em todas as filas e pode processar até cinco consultas ao mesmo tempo. O modo está definido como automático.

> **Note**
>
> O exemplo é mostrado em várias linhas para fins de demonstração. Os comandos reais não devem ter quebras de linha.

```
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}
]'
```

Veja a seguir um exemplo de como configurar regras de monitoramento de consultas do WLM para uma configuração de WLM automático. O exemplo cria um parameter group chamado `example-monitoring-rules`. A configuração define as mesmas três filas do exemplo anterior, mas `query_concurrency` e `memory_percent_to_use` não são mais especificadas. A configuração também adiciona as seguintes regras e prioridades de consulta:

- A primeira fila define uma regra chamada `rule_1`. A regra tem dois predicados: `query_cpu_time > 10000000` e `query_blocks_read > 1000`. A ação da regra é `log`. A prioridade dessa fila é `Normal`.
- A segunda fila define uma regra chamada `rule_2`. A regra tem dois predicados: `query_execution_time > 600000000` e `scan_row_count > 1000000000`. A ação da regra é `abort`. A prioridade dessa fila é `Highest`.
- A última fila na configuração é a padrão. A prioridade dessa fila é `Low`.

> **Note**
>
> O exemplo é mostrado em várias linhas para fins de demonstração. Os comandos reais não devem ter quebras de linha.

```
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
} ]'
```

Configurar o WLM usando a AWS CLI na linha de comando com um arquivo JSON

É possível modificar o parâmetro `wlm_json_configuration` usando a AWS CLI e transmitir o valor do argumento `parameters` como um arquivo JSON.

```
aws redshift modify-cluster-parameter-group --parameter-group-name
 myclusterparaametergroup --parameters file://modify_pg.json
```

Os argumentos para `--parameters` são armazenados no arquivo `modify_pg.json`. A localização do arquivo é especificada no formato do seu sistema operacional. Para obter mais informações, consulte Carregar parâmetros de um arquivo. A seguir são exibidos exemplos do conteúdo do arquivo JSON `modify_pg.json`.

```
[
    {
        "ParameterName": "wlm_json_configuration",
        "ParameterValue": "[{\"user_group\":\"example_user_group1\",\"query_group\":
 \"example_query_group1\", \"query_concurrency\":7},{\"query_concurrency\":5}]"
    }
]
```

```
[
    {
        "ParameterName": "wlm_json_configuration",
        "ParameterValue": "[{\"query_group\":[\"reports\"],\"query_group_wild_card\":0,
\"query_concurrency\":4,\"max_execution_time\":20000,\"memory_percent_to_use\":25},
{\"user_group\":[\"admin\",\"dba\"],\"user_group_wild_card\":1,\"query_concurrency\":5,
\"memory_percent_to_use\":40},{\"query_concurrency\":5,\"memory_percent_to_use\":35},
{\"short_query_queue\": true, \"max_execution_time\": 5000 }]",
        "ApplyType": "dynamic"
    }
]
```

Regras para configurar o WLM usando a AWS CLI na linha de comando nos sistemas operacionais Linux e macOS X

Siga estas regras para executar um comando da AWS CLI com parâmetros em uma linha:

- Toda a estrutura JSON deve estar entre aspas simples (‘) e colchetes ([ ]).

- Todos os nomes e valores de parâmetro devem estar entre aspas duplas (").
- Dentro do valor `ParameterValue`, você deve colocar toda a estrutura aninhada entre aspas duplas (") e colchetes ([ ]).
- Dentro da estrutura aninhada, cada uma das propriedades e dos valores para cada fila deve estar entre chaves ({ }).
- Dentro da estrutura aninhada, você deve usar o caractere de escape de barra invertida (\) antes das aspas duplas (").
- Para pares de nome/valor, dois-pontos (:) separa cada propriedade do valor.
- Cada par de nome/valor é separado de outros por uma vírgula (,).
- Várias filas são separadas por uma vírgula (,) entre o fim da chave (}) de uma fila e o início da chave ({) da próxima fila.

Regras para configurar o WLM usando a AWS CLI no Windows PowerShell em sistemas operacionais Microsoft Windows

Siga estas regras para executar um comando da AWS CLI com parâmetros em uma linha:

- Toda a estrutura JSON deve estar entre aspas simples (‘) e colchetes ([ ]).
- Todos os nomes e valores de parâmetro devem estar entre aspas duplas (").
- Dentro do valor `ParameterValue`, você deve colocar toda a estrutura aninhada entre aspas duplas (") e colchetes ([ ]).
- Dentro da estrutura aninhada, cada uma das propriedades e dos valores para cada fila deve estar entre chaves ({ }).
- Dentro da estrutura aninhada, você deve usar o caractere de escape de barra invertida (\) antes das aspas duplas (") e do caractere de escape de barra invertida (\). Esse requisito significa que você usará três barras invertidas e aspas duplas para verificar se as propriedades são passadas corretamente (\\\").
- Para pares de nome/valor, dois-pontos (:) separa cada propriedade do valor.
- Cada par de nome/valor é separado de outros por uma vírgula (,).
- Várias filas são separadas por uma vírgula (,) entre o fim da chave (}) de uma fila e o início da chave ({) da próxima fila.

Regras para configurar o WLM usando o prompt de comando em sistemas operacionais Windows

Siga estas regras para executar um comando da AWS CLI com parâmetros em uma linha:

- Toda a estrutura JSON deve estar entre aspas duplas (“) e colchetes ([ ]).
- Todos os nomes e valores de parâmetro devem estar entre aspas duplas (").
- Dentro do valor `ParameterValue`, você deve colocar toda a estrutura aninhada entre aspas duplas (") e colchetes ([ ]).
- Dentro da estrutura aninhada, cada uma das propriedades e dos valores para cada fila deve estar entre chaves ({ }).
- Dentro da estrutura aninhada, você deve usar o caractere de escape de barra invertida (\) antes das aspas duplas (") e do caractere de escape de barra invertida (\). Esse requisito significa que você usará três barras invertidas e aspas duplas para verificar se as propriedades são passadas corretamente (\\\").
- Para pares de nome/valor, dois-pontos (:) separa cada propriedade do valor.
- Cada par de nome/valor é separado de outros por uma vírgula (,).
- Várias filas são separadas por uma vírgula (,) entre o fim da chave (}) de uma fila e o início da chave ({) da próxima fila.

# Gerenciamento de grupos de parâmetros usando o console

Você pode visualizar, criar, modificar e excluir grupos de parâmetros no console do Amazon Redshift.

Você pode visualizar qualquer um dos grupos de parâmetros para ver um resumo dos valores dos parâmetros e do gerenciamento do workload (WLM - workload management). Parâmetros de grupo são exibidos na guia Parameters (Parâmetros), e Workload queues (Filas de workloads) são exibidas na guia Workload Management (Gerenciamento do workload).

## Criar um parameter group

Para definir valores de parâmetros diferentes do grupo de parâmetros padrão, você pode criar seu próprio grupo de parâmetros.

Para criar um parameter group

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Configurations (Configurações) e Workload management (Gerenciamento de workload) para exibir a página Workload management (Gerenciamento de workload).
3. Escolha Create (Criar) para exibir a janela Create parameter group (Criar grupo de parâmetros).
4. Insira um valor para Parameter group name (Nome do grupo de parâmetros) e Description (Descrição).
5. Para criar o grupo de parâmetros, escolha Create (Criar).

## Modificar um parameter group

Você pode modificar parâmetros para alterar as configurações de parâmetro e as propriedades de configuração de WLM.

> **Note**
>
> Você não pode modificar o grupo de parâmetro padrão.

Para modificar um grupo de parâmetros

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Configurations (Configurações) e Workload management (Gerenciamento de workload) para exibir a página Workload management (Gerenciamento de workload).
3. Escolha o grupo de parâmetros que você deseja modificar para exibição na página de detalhes, com as guias Parameters (Parâmetros) e Workload management (Gerenciamento do workload).
4. Use a guia Parameters (Parâmetros) para visualizar as configurações atuais dos parâmetros.
5. Escolha Edit parameters (Editar parâmetros) para habilitar a alteração das configurações destes parâmetros:

   - `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

Para mais informações sobre esses parâmetros, consulte Grupos de parâmetros do Amazon Redshift.

6. Insira suas alterações e escolha Save (Salvar) para atualizar o grupo de parâmetros.

Para modificar a configuração do WLM de um grupo de parâmetros

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Configurations (Configurações) e Workload management (Gerenciamento de workload) para exibir a página Workload management (Gerenciamento de workload).
3. Escolha o grupo de parâmetros que você deseja modificar para exibição na página de detalhes, com as guias Parameters (Parâmetros) e Workload management (Gerenciamento do workload).
4. Escolha a guia Workload management (Gerenciamento do workload) para visualizar a configuração do WLM.
5. Escolha Edit workload queues (Editar filas de workload) para editar a configuração do WLM.
6. (Opcional) Selecione Enable short query acceleration (Habilitar aceleração de consultas breves) para habilitar a aceleração de consultas breves (SQA).

Ao habilitar a SQA, Tempo máximo de execução de consultas breves (1 a 20 segundos) é definido para Dinâmico por padrão. Para definir o tempo de execução máximo para um valor fixo, escolha um valor de 1–20.

7. Complete uma ou mais das seguintes opções para modificar a configuração da fila:

   - Escolha Switch WLM mode (Alternar modo de WLM) para selecionar entre Automatic WLM (WLM automático) e Manual WLM (WLM manual).

     Com Automatic WLM (WLM automático), os valores de Memory (Memória) e Concurrency on main (Simultaneidade no principal) são definidos como auto (automático).
   - Para criar uma fila, escolha Edit workload queues (Editar filas de workload) e escolha Add Queue (Adicionar fila).
   - Para modificar uma fila, altere valores de propriedades na tabela. Dependendo do tipo da fila, as propriedades podem incluir o seguinte:
     - Queue name (Nome da fila) pode ser alterado.
     - Memory (%) (Memória (%))
     - Concurrency on main (Simultaneidade no principal) cluster
     - Concurrency Scaling mode (Modo de escalabilidade da simultaneidade) pode estar off (desligado) ou auto (automático).
     - Timeout (Tempo limite) (ms)
     - User groups (Grupos de usuários)
     - Query groups (Grupos de consultas)
     - Perfis de usuário

     Para obter mais informações sobre essas propriedades, consulte Propriedades para o parâmetro wlm_json_configuration.

     > **Important**
     >
     > Se você alterar um nome de fila, o valor da dimensão `QueueName` de métricas de fila do WLM (como WLMQueueLength, WLMQueueWaitTime, WLMQueriesCompletedPerSecond, WLMQueryDuration, WLMRunningQueries e assim por diante) também mudará. Portanto, se você alterar o nome de uma fila, pode ser necessário alterar os alarmes do CloudWatch que você configurou.

- Para alterar a ordem das filas, escolha os botões de seta para cima e para baixo.
- Para excluir uma fila, selecione Excluir na linha da fila na tabela.

8. (Opcional) Selecione Defer dynamic changes until reboot (Adiar mudanças dinâmicas até a reinicialização) para que as alterações sejam aplicadas aos clusters associados após a próxima reinicialização.

> **Note**
>
> Algumas mudanças exigem uma reinicialização do cluster independentemente desta configuração. Para ter mais informações, consulte Propriedades dinâmicas e estáticas do WLM.

9. Escolha Salvar.

## Criação ou modificação de uma regra de monitoramento de consulta usando o console

Você pode usar o console do Amazon Redshift para criar e modificar regras de monitoramento de consulta WLM. Regras de monitoramento de consulta fazem parte do parâmetros de configuração do WLM para um parameter group. Se você modificar uma regra de monitoramento de consulta (QMR), a mudança acontecerá automaticamente sem a necessidade de modificar o cluster. Para obter mais informações, consulte Regras de monitoramento de consultas do WLM.

Ao criar uma regra, você define o nome de regra, um ou mais predicados e uma ação.

Quando você salva a configuração do WLM incluindo uma regra, você pode visualizar o código JSON para a definição da regra como parte do JSON para o parâmetro de configuração do WLM.

Para criar uma regra de monitoramento de consulta

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Configurations (Configurações) e Workload management (Gerenciamento de workload) para exibir a página Workload management (Gerenciamento de workload).

3. Escolha o grupo de parâmetros que você deseja modificar para exibição na página de detalhes, com as guias Parameters (Parâmetros) e Workload management (Gerenciamento do workload).
4. Escolha a guia Workload management (Gerenciamento do workload) e escolha Edit workload queues (Editar filas de workload)  para editar a configuração de WLM.
5. Adicione uma nova regra usando um modelo predefinido ou criado do zero.

   Para usam um modelo predefinido, faça o seguinte:

   1. Escolha Add rule from template (Adicionar regra de modelo) no grupo Query monitoring rules (Regras de monitoramento de consultas). A listra de modelos de regras é exibida.
   2. Escolha um ou mais modelos de regra. Quando você escolhe Save (Salvar), o WLM cria uma regra para cada modelo que você escolher.
   3. Insira ou confirme valores para a regra incluindo Rule names (Nomes de regras), Predicates (Predicados) e Actions (Ações).
   4. Escolha Salvar.

   Para adicionar uma nova regra criada do zero, faça o seguinte:

   1. Para adicionar mais predicados, escolha Add predicate (Adicionar predicado). Você pode ter até três predicados para cada regra. Se todos os predicados são atendidos, o WLM dispara ação associada.
   2. Escolha uma Ação. Cada regra tem uma ação.
   3. Escolha Salvar.

O Amazon Redshift gera seu parâmetro de configuração WLM no formato JSON e o exibe na seção JSON.

## Exclusão de um grupo de parâmetros

Você pode excluir um parameter group se você não for precisar mais dele e ele não estiver associado a qualquer cluster. Você pode excluir somente grupos de parâmetros personalizados.

Para excluir um parameter group

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

2. No menu de navegação, escolha Configurations (Configurações) e Workload management (Gerenciamento de workload) para exibir a página Workload management (Gerenciamento de workload).
3. Em Parameter groups, escolha o parameter group que deseja modificar.

> **Note**
>
> Não é possível excluir o grupo de parâmetros padrão.

4. Escolha Delete (Excluir) e confirme que deseja excluir o grupo de parâmetros.

### Associar um parameter group a um cluster

Quando você executa um cluster, você deve associá-lo a um parameter group. Se você quiser alterar o parameter group mais tarde, você pode modificar o cluster e escolher um parameter group diferente.

## Gerenciar grupos de parâmetros usando a AWS CLI e a API do Amazon Redshift

É possível usar as seguintes operações do Amazon Redshift na AWS CLI para gerenciar grupos de parâmetros.

- create-cluster-parameter-group
- delete-cluster-parameter-group
- describe-cluster-parameters
- describe-cluster-parameter-groups
- describe-default-cluster-parameters
- modify-cluster-parameter-group
- reset-cluster-parameter-group

Você pode usar as operações de API do Amazon Redshift a seguir para gerenciar grupos de parâmetros.

- CreateClusterParameterGroup

- DeleteClusterParameterGroup
- DescribeClusterParameters
- DescribeClusterParameterGroups
- DescribeDefaultClusterParameters
- ModifyClusterParameterGroup
- ResetClusterParameterGroup

# Integração do Amazon Redshift com um Parceiro da AWS

Ao trabalhar com o Amazon Redshift, você pode integrar com os Parceiros da AWS na página Detalhes do cluster no console do Amazon Redshift. Em Detalhes do cluster, você pode acelerar a integração de dados no seu data warehouse do Amazon Redshift com aplicações de Parceiros da AWS. Você também pode unir e analisar dados de diferentes fontes juntamente com dados existentes em seu cluster. Antes de concluir a integração com a Informatica, você deve adicionar os endereços IP do parceiro à lista de permissões do tráfego de entrada. Os seguintes Parceiros da AWS podem se integrar ao Amazon Redshift:

- Datacoral
- Etleap
- Fivetran
- SnapLogic
- Stitch
- Upsolver
- Matillion (pré-visualizar)
- Sisense (pré-visualizar)
- Thoughtspot

Os Parceiros da AWS podem se integrar ao Amazon Redshift usando a AWS CLI ou operações de API do Amazon Redshift. Para obter mais informações, consulte Referência de comandos da AWS CLI ou a Referência de API do Amazon Redshift.

## Integração de Parceiros da AWS usando o console do Amazon Redshift

Use o procedimento a seguir para integrar um cluster a um Parceiro da AWS.

Para integrar um cluster do Amazon Redshift a parceiro da AWS

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters.

3. Escolha o cluster que você deseja usar.
4. Escolha Adicionar integração para parceiros. A página Escolher parceiro abre com detalhes sobre os Parceiros da AWS disponíveis.
5. Escolha um Parceiro da AWS e então escolha Próximo.

   Mais detalhes sobre o Parceiro da AWS escolhido aparecem, juntamente com detalhes sobre o cluster que você está integrando. A seção Detalhes do cluster inclui informações que você fornece no site do Parceiro da AWS, como o Identificador de cluster, o Endpoint, o Nome do banco de dados e o Nome de usuário(que é um nome de usuário do banco de dados). Essas informações são enviadas para o parceiro que você escolheu.
6. Escolha Adicionar parceiro para abrir o site do Parceiro da AWS.
7. Configure a integração com seu cluster do Amazon Redshift no site do parceiro. No site do parceiro, você pode selecionar e configurar as origens dos dados carregadas no cluster do Amazon Redshift. Você também pode definir transformações adicionais de extração, carregamento e transformação (ELT) para processar seus dados de negócios, juntá-los a outros conjuntos de dados e construir visualizações consolidadas para análise e emissão de relatórios.

É possível visualizar e gerenciar integrações de Parceiros da AWS a partir da guia de detalhes do cluster Propriedades. A seção Integrações lista o nome do Parceiro que você pode usar para vincular ao site do Parceiro da AWS, o Status da integração, o Banco de dados que recebe os dados e a Última conexão bem-sucedida que pode ter atualizado o cluster.

Os valores de status possíveis são os seguintes:

- Ativo — O Parceiro da AWS pode se conectar ao cluster e concluir tarefas configuradas.
- Inativo — A integração do Parceiro da AWS não existe.
- Falha de tempo de execução — O Parceiro da AWS pode se conectar ao cluster, porém não pode concluir tarefas configuradas.
- Falha de conexão — O Parceiro da AWS não pode se conectar ao cluster.

Depois que você excluir uma integração do Parceiro da AWS do Amazon Redshift, os dados continuam fluindo para o seu cluster. Conclua a exclusão no site do parceiro.

# Carregar dados com parceiros da AWS

Além de integrar um parceiro a um cluster do Amazon Redshift, você também pode mover dados de mais de 30 fontes para o cluster do Amazon Redshift usando as ferramentas de carregamento de dados do nosso parceiro. Antes de fazer isso, você deve adicionar os endereços IP do parceiro (encontrados abaixo) à lista de permissões das regras de entrada. Para obter mais informações sobre como adicionar regras a um grupo de segurança do Amazon EC2, consulte Autorizar tráfego de entrada para as instâncias no Guia do usuário do Amazon EC2 para instâncias do Linux. Observe que, embora a ferramenta Informatica Data Loader seja gratuita, taxas de entrada de dados poderão ser aplicadas dependendo das fontes de dados e dos destinos que você escolher.

É possível carregar dados dos seguintes parceiros:

- Informatica: endereços IP

Como integrar um cluster do Amazon Redshift com a Informatica

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha a integração de parceiro da AWS, depois selecione o parceiro com o qual deseja integrar o cluster.
3. Escolha Complete <partner-name> integration (Concluir integração com <partner-name>). Você será redirecionado para o site de integração do parceiro.
4. Insira os detalhes necessários no site do parceiro e conclua a integração.

# Comprar nós reservados do Amazon Redshift

## Visão geral

Na AWS, as cobranças que você acumula pelo uso do Amazon Redshift são baseadas em nós de computação. Cada nó de computação é faturado por uma taxa horária. A taxa horária varia de acordo com fatores como a região, o tipo de nó e se é possível ou não aplicar ao nó as definições de preços sob demanda ou de preços de nós reservados.

O preço de nós sob demanda é a opção mais cara, porém é a mais flexível no Amazon Redshift. Com as taxas sob demanda, você é cobrado somente pelos nós de computação que possui em um cluster em execução. Se você fechar ou excluir um cluster, não será mais cobrado pelos nós de computação que estavam nesse cluster. Você é cobrado apenas pelos nós de computação que usa, e nada além disso. A taxa horária cobrada para cada nó de computação varia de acordo com fatores como a região e o tipo do nó.

A definição de preço dos nós reservados é menos cara do que a definição de preços sob demanda, pois os nós de computação são faturados por uma taxa horária com desconto. No entanto, para receber essas taxas com desconto, você precisa comprar as ofertas de nós reservados. Quando você compra uma oferta, faz uma reserva. O ato da reserva define uma taxa com desconto para cada nó que você reserva para a duração da reserva. A taxa com desconto em uma oferta varia de acordo com fatores como região, tipo de nó, duração e opção de pagamento.

É possível designar um nó como um nó reservado chamando a operação de API `PurchaseReservedNodeOffering` ou escolhendo Purchase reserved nodes (Comprar nós reservados) no console do Amazon Redshift. Ao comprar um nó reservado, você deve especificar uma região da AWS, tipo de nó, condição, quantidade de nós e tipo de oferta para o tipo de nó reservado aplicável. O nó reservado só pode ser usado na região da AWS designada.

Este tópico discute o que são ofertas de nós reservadas e como você pode comprá-las para reduzir o custo de execução de seus clusters do Amazon Redshift. Este tópico discute as taxas de maneira geral, por exemplo, taxas sob demanda ou com desconto, para que você possa compreender os conceitos de definição de preços e como a definição de preços afeta o faturamento. Para obter mais informações sobre taxas específicas, consulte Preço do Amazon Redshift.

# Sobre as ofertas de nós reservados

Se você pretende manter seu cluster do Amazon Redshift em execução continuamente por um período prolongado, deve considerar a compra de ofertas de nós reservadas. Essas ofertas representam uma economia significativa em relação aos preços cobrados sob demanda, mas exigem que você reserve nós de computação e se comprometa a pagar por eles por um período de um ou três anos.

A reserva de nós é um conceito de faturamento usado estritamente para determinar a taxa que é cobrada pelos nós. Reservar um nó não cria de fato nenhum nó para você. Você é cobrado pelos nós reservados independentemente do uso, o que significa que é preciso pagar por cada nó reservado pelo período de duração da reserva, não importando se você tem ou não algum nó em um cluster em execução ao qual a taxa com desconto se aplica.

Na fase de avaliação do seu projeto, ou quando você está desenvolvendo uma prova de conceito, a definição de preço sob demanda proporciona a flexibilidade de pagamento conforme o uso, ou seja, de pagar somente pelo que você usa, e de parar de pagar a qualquer momento, ao desligar ou excluir os clusters. Depois de estabelecer as necessidades de seu ambiente de produção e ao iniciar a fase de implementação, você deve considerar a reserva de nós de computação e a compra de uma ou mais oferta.

Um oferta pode se referir a um ou mais nós de computação. Você especifica o número de nós de computação a serem reservados quando compra a oferta. Você pode optar por comprar uma oferta com vários nós de computação ou pode preferir comprar várias ofertas e especificar um determinado número de nós de computação em cada oferta.

Como exemplo, veja a seguir algumas maneiras válidas de comprar uma oferta para três nós de computação:

- Compre uma oferta e especifique três nós de computação.
- Compre duas ofertas e especifique um nó de computação para a primeira oferta e dois nós de computação para a segunda oferta.
- Compre três ofertas e especifique um nó de computação para cada uma das ofertas.

# Comparação das definições de preço entre as ofertas de nós reservados

O Amazon Redshift oferece várias opções de pagamento para ofertas. A opção de pagamento que você escolhe influencia a programação dos pagamentos e a taxa com desconto que é cobrada pela reserva. Quanto mais você paga adiantado pela reserva, mais você economiza no valor total.

As opções de pagamento disponíveis para as ofertas são apresentadas a seguir. As ofertas estão relacionadas na ordem de menor para maior economia em relação às taxas sob demanda.

> **Note**
>
> Será cobrada a taxa horária aplicável por cada hora pelo período de duração específico da reserva, independente de você usar o nó reservado ou não. A opção de pagamento apenas determina a frequência dos pagamentos e o desconto a ser aplicado. Para ter mais informações, consulte Sobre as ofertas de nós reservados.

Comparação de ofertas de nós reservados

| Opção de pagamento | Programação de pagamentos | Economias comparativas | Duração | Cobranças adiantadas | Cobranças mensais recorrentes |
|---|---|---|---|---|---|
| Sem taxas iniciais | Prestações mensais pelo período de duração da reserva. Nenhum pagamento adiantado. | Um desconto de cerca de 20 por cento em relação às taxas sob demanda. | Período de vigência de um ou três anos | Nenhum | Sim |
| Adiantado parcial | Pagamento adiantado parcial e prestações mensais pelo período de duração da reserva. | Desconto entre 41 e 73 por cento dependendo do período de duração. | Período de vigência de um ou três anos | Sim | Sim |
| Adiantado integral | Pagamento total adiantado para a | Desconto entre 42 e 76 por cento, | Período de vigência | Sim | Nenhum |

| Opção de pagamento | Programação de pagamentos | Economias comparativas | Duração | Cobranças adiantadas | Cobranças mensais recorrentes |
|---|---|---|---|---|---|
| | reserva. Nenhuma cobrança mensal. | dependendo do período de duração. | de um ou três anos | | |

As opções e durações específicas estão sujeitas à disponibilidade.

> **Note**
>
> Se você adquiriu anteriormente ofertas de Utilização pesada para o Amazon Redshift, a oferta comparável é a oferta Inicial parcial.

## Como os nós reservados funcionam

Com as ofertas de nós reservados, você paga de acordo com os termos de pagamento descritos na seção anterior. Você paga dessa maneira quer você já tenha um cluster em execução, quer você execute um cluster depois de fazer uma reserva.

Quando você compra uma oferta, sua reserva fica em status payment-pending até que a reserva seja processada. Se o processamento da reserva falhar, o status exibido será payment-failed e você poderá tentar processá-lo novamente. Uma vez que sua reserva seja processada com êxito, o status muda para active. A taxa com desconto aplicável para a reserva não é aplicada à sua fatura até que o status seja alterado para active. Após o fim do período de duração da reserva, o status é alterado para retired, mas você pode continuar a acessar as informações sobre a reserva para acompanhar o histórico. Quando uma reserva é retired, seus clusters continuam a ser executados mas você pode ser cobrado pela taxa sob demanda, a menos que possua uma outra reserva que aplique a definição de preços com desconto para os nós.

Os nós reservados são específicos da região na qual você compra a oferta. Se você está comprando uma oferta usando o console do Amazon Redshift, selecione a região da AWS na qual deseja comprar a oferta e, em seguida, conclua o processo de reserva. Se você comprar uma oferta programaticamente, a região será determinada pelo endpoint do Amazon Redshift ao qual você se conecta. Para obter mais informações sobre regiões do Amazon Redshift, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

Para garantir que a taxa com desconto seja aplicada a todos os nós quando você executa um cluster, certifique-se de que a região, o tipo do nó e o número de nós selecionados correspondam a uma ou mais reservas ativas. Caso contrário, os nós que não corresponderem a uma reserva ativa serão cobrados pela taxa sob demanda.

Para um cluster em execução, se você ultrapassar o número de nós que reservou, começará a acumular cobranças pelos nós adicionais pela taxa sob demanda. Essa acumulação significa que é possível que você seja cobrado com taxas diferentes para nós no mesmo cluster, dependendo de quantos nós reservou. Você pode comprar uma outra oferta para cobrir os nós adicionais e, dessa forma, a taxa com desconto será aplicada a esses nós pelo restante do período de duração, uma vez que o status da reserva se torne active.

Se você redimensionar seu cluster para um tipo de nó diferente e não tiver reservado nós daquele tipo, será cobrado pela taxa sob demanda. Você pode comprar uma outra oferta com o novo tipo de nó se desejar receber taxas com desconto para o seu cluster redimensionado. Contudo, você também continuará pagando pela reserva original até que o período de duração termine. Se você precisar alterar suas reservas antes que o prazo expire, crie um caso de suporte usando o Console da AWS.

## Nós reservados e faturamento consolidado

Os benefícios da definição de preços dos nós reservados são compartilhados quando a conta que faz a compra é parte de um conjunto de contas que são faturadas sob uma conta pagante de faturamento consolidado. A utilização por hora em todas as subcontas é agregada todo mês na conta pagante. Em geral, isso é útil para empresas em que há equipes ou grupos funcionais diferentes; dessa forma, a lógica usual dos nós reservados é aplicada para calcular a conta. Para obter mais informações, consulte Faturamento consolidado no Manual do usuário do AWS Billing.

## Exemplos de nós reservados

Os cenários nesta seção demonstram como os nós acumulam as cobranças com base nas taxas sob demanda e nas taxas com desconto, usando os seguintes detalhes de reserva:

- Região: Oeste dos EUA (Oregon)
- Tipo de nó: ra3.xlplus
- Opção de pagamento: nenhum pagamento adiantado
- Duração: um ano
- Número de nós reservados: 16

## Exemplo 1

Você tem um cluster na região Oeste dos EUA (Oregon) com 20 nós.

Neste cenário, 16 nós recebem a taxa com o desconto da reserva, mas os 4 nós adicionais no cluster são faturados pela taxa sob demanda.

## Exemplo 2

Você tem um cluster na região Oeste dos EUA (Oregon) com 12 nós.

Neste cenário, todos os 12 nós no cluster recebem a taxa com desconto da reserva. Contudo, você também paga pelos demais nós reservados na reserva, mesmo que não tenha no momento um cluster em execução ao qual eles se aplicam.

## Exemplo 3

Você tem um cluster na região Oeste dos EUA (Oregon) com 12 nós. Depois de vários meses executando o cluster com essa configuração, é preciso adicionar nós ao cluster. Você redimensiona o cluster, escolhendo o mesmo tipo de nó e especificando um total de 16 nós.

Neste cenário, a cobrança é feita pela taxa com desconto para os 16 nós. Sua cobrança permanece a mesma durante um ano completo, pois o número de nós existentes no cluster é igual ao número de nós reservados.

## Exemplo 4

Você tem um cluster na região Oeste dos EUA (Oregon) com 16 nós. Depois de vários meses executando o cluster com essa configuração, é preciso adicionar nós. Você redimensiona o cluster, escolhendo o mesmo tipo de nó e especificando um total de 20 nós.

Neste cenário, a cobrança é feita pela taxa com desconto para todos os nós antes do redimensionamento. Após o redimensionamento, você é cobrado pela taxa com desconto para os 16 nós no restante do ano e é cobrado pela taxa sob demanda para os 4 nós adicionais que adicionou ao cluster.

## Exemplo 5

Você tem dois clusters na região Oeste dos EUA (Oregon). Um dos clusters tem 6 nós e o outro tem 10 nós.

Neste cenário, a cobrança é feita pela taxa com desconto para todos os nós, pois o número total de nós em ambos os clusters é igual ao número de nós reservados.

### Exemplo 6

Você tem dois clusters na região Oeste dos EUA (Oregon). Um dos clusters tem 4 nós e o outro tem 6 nós.

Neste cenário, você é cobrado pela taxa com desconto para os 10 nós que possui nos clusters que estão em execução e também paga a taxa com desconto para os 6 nós adicionais que reservou, mesmo que não tenha no momento nenhum cluster em execução ao qual eles se aplicam.

## Comprar uma oferta de nó reservado com o console do Amazon Redshift

Você usa a página de Nós reservados no console do Amazon Redshift para comprar ofertas de nós reservados e para visualizar as reservas atuais e anteriores.

Depois de comprar uma oferta, a lista Reserved Node exibirá as reservas e os detalhes de cada uma, como o tipo de nó, o número de nós e o status da reserva. Para obter mais informações sobre os detalhes da reserva, consulte Como os nós reservados funcionam.

Para comprar um nó reservado

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters e Reserved nodes (Nós reservados) para exibir a lista de nós reservados.
3. Escolha Purchase reserved nodes (Comprar nós reservados) para exibir a página para escolher as propriedades do nó que você deseja comprar.
4. Insira as propriedades do nó e escolha Purchase reserved nodes (Comprar nós reservados).

Para atualizar um nó reservado, use a AWS CLI.

Você não pode converter todos os tipos de nós em nós reservados, e também é possível que um nó reservado existente não esteja disponível para renovação. Isso pode ocorrer porque o tipo de nó foi descontinuado. Entre em contato com o suporte ao cliente para renovar um tipo de nó descontinuado.

# Atualizar nós reservados com a AWS CLI

Para atualizar a reserva de um nó reservado com a AWS CLI

1. Obtenha uma lista de ReservedNodeOfferingID para ofertas que atendem aos seus requisitos de tipo de pagamento, período de vigência e cobranças. O exemplo a seguir essa etapa.

```
aws redshift get-reserved-node-exchange-offerings --reserved-node-id xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxx
{
    "ReservedNodeOfferings": [
        {
            "Duration": 31536000,
            "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
            "UsagePrice": 0.0,
            "NodeType": "dc2.large",
            "RecurringCharges": [
                {
                    "RecurringChargeFrequency": "Hourly",
                    "RecurringChargeAmount": 0.2
                }
            ],
            "CcurrencyCode": "USD",
            "OfferingType": "No Upfront",
            "ReservedNodeOfferingType": "Regular",
            "FixedPrice": 0.0
        }
    ]
}
```

2. Chame `accept-reserved-node-exchange` e forneça o ID do nó reservado DC1 que deseja trocar com o ReservedNodeOfferingID obtido na etapa anterior.

   O exemplo a seguir essa etapa.

```
aws redshift accept-reserved-node-exchange --reserved-node-id xxxxxxxx-xxxx-xxxx-
xxxx-xxxxxxxxxxxx --target-reserved-node-offering-id yyyyyyyy-yyyy-yyyy-yyyy-
yyyyyyyyyyyy
{
    "ExchangedReservedNode": {
```

```
        "UsagePrice": 0.0,
        "OfferingType": "No Upfront",
        "State": "exchanging",
        "FixedPrice": 0.0,
        "CurrencyCode": "USD",
        "ReservedNodeId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzz",
        "NodeType": "dc2.large",
        "NodeCount": 1,
        "RecurringCharges": [
            {
                "RecurringChargeFrequency": "Hourly",
                "RecurringChargeAmount": 0.2
            }
        ],
        "ReservedNodeOfferingType": "Regular",
        "StartTime": "2018-06-27T18:02:58Z",
        "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
        "Duration": 31536000
    }
}
```

É possível confirmar que a troca foi concluída chamando describe-reserved-nodes e verificando o valor de `Node type`.

## Comprar uma oferta de nó reservado usando a AWS CLI e a API do Amazon Redshift

Você pode usar as operações da AWS CLI a seguir para comprar ofertas de nó reservado.

- purchase-reserved-node-offering
- describe-reserved-node-offerings
- describe-orderable-cluster-options

É possível usar as operações da API do Amazon Redshift a seguir para comprar ofertas de nó reservado.

- PurchaseReservedNodeOffering
- DescribeReservedNodeOfferings

- DescribeOrderableClusterOptions

Você não pode converter todos os tipos de nós em nós reservados, e também é possível que um nó reservado existente não esteja disponível para renovação. Isso pode ocorrer porque o tipo de nó foi descontinuado.

# Segurança no Amazon Redshift

A segurança na nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem da AWS. A AWS também fornece serviços que podem ser usados com segurança. A eficácia da nossa segurança é regularmente testada e verificada por auditores de terceiros como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de compatibilidade que se aplicam ao Amazon Redshift, consulte Serviços da AWS no escopo pelo programa de compatibilidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, inclusive a confidencialidade dos dados, os requisitos da organização, as leis e as regulamentações vigentes.

O acesso aos recursos do Amazon Redshift é controlado em quatro níveis:

- Gerenciamento de cluster: a capacidade de criar, configurar e excluir clusters é controlada pelas permissões dadas ao usuário ou conta referente às suas credenciais de segurança da AWS. Os usuários que têm as permissões adequadas podem usar o AWS Management Console, a AWS Command Line Interface (CLI) ou a interface de programação de aplicações (API) do Amazon Redshift para gerenciar seus clusters. Esse acesso é gerenciado pelo uso de políticas do IAM.

  > **Important**
  >
  > O Amazon Redshift tem um conjunto de práticas recomendadas para gerenciar permissões, identidades e acesso seguro. Recomendamos que você se familiarize com essas práticas ao começar a usar o Amazon Redshift. Para obter mais informações, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift.

- Conectividade de cluster – Os grupos de segurança do Amazon Redshift especificam as instâncias da AWS que são autorizadas a conectar a um cluster do Amazon Redshift em formato de roteamento sem classe entre domínios (CIDR). Para obter informações sobre a criação de grupos

de segurança do Amazon Redshift, Amazon EC2 e Amazon VPC e como associá-los aos clusters, consulte Grupos de segurança de clusters do Amazon Redshift.

- Acesso ao banco de dados: a capacidade de acessar objetos do banco de dados, como tabelas e visualizações, é controlada por contas de usuários de banco de dados no banco de dados do Amazon Redshift. Os usuários só podem acessar recursos no banco de dados do qual suas contas de usuário receberam permissão para acessar. Você cria essas contas de usuário do Amazon Redshift e gerencia as permissões usando as instruções SQL CREATE USER, CREATE GROUP, GRANT, e REVOKE. Para obter mais informações, consulte Gerenciamento de banco de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- Credenciais de banco de dados temporárias e logon único – Além de criar e gerenciar usuários de banco de dados usando comandos SQL, como CREATE USER e ALTER USER, você pode configurar seu cliente SQL com drivers JDBC ou ODBC personalizados do Amazon Redshift. Esses drivers gerenciam o processo de criação de usuários de banco de dados e senhas temporárias como parte do processo de logon do banco de dados.

  Os drivers autenticam os usuários de banco de dados com base na autenticação do AWS Identity and Access Management (IAM). Se você já gerencia identidades de usuário fora da AWS, pode usar um provedor de identidades (IdP) compatível com SAML 2.0 para gerenciar o acesso aos recursos do Amazon Redshift. Use uma função do IAM para configurar o IdP e a AWS para permitir que os usuários federados gerem credenciais de banco de dados temporárias e façam logon nos bancos de dados do Amazon Redshift. Para obter mais informações, consulte Usar a autenticação do IAM para gerar credenciais do usuário do banco de dados.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon Redshift. Os tópicos a seguir mostram como configurar o Amazon Redshift para atender aos seus objetivos de segurança e de compatibilidade. Saiba também como usar outros serviços da AWS que ajudam você a monitorar e proteger os recursos do Amazon Redshift.

Tópicos


- Proteção de dados no Amazon Redshift
- Gerenciamento de Identidade e Acesso no Amazon Redshift
- Gerenciamento das senhas de administrador do Amazon Redshift usando AWS Secrets Manager
- Registrar em log e monitorar no Amazon Redshift
- Validação de compatibilidade do Amazon Redshift
- Resiliência no Amazon Redshift

- Segurança da infraestrutura no Amazon Redshift
- Análise de configuração e vulnerabilidade no Amazon Redshift

# Proteção de dados no Amazon Redshift

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no Amazon Redshift. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para mais informações sobre a proteção de dados na Europa, consulte o artigo AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja asConta da AWS credenciais da e configure as contas de usuário individuais com o AWS IAM Identity Center ou o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os atributos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o .AWS CloudTrail
- Use AWS as soluções de criptografia da , juntamente com todos os controles de segurança padrão dos Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comandos ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um

campo Name (Nome). Isso inclui quando você trabalha com o Amazon Redshift ou outros Serviços da AWS usando o console, a API, a AWS CLI ou AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

## Criptografia de dados

Proteção de dados refere-se à proteção de dados durante o trânsito (enquanto eles viajam de e para o Amazon Redshift) e em repouso (enquanto são armazenados em discos nos datacenters do Amazon Redshift). Você pode proteger os dados em trânsito, utilizando SSL ou a criptografia no lado do cliente. Você tem as opções a seguir de proteção de dados em repouso no Amazon Redshift.

- Usar criptografia do lado do servidor – Você solicita que o Amazon Redshift criptografe seus dados antes de salvá-los em discos em seus datacenters e descriptografá-los ao baixar os objetos.
- Usar criptografia do lado do cliente — Você pode criptografar dados no lado do cliente e carregar os dados criptografados no Amazon Redshift. Nesse caso, você gerencia o processo de criptografia, as chaves de criptografia e as ferramentas relacionadas.

### Criptografia inativa

A criptografia do lado do servidor trata da criptografia de dados em repouso - ou seja, o Amazon Redshift criptografa opcionalmente seus dados à medida que os grava em seus datacenters e os descriptografa para você quando você os acessa. Contanto que você autentique sua solicitação e tenha permissões de acesso, não há diferença na forma de acesso aos dados criptografados ou não criptografados.

O Amazon Redshift protege os dados em repouso por meio de criptografia. Opcionalmente, você pode proteger todos os dados armazenados em discos dentro de um cluster e todos os backups no Amazon S3 com Advanced Encryption Standard AES-256.

Para gerenciar as chaves usadas para criptografar e descriptografar seus recursos do Amazon Redshift, use o AWS Key Management Service (AWS KMS). O AWS KMS combina hardware e software seguros e altamente disponíveis para fornecer um sistema de gerenciamento de chaves escalado para a nuvem. utilizando o AWS KMS, é possível criar chaves de criptografia e definir as políticas que controlam como elas podem ser usadas. O AWS KMS é compatível com o AWS CloudTrail, o que possibilita a auditoria do uso de chaves para verificar se elas estão sendo usadas adequadamente. Você pode usar suas chaves AWS KMS em combinação com o Amazon Redshift

e serviços compatíveis da AWS. Para obter uma lista de serviços compatíveis com o AWS KMS, consulte Como os serviços da AWS usam o AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Se você optar por gerenciar o cluster provisionado ou a senha de administrador do namespace de tecnologia sem servidor usando AWS Secrets Manager, o Amazon Redshift também aceitará uma chave KMS da AWS usada pelo AWS Secrets Manager para criptografar as credenciais. Essa chave adicional pode ser uma chave gerada automaticamente pelo AWS Secrets Manager ou uma chave personalizada fornecida por você.

O editor de consultas v2 do Amazon Redshift armazena com segurança as informações inseridas no editor de consultas da seguinte maneira:

- O nome do recurso da Amazon (ARN) da chave KMS a ser usada para criptografar os dados do editor de consultas v2.
- Informações da conexão do banco de dados.
- Nomes e conteúdo de arquivos e pastas.

O editor de consultas v2 do Amazon Redshift criptografa informações usando criptografia em nível de bloco com a chave KMS ou a chave KMS da conta de serviço. A criptografia dos dados do Amazon Redshift é controlada pelas propriedades do cluster do Amazon Redshift.

Tópicos

- Criptografia de banco de dados do Amazon Redshift

## Criptografia de banco de dados do Amazon Redshift

No Amazon Redshift, você pode habilitar a criptografia de banco de dados para seus clusters para ajudar a proteger os dados em repouso. Quando você ativar a criptografia de um cluster, os blocos de dados e os metadados do sistema serão criptografados para o cluster o os snapshots.

É possível habilitar a criptografia ao iniciar o cluster ou modificar um cluster não criptografado para usar criptografia do AWS Key Management Service (AWS KMS). Para fazer isso, você pode usar uma chave gerenciada pela AWS ou uma chave gerenciada pelo cliente. Ao modificar o cluster para habilitar a criptografia do AWS KMS, o Amazon Redshift migra automaticamente os dados para um novo cluster criptografado. Os snapshots criados a partir do cluster criptografado também são criptografados. Você também pode migrar um cluster criptografado para um cluster não

criptografado, modificando o cluster e alterando a opção Encrypt database (Criptografar banco de dados). Para ter mais informações, consulte Alterar a criptografia do cluster.

Embora a criptografia seja uma configuração opcional no Amazon Redshift, recomendamos que você a habilite para clusters que contêm dados sigilsos. Além disso, talvez seja necessário usar a criptografia, dependendo das diretrizes ou das regulamentações que regem os dados. Por exemplo, PCI DSS (Payment Card Industry Data Security Standard), SOX (Sarbanes-Oxley Act), HIPAA (Health Insurance Portability and Accountability Act) e outras regulamentações determinam as diretrizes para processar tipos de dados específicos.

O Amazon Redshift usa uma hierarquia de chaves de criptografia para criptografar o banco de dados. Você pode usar o AWS Key Management Service (AWS KMS) ou um Hardware Security Module (HSM – Módulo de segurança de hardware) para gerenciar as chaves de criptografia de nível superior nessa hierarquia. O processo usado pelo Amazon Redshift é diferente de acordo com a maneira que você gerencia chaves. O Amazon Redshift se integra automaticamente ao AWS KMS mas não com um HSM. Ao usar um HSM, você deve usar certificados de cliente e servidor para configurar uma conexão confiável entre o Amazon Redshift e seu HSM.

Melhorias no processo de criptografia para aumentar a performance e a disponibilidade

Criptografia com nós RA3

As atualizações no processo de criptografia dos nós RA3 melhoraram muito a experiência. Consultas de leitura e gravação podem ser executadas durante o processo, com menos impacto na performance decorrente da criptografia. Além disso, a criptografia termina muito mais rapidamente. As etapas atualizadas do processo incluem uma operação de restauração e a migração dos metadados do cluster para um cluster de destino. A experiência aprimorada se aplica a tipos de criptografia como o AWS KMS, por exemplo. Em casos de volumes de dados na escala de petabytes, a operação foi reduzida de semanas para dias.

Antes de criptografar um cluster, se você planeja continuar executando workloads de banco de dados, poderá melhorar a performance e acelerar o processo adicionando nós com redimensionamento elástico. Não é possível usar o redimensionamento elástico quando a criptografia está em andamento, então faça isso antes de iniciar a criptografia. Observe que a adição de nós normalmente resulta em um custo mais alto.

Criptografia com outros tipos de nós

Ao criptografar um cluster com nós DC2 ou DS2, não é possível executar consultas de gravação, ao contrário dos nós RA3. Somente consultas de leitura podem ser executadas.

## Notas de uso para criptografia com nós RA3

Os insights e recursos a seguir ajudam você a se preparar para a criptografia e monitorar o processo.

- Execução de consultas depois de iniciar a criptografia: depois que a criptografia é iniciada, as leituras e gravações ficam disponíveis em até 15 minutos. O tempo necessário para concluir todo o processo de criptografia depende da quantidade de dados no cluster e dos níveis de workload.
- Quanto tempo demora a criptografia? O tempo necessário para criptografar os dados depende de vários fatores, como o número de workloads em execução, os recursos computacionais usados, o número de nós e os tipos de nós. Recomendamos que você execute a criptografia em um ambiente de teste primeiro. Como regra geral, se você estiver trabalhando com volumes de dados na escala de petabytes, a criptografia provavelmente levará de um a três dias para ser concluída.
- Como saber se a criptografia foi concluída? – Depois de habilitar a criptografia, a conclusão do primeiro snapshot confirma que a criptografia foi concluída.
- Reversão da criptografia: se você precisar reverter a operação de criptografia, a melhor maneira de fazer isso será restaurar o backup mais recente feito antes do início da criptografia. Você precisará reaplicar todas as novas atualizações (atualizações/exclusões/inserções) feitas depois do último backup.
- Execução de uma restauração de tabela: observe que você não pode restaurar uma tabela de um cluster não criptografado para um cluster criptografado.
- Criptografia de um cluster de nó único: esse tipo de criptografia apresenta limitações de performance. Ela é mais longa que a criptografia de um cluster de vários nós.
- Criação de um backup depois da criptografia: quando você criptografa os dados de um cluster, nenhum backup será criado enquanto o cluster não estiver totalmente criptografado. A quantidade de tempo que isso leva pode variar. O tempo necessário para criação do backup pode ser de horas a dias, dependendo do tamanho do cluster. Após a conclusão da criptografia, poderá haver um atraso até que você possa criar um backup.

  Observe que, como ocorre uma operação de backup e restauração durante o processo de criptografia, nenhuma tabela ou visão materializada criada com `BACKUP NO` é retida. Para obter mais informações, consulte CRIAR TABELA ou CRIAR VISÃO MATERIALIZADA.

### Tópicos

- Criptografia de banco de dados do Amazon Redshift usando AWS KMS
- Criptografia para Amazon Redshift usando módulos de segurança de hardware

- Alternância de chave de criptografia no Amazon Redshift
- Alterar a criptografia do cluster
- Configuração da criptografia do banco de dados usando o console
- Configurar a criptografia do banco de dados usando a API do Amazon Redshift e a AWS CLI

### Criptografia de banco de dados do Amazon Redshift usando AWS KMS

Quando você escolhe o AWS KMS para gerenciamento de chaves com o Amazon Redshift, há uma hierarquia de quatro camadas de chaves de criptografia. Essas chaves, em ordem hierárquica, são a chave raiz , uma chave de criptografia de cluster (CEK), uma chave de criptografia de banco de dados (DEK) e chaves de criptografia dos dados.

Quando você inicia seu cluster, o Amazon Redshift retorna uma lista das AWS KMS keys que sua conta da AWS criou ou tem permissão para usar no AWS KMS. Selecione uma chave KMS a ser usada como a chave raiz na hierarquia da criptografia.

Por padrão, o Amazon Redshift seleciona a chave padrão como a chave raiz. Sua chave padrão é uma chave gerenciada pela AWS que é criada para sua conta da AWS para uso no Amazon Redshift. O AWS KMS cria essa chave na primeira vez que você inicia um cluster criptografado em uma região da AWS e escolhe a chave padrão.

Se não quiser usar a chave padrão, você deve ter (ou criar) uma chave KMS gerenciada pelo cliente separadamente no AWS KMS antes de iniciar seu cluster no Amazon Redshift. As chaves gerenciadas pelo cliente dão mais flexibilidade, inclusive a possibilidade de criar, alternar, desativar e definir controle de acesso, além de auditar as chaves de criptografia usadas para ajudar a proteger os dados. Para obter mais informações sobre como criar chaves KMS, consulte Criar chaves no Guia do desenvolvedor do AWS Key Management Service.

Se quiser usar uma chave AWS KMS de outra conta da AWS, você deve ter permissão para usar a chave e especificar seu nome do recurso da Amazon (ARN) no Amazon Redshift. Para obter mais informações sobre acesso a chaves do AWS KMS, consulte Controlar o acesso a suas chaves no Guia do desenvolvedor do AWS Key Management Service.

Depois de escolher uma chave raiz, o Amazon Redshift solicita que o AWS KMS gere uma chave de dados e a criptografe usando a chave raiz selecionada. Essa chave de dados é usada como o CEK no Amazon Redshift. O AWS KMS exporta o CEK criptografado para o Amazon Redshift, onde é armazenado internamente em disco em uma rede separada do cluster junto com a concessão à chave KMS e o contexto de criptografia para o CEK. Somente o CEK criptografado é exportado para

o Amazon Redshift; e a chave KMS permanece no AWS KMS. O Amazon Redshift também passa o CEK criptografado por um canal seguro para o cluster e o carrega na memória. Em seguida, o Amazon Redshift chama o AWS KMS para descriptografar o CEK e carrega o CEK descriptografado na memória. Para obter mais informações sobre concessões, contexto de criptografia e outros conceitos relacionados ao AWS KMS, consulte Conceitos no Guia do desenvolvedor do AWS Key Management Service.

Em seguida, o Amazon Redshift gera aleatoriamente uma chave para usar como DEK e a carrega na memória do cluster. O CEK descriptografado é usado para criptografar o DEK, que é então passado por um canal seguro do cluster para ser armazenado internamente pelo Amazon Redshift em disco em uma rede separada do cluster. Assim como a CEK, as versões criptografadas e descriptografadas da DEK são carregadas na memória no cluster. Em seguida, a versão descriptografada da DEK é usada para criptografar as chaves de criptografia individuais geradas aleatoriamente para cada bloco de dados no banco de dados.

Quando o cluster é reinicializado, o Amazon Redshift começa com as versões criptografadas e armazenadas internamente do CEK e do DEK, recarrega-as na memória e chama o AWS KMS para descriptografar o CEK com a chave KMS novamente para que possa ser carregada na memória. Em seguida, a CEK descriptografada é usada para descriptografar a DEK novamente, e a DEK descriptografada é carregada na memória e usada para criptografar e descriptografar as chaves do bloco de dados conforme necessário.

Para obter mais informações sobre como criar clusters do Amazon Redshift que são criptografados com chaves AWS KMS, consulte Criar um cluster e Gerenciar clusters usando a AWS CLI e a API do Amazon Redshift.

Copiar snapshots criptografados pelo AWS KMS para outra região da AWS

As chaves AWS KMS são específicas para uma região da AWS. Se você habilitar a cópia de snapshots do Amazon Redshift para outra região da AWS e o cluster de origem e seus snapshots forem criptografados usando uma chave raiz do AWS KMS, será necessário configurar uma concessão para o Amazon Redshift para usar uma chave raiz na região da AWS de destino. Essa concessão permite que o Amazon Redshift criptografe snapshots na região da AWS de destino. Para obter mais informações sobre uma cópia do snapshot em várias regiões, consulte Copiar snapshots para outra região da AWS.

> **Note**
>
> Se ativar a cópia de snapshots de um cluster criptografado e usar o AWS KMS para a chave raiz, você não poderá renomear o cluster porque o nome do cluster faz parte do contexto da criptografia. Se você precisar renomear seu cluster, poderá desabilitar a cópia de snapshots na região da AWS de fonte, renomear o cluster e, em seguida, configurar e habilitar a cópia de snapshots novamente.

O processo para configurar a concessão para cópia de snapshots é este.

1. Na região da AWS de destino, crie uma concessão de cópia de snapshot fazendo o seguinte:
   - Se você ainda não tiver uma chave do AWS KMS a ser usada, crie uma. Para obter mais informações sobre como criar chaves AWS KMS, consulte Criar chaves no Guia do desenvolvedor do AWS Key Management Service.
   - Especifique um nome para a concessão de cópia do snapshot. Este nome deve ser único naquela região da AWS para sua conta da AWS.
   - Especifique o ID da chave do AWS KMS para o qual você está criando a concessão. Se você não especificar um ID da chave, a concessão se aplicará à chave padrão.
2. Na região da AWS de origem, habilite a cópia de snapshots e especifique o nome da concessão de cópia de snapshot que você criou na região da AWS de destino.

Este processo anterior só é necessário se você habilitar a cópia de snapshots usando a AWS CLI, a API do Amazon Redshift ou SDKs. Se você usar o console, o Amazon Redshift fornece o fluxo de trabalho adequado para configurar a concessão ao habilitar a cópia de snapshot entre regiões. Para obter mais informações sobre como configurar a cópia de snapshot em todas as regiões para clusters criptografados pelo AWS KMS usando o console, consulte Configurar a cópia de snapshot entre regiões para um cluster criptografado pelo AWS KMS.

Antes que o snapshot seja copiado para a região da AWS de destino, o Amazon Redshift descriptografa o snapshot usando a chave raiz na região da AWS de fonte e recriptografa temporariamente usando uma chave RSA gerada aleatoriamente que o Amazon Redshift gerencia internamente. Em seguida, o Amazon Redshift copia o snapshot em um canal seguro para a região da AWS de destino, descriptografa o snapshot usando a chave RSA gerenciada internamente e, em seguida, criptografa novamente o snapshot usando a chave raiz na região da AWSde destino.

Para obter mais informações sobre como configurar concessões de cópia do snapshot para clusters criptografados pelo AWS KMS, consulte Configurar o Amazon Redshift para usar chaves de criptografia AWS KMS usando a API do Amazon Redshift e a AWS CLI.

Criptografia para Amazon Redshift usando módulos de segurança de hardware

Se você não usa o AWS KMS para gerenciamento de chaves, pode usar um módulo de segurança de hardware (HSM) para gerenciamento de chaves com o Amazon Redshift.

> **Important**
>
> A criptografia de HSM não é compatível com tipos de nós DC2 e RA3.

HSMs são dispositivos que oferecem controle direto sobre a geração e o gerenciamento de chaves. Eles fornecem maior segurança separando o gerenciamento de chaves das camadas de aplicação e banco de dados. O Amazon Redshift oferece suporte ao AWS CloudHSM Classic para gerenciamento de chaves. O processo de criptografia é diferente quando você usa o HSM para gerenciar as chaves de criptografia, em vez do AWS KMS.

> **Important**
>
> O Amazon Redshift suporta apenas AWS CloudHSM Classic. Não há suporte para o serviço mais recente do AWS CloudHSM.
> O AWS CloudHSM Classic está fechado para novos clientes. Para obter mais informações, consulte Preço do CloudHSM Classic.AWS CloudHSM O Classic não está disponível em todas as regiões da AWS. Para obter mais informações sobre as regiões da AWS disponíveis, consulte a Tabela de regiões da AWS.

Quando você configura seu cluster para usar um HSM, o Amazon Redshift envia uma solicitação ao HSM para gerar e armazenar uma chave a ser usada como CEK. No entanto, ao contrário do AWS KMS, o HSM não exporta o CEK para o Amazon Redshift. Em vez disso, o Amazon Redshift gera aleatoriamente o DEK no cluster e o passa para o HSM para ser criptografado pelo CEK. O HSM retorna a DEK criptografada ao Amazon Redshift, onde ela é mais criptografada usando uma chave raiz interna gerada aleatoriamente e armazenada internamente em disco em uma rede à parte do cluster. O Amazon Redshift também carrega a versão descriptografada da DEK na memória no cluster, de maneira que a DEK possa ser usada para criptografar e descriptografar as chaves individuais dos blocos de dados.

Se o cluster for reinicializado, o Amazon Redshift descriptografa a DEK criptografada duplamente armazenada internamente usando a chave raiz interna para retornar a DEK armazenada internamente ao estado criptografado por CEK. O DEK criptografado por CEK é então passado ao HSM para ser descriptografado e devolvido ao Amazon Redshift, onde pode ser carregado na memória novamente para uso com as chaves de bloco de dados individuais.

Configurar uma conexão confiável entre o Amazon Redshift e um HSM

Quando você opta por usar um HSM para gerenciamento de sua chave de cluster, você precisa configurar um link de rede confiável entre o Amazon Redshift e seu HSM. Isso exige a configuração dos certificados de cliente e servidor. A conexão confiável é usada para passar as chaves de criptografia entre o HSM e o Amazon Redshift durante as operações de criptografia e descriptografia.

O Amazon Redshift cria um certificado de cliente público a partir de um par de chaves públicas e privadas gerado aleatoriamente. Elas são criptografadas e armazenadas internamente. Você faz download e registra o certificado cliente público no HSM, além de atribui-lo à partição do HSM aplicável.

Você fornece ao Amazon Redshift o endereço IP HSM, o nome da partição HSM, a senha da partição HSM e um certificado de servidor HSM público, que é criptografado usando uma chave raiz interna. O Amazon Redshift conclui o processo de configuração e verifica se ele pode se conectar ao HSM. Se não puder, o cluster será colocado no estado INCOMPATIBLE_HSM, e não será criado. Nesse caso, você deve excluir o cluster incompleto e tentar novamente.

> **Important**
>
> Quando você modifica seu cluster para usar uma partição HSM diferente, o Amazon Redshift verifica se ele pode se conectar à nova partição, mas não verifica se existe uma chave de criptografia válida. Para usar a nova partição, você deve replicar as chaves para a nova partição. Se o cluster for reiniciado e o Amazon Redshift não puder encontrar uma chave válida, a reinicialização falhará. Para obter mais informações, consulte Replicação de chaves entre os HSMs.

Após a configuração inicial, se o Amazon Redshift não conseguir se conectar ao HSM, um evento será registrado. Para obter mais informações sobre esses eventos, consulte Notificações de evento do Amazon Redshift.

### Alternância de chave de criptografia no Amazon Redshift

No Amazon Redshift, você pode alternar as chaves de criptografia para clusters criptografados. Quando você inicia o processo de alternância de chaves, o Amazon Redshift alterna a CEK do cluster especificado e de qualquer snapshot automatizado ou manual do cluster. O Amazon Redshift também alterna a DEK do cluster especificado, mas não pode alternar a DEK dos snapshots enquanto eles permanecem armazenados internamente no Amazon Simple Storage Service (Amazon S3) e criptografados usando-se a DEK existente.

Enquanto a alternância está em andamento, o cluster é colocado em um estado ROTATING_KEYS até a conclusão, momento em que o cluster retorna ao estado AVAILABLE. O Amazon Redshift lida com a descriptografia e a recriptografia durante o processo de alternância da chave.

> **Note**
>
> Você não pode alternar chaves para snapshots sem um cluster de origem. Para excluir um cluster, leve em consideração se os snapshots dependem do rodízio da chave.

Como o cluster está temporariamente indisponível durante o processo de rodízio da chave, você deverá alternar as chaves somente com a frequência que os dados exigirem ou quando suspeitar de que as chaves foram comprometidas. Como melhores práticas, você deve examinar o tipo de dados que armazena e planejar com que frequência alternar as chaves que criptografam esses dados. A frequência para alternar chaves varia de acordo com as políticas corporativas da segurança de dados e todos os padrões do setor referentes aos dados confidenciais e à compatibilidade regulatória. Verifique se o plano equilibra necessidades de segurança com considerações sobre disponibilidade para o cluster.

Para obter mais informações sobre como alternar chaves, consulte Alternância de chaves de criptografia usando o console do Amazon Redshift e Alternância de chaves de criptografia usando a API do Amazon Redshift e a AWS CLI.

### Alterar a criptografia do cluster

É possível modificar um cluster não criptografado para usar a criptografia do AWS Key Management Service (AWS KMS) usando uma chave gerenciada pela AWS ou uma chave gerenciada pelo cliente. Ao modificar o cluster para habilitar a criptografia do AWS KMS, o Amazon Redshift migra automaticamente os dados para um novo cluster criptografado. Você também pode migrar um cluster não criptografado para um cluster criptografado, modificando o cluster.

Durante a operação de migração, o cluster fica disponível em modo de somente leitura e o status do cluster é exibido como resizing (redimensionando).

Se o seu cluster estiver configurado para habilitar a cópia de snapshot entre regiões da AWS, você deve desabilitá-lo antes de alterar a criptografia. Para obter mais informações, consulte Copiar snapshots para outra região da AWS e Configurar a cópia de snapshot entre regiões para um cluster criptografado pelo AWS KMS. Você não pode habilitar a criptografia do módulo de segurança de hardware (HSM) modificando o cluster. Em vez disso, crie um cluster criptografado por HSM e migre seus dados para esse cluster. Para ter mais informações, consulte Migrar para um cluster criptografado por HSM.

Para modificar a criptografia do banco de dados em um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, depois selecione o cluster para o qual você deseja modificar a criptografia.
3. Escolha Properties (Propriedades).
4. Na seção Configurações do banco de dados, escolha Editar e, depois, escolha Editar criptografia.
5. Escolha uma das opções de criptografia e escolha Salvar alterações.

Para alterar a criptografia de cluster usando a CLI

Para modificar o cluster não criptografado para usar o AWS KMS, execute o comando `modify-cluster` da CLI e especifique `--encrypted`, como mostrado a seguir. Por padrão, a chave do KMS padrão é usada. Para especificar uma chave gerenciada pelo cliente, inclua a opção `--kms-key-id`.

```
aws redshift modify-cluster --cluster-identifier <value> --encrypted --kms-key-id
 <value>
```

Para remover a criptografia do cluster, execute o seguinte comando da CLI.

```
aws redshift modify-cluster --cluster-identifier <value> --no-encrypted
```

### Migrar para um cluster criptografado por HSM

Para migrar um cluster não criptografado para um cluster criptografado usando um módulo de segurança de hardware (HSM), crie um cluster criptografado e mova os dados para esse cluster. Não é possível migrar para um cluster criptografado por HSM modificando o cluster.

Para migrar de um cluster não criptografado para um cluster criptografado por HSM, descarregue os dados do seu cluster de origem existente. Em seguida, recarregue os dados em um novo cluster de destino com a configuração de criptografia escolhida. Para obter mais informações sobre como executar um cluster criptografado, consulte Criptografia de banco de dados do Amazon Redshift.

Durante o processo de migração, seu cluster de origem ficará disponível somente para consultas de leitura até a última etapa. A última etapa é renomear os clusters de origem e de destino, o que modifica os endpoints para que todo o tráfego seja roteado para o novo cluster de destino. Quando você renomear o cluster de destino, ele ficará disponível somente após a reinicialização. Suspenda todas as cargas de dados e outras operações de gravação no cluster de origem enquanto os dados estiverem sendo transferidos.

#### Preparo para a migração

1. Identifique todos os sistemas dependentes que interagem com o Amazon Redshift, por exemplo, ferramentas de business intelligence (BI) e sistemas de extrair, transformar e carregar (ETL).
2. Identifique as consultas de validação para testar a migração.

   Por exemplo, você pode usar a seguinte consulta para localizar o número de tabelas definidas pelo usuário.

   ```
   select count(*)
   from pg_table_def
   where schemaname != 'pg_catalog';
   ```

   A consulta a seguir retorna uma lista de todas as tabelas definidas pelo usuário e o número de linhas em cada tabela.

   ```
   select "table", tbl_rows
   from svv_table_info;
   ```
3. Escolha o momento adequado para a sua migração. Para saber o horário em que o uso do cluster é mais baixo, monitore as métricas do cluster, como a utilização da CPU e o número

de conexões do banco de dados. Para ter mais informações, consulte Visualizar dados de performance do cluster.

4. Remova tabelas não utilizadas.

   Para criar uma lista das tabelas e o número de vezes que cada tabela foi consultada, execute a seguinte consulta.

```
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. Execute um novo cluster criptografado.

   Use o mesmo número de porta para o cluster de destino e o cluster de origem. Para obter mais informações sobre como executar um cluster criptografado, consulte Criptografia de banco de dados do Amazon Redshift.

6. Configure o processo de descarregamento e o carregamento.

   Você pode usar o Utilitário de descarregamento/cópia do Amazon Redshift para lhe ajudar na migração de dados entre clusters. O utilitário exporta dados do cluster de origem para um local no Amazon S3. Os dados são criptografados com o AWS KMS. Em seguida, o utilitário importa automaticamente os dados para o destino. Opcionalmente, você pode usar o utilitário para limpar o Amazon S3 após a conclusão da migração.

7. Execute um teste para verificar seu processo e estime por quanto tempo as operações de gravação precisam ser suspensas.

Durante as operações de descarregamento e carregamento, mantenha a consistência dos dados suspendendo os carregamentos deles e outras operações de gravação. Usando uma das suas maiores tabelas, execute o processo de descarregamento e carregamento para ajudar você a estimar o tempo.

8. Crie objetos de banco de dados, como esquemas, visualizações e tabelas. Para ajudá-lo a gerar as instruções de linguagem de definição de dados (DDL) necessárias, você pode usar os scripts em AdminViews no repositório GitHub da AWS.

Para migrar o cluster

1. Encerre todos os processos ETL no cluster de origem.

   Para confirmar que não há operações de gravação em andamento, use o Console de gerenciamento do Amazon Redshift para monitorar IOPS de gravação. Para ter mais informações, consulte Visualizar dados de performance do cluster.

2. Execute as consultas de validação identificadas anteriormente para coletar informações sobre o cluster de origem não criptografado antes da migração.

3. (Opcional) Crie uma fila de gerenciamento de workload (WLM) para usar o máximo de recursos disponíveis nos clusters de origem e de destino. Por exemplo, crie uma fila chamada `data_migrate` e configure a fila com memória de 95% e simultaneidade de 4%. Para obter mais informações, consulte Roteamento de consultas para filas baseadas em grupos de usuários e grupos de consultas no Guia do desenvolvedor de banco de dados do Amazon Redshift.

4. Usando a fila `data_migrate`, execute UnloadCopyUtility.

   Monitore o processo de UNLOAD e COPY usando o console do Amazon Redshift.

5. Execute as consultas de validação novamente e verifique se os resultados correspondem aos resultados do cluster de origem.

6. Renomeie seus clusters de origem e destino para trocar os endpoints. Para evitar interrupções, execute esta operação fora do horário comercial.

7. Verifique se é possível se conectar ao cluster de destino usando todos os seus clientes SQL, como o ETL e as ferramentas de relatórios.

8. Desligue o cluster de origem não criptografado.

### Configuração da criptografia do banco de dados usando o console

Você pode usar o console do Amazon Redshift para configurar o Amazon Redshift para usar um HSM e alternar as chaves de criptografia. Para obter informações sobre como criar clusters usando chaves de criptografia AWS KMS, consulte Criar um cluster e Gerenciar clusters usando a AWS CLI e a API do Amazon Redshift.

Para modificar a criptografia do banco de dados em um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, depois selecione o cluster para o qual você deseja mover snapshots.
3. Em Actions (Ações), escolha Modify (Modificar) para exibir a página de configuração.
4. Na seção Database configuration (Configuração do banco de dados), escolha uma configuração de Encryption (Criptografia) e escolha Modify cluster (Modificar cluster).

### Alternância de chaves de criptografia usando o console do Amazon Redshift

Você pode usar o procedimento a seguir para alternar as chaves de criptografia usando o console do Amazon Redshift.

Para alternar as chaves de criptografia de um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, depois selecione o cluster para o qual você deseja atualizar as chaves de criptografia.
3. Em Actions (Ações), escolha Rotate encryption (Alternar criptografia) para exibir a página Rotate encryption keys (Alternar chaves de criptografia).
4. Na página Rotate encryption keys (Alternar chaves de criptografia), escolha Rotate encryption keys (Alternar chaves de criptografia).

### Configurar a criptografia do banco de dados usando a API do Amazon Redshift e a AWS CLI

Use a API do Amazon Redshift e a AWS Command Line Interface(AWS CLI) para configurar opções de chave de criptografia para bancos de dados do Amazon Redshift. Para obter mais informações sobre criptografia de banco de dados, consulte Criptografia de banco de dados do Amazon Redshift.

### Configurar o Amazon Redshift para usar chaves de criptografia AWS KMS usando a API do Amazon Redshift e a AWS CLI

Você pode usar as seguintes ações da API do Amazon Redshift para configurar o Amazon Redshift para usar chaves de criptografia AWS KMS.

- CreateCluster
- CreateSnapshotCopyGrant
- DescribeSnapshotCopyGrants
- DeleteSnapshotCopyGrant
- DisableSnapshotCopy
- EnableSnapshotCopy

Você pode usar as seguintes operações da CLI do Amazon Redshift para configurar o Amazon Redshift para usar chaves de criptografia AWS KMS.

- create-cluster
- create-snapshot-copy-grant
- describe-snapshot-copy-grants
- delete-snapshot-copy-grant
- disable-snapshot-copy
- enable-snapshot-copy

### Configurando o Amazon Redshift para usar um HSM usando a API do Amazon Redshift e a AWS CLI

Você pode usar as seguintes ações da API do Amazon Redshift para gerenciar módulos de segurança de hardware.

- CreateHsmClientCertificate
- CreateHsmConfiguration

- DeleteHsmClientCertificate
- DeleteHsmConfiguration
- DescribeHsmClientCertificates
- DescribeHsmConfigurations

Você pode usar as seguintes operações da AWS CLI para gerenciar os módulos de segurança de hardware.

- create-hsm-client-certificate
- create-hsm-configuration
- delete-hsm-client-certificate
- delete-hsm-configuration
- describe-hsm-client-certificates
- describe-hsm-configurations

Alternância de chaves de criptografia usando a API do Amazon Redshift e a AWS CLI

Você pode usar as ações da API do Amazon Redshift a seguir para alternar as chaves de criptografia.

- RotateEncryptionKey

Você pode usar as seguintes operações de AWS CLI para girar chaves de criptografia.

- rotate-encryption-key

## Criptografia em trânsito

Você pode configurar seu ambiente para proteger a confidencialidade e integridade de dados em trânsito.

Criptografia de dados em trânsito entre um cluster Amazon Redshift e clientes SQL sobre JDBC/ODBC:

- Você pode se conectar a clusters do Amazon Redshift a partir de ferramentas de cliente SQL em conexões Java Database Connectivity (JDBC) e Open Database Connectivity (ODBC).

- O Amazon Redshift oferece suporte a conexões Secure Sockets Layer (SSL) para criptografar dados e certificados do servidor para validar o certificado do servidor ao qual o cliente se conecta. O cliente se conecta ao nó líder de um cluster do Amazon Redshift. Para obter mais informações, consulte Configurar as opções de segurança para conexões.
- Para oferecer suporte a conexões SSL, o Amazon Redshift cria e instala certificados AWS Certificate Manager (ACM) emitidos em cada cluster. Para obter mais informações, consulte Transição para certificados ACM das conexões SSL.
- Para proteger seus dados em trânsito na Nuvem AWS, o Amazon Redshift usa SSL acelerado por hardware para se comunicar com o Amazon S3 ou Amazon DynamoDB para operações de COPY, UNLOAD, backup e restauração.

Criptografia de dados em trânsito entre um cluster do Amazon Redshift e o Amazon S3 ou o DynamoDB:

- O Amazon Redshift usa SSL acelerado por hardware para se comunicar com o Amazon S3 ou DynamoDB para operações de COPY, UNLOAD, backup e restauração.
- O Redshift Spectrum oferece suporte à criptografia no lado do servidor (SSE) do Amazon S3 usando a chave padrão da conta gerenciada pelo AWS Key Management Service (KMS).
- Criptografe o Amazon Redshift com o Amazon S3 e o AWS KMS. Para obter mais informações, consulte Criptografar seus carregamentos do Amazon Redshift com o Amazon S3 e o AWS KMS.

Criptografia e assinatura de dados em trânsito entre clientes AWS CLI, SDK ou API e endpoints do Amazon Redshift:

- O Amazon Redshift fornece endpoints HTTPS para criptografar dados em trânsito.
- Para proteger a integridade das solicitações de API para o Amazon Redshift, as chamadas de API devem ser assinadas pelo autor da chamada. As chamadas são assinadas por um certificado X.509 ou pela chave de acesso secreta AWS de acordo com o Processo de assinatura do Signature versão 4 (Sigv4). Para obter mais informações, consulte o Processo de assinatura do Signature versão 4 em Referência geral da AWS.
- Use a AWS CLI ou um dos AWS SDKs para fazer solicitações à AWS. Essas ferramentas autenticam automaticamente as solicitações para você com a chave de acesso especificada na configuração das ferramentas.

Criptografia de dados em trânsito entre clusters do Amazon Redshift e o editor de consultas v2 do Amazon Redshift

- Os dados são transmitidos entre os clusters do editor de consultas v2 do Amazon Redshift em um canal criptografado com TLS.

## Gerenciamento de chaves

É possível configurar o ambiente para proteger os dados com chaves:

- O Amazon Redshift se integra automaticamente com o AWS Key Management Service (AWS KMS) para gerenciamento de chaves. O AWS KMS usa criptografia de envelope. Para obter mais informações, consulte Criptografia de envelope.
- Quando as chaves de criptografia são gerenciadas no AWS KMS, o Amazon Redshift usa uma arquitetura baseada em chave de quatro camadas para criptografia. A arquitetura consiste em chaves de criptografia dos dados AES-256 geradas aleatoriamente, uma chave de banco de dados, uma chave de cluster e uma chave raiz. Para obter mais informações, consulte Como o Amazon Redshift usa o AWS KMS.
- É possível criar sua própria chave gerenciada pelo cliente no AWS KMS. Para obter mais informações, consulte Criação de chaves.
- Você também pode importar seu próprio material de chaves para novas AWS KMS keys. Para obter mais informações, consulte Importando material chave no AWS Key Management Service (AWS KMS).
- O Amazon Redshift oferece suporte ao gerenciamento de chaves de criptografia em módulos de segurança de hardware externos (HSMs). O HSM pode ser on-premises ou pode ser AWS CloudHSM. Ao usar um HSM, você deve usar certificados de cliente e servidor para configurar uma conexão confiável entre o Amazon Redshift e seu HSM. O Amazon Redshift oferece suporte apenas para AWS CloudHSM Classic para gerenciamento de chaves. Para obter mais informações, consulte Criptografia para Amazon Redshift usando módulos de segurança de hardware. Para obter informações sobre o AWS CloudHSM, consulte O que é o AWS CloudHSM?
- Você pode alternar chaves de criptografia para clusters criptografados. Para obter mais informações, consulte Alternância de chave de criptografia no Amazon Redshift.

## Tokenização de dados

Tokenização é o processo de substituição de valores reais por valores opacos para fins de segurança de dados. Aplicativos sensíveis à segurança usam tokenização para substituir dados confidenciais, como informações de identificação pessoal (PII) ou informações de saúde protegidas (PHI) por tokens para reduzir os riscos de segurança. Destokenização reverte tokens com valores reais para usuários autorizados com políticas de segurança apropriadas.

Para integração com serviços de tokenização de terceiros, você pode usar as funções definidas pelo usuário (UDFs) do Amazon Redshift criadas usando o AWS Lambda. Para obter mais informações, consulte Funções definidas pelo usuário do Lambda no Guia do desenvolvedor de banco de dados do Amazon Redshift. Por exemplo, consulte Protegrity.

O Amazon Redshift envia solicitações de tokenização para um servidor de tokenização acessado por meio de uma API REST ou endpoint predefinido. Duas ou mais funções gratuitas do Lambda processam as solicitações de tokenização e destokenização. Para esse processamento, você pode usar funções do Lambda fornecidas por um provedor de tokenização de terceiros. Você também pode usar funções do Lambda registradas como UDFs do Lambda no Amazon Redshift.

Por exemplo, suponha que uma consulta é enviada que invoca um UDF de tokenização ou destokenização em uma coluna. O cluster do Amazon Redshift faz spool as linhas de argumentos aplicáveis e envia essas linhas em lotes para a função do Lambda em paralelo. As transferências de dados entre os nós de computação do Amazon Redshift e o Lambda em uma conexão de rede separada e isolada que não é acessível aos clientes. A função do Lambda passa os dados para o endpoint do servidor de tokenização. O servidor de tokenização tokeniza ou destokeniza os dados conforme necessário e os retorna. Em seguida, as funções do Lambda transmitem os resultados para o cluster do Amazon Redshift para processamento adicional, se necessário, e retornam os resultados da consulta.

## Privacidade do tráfego entre redes

Para rotear o tráfego entre o Amazon Redshift e clientes e aplicações em uma rede corporativa:

- Configure uma conexão privada entre a nuvem privada virtual (VPC) e sua rede corporativa. Configure uma conexão VPN IPsec pela Internet ou uma conexão física privada usando a conexão AWS Direct Connect. AWS Direct Connect permite que você estabeleça uma interface virtual privada de sua rede local diretamente para seu Amazon VPC, fornecendo uma conexão de rede privada de alta largura de banda entre sua rede e sua VPC. Com várias interfaces virtuais, você

pode inclusive estabelecer uma conectividade privada com múltiplas VPCs enquanto mantém o isolamento da rede. Para obter mais informações, consulte O que é a Site-to-Site VPN da AWS? e O que é o AWS Direct Connect?

Para rotear o tráfego entre um cluster do Amazon Redshift em um VPC e buckets do Amazon S3 na mesma região da AWS:

- Configure um endpoint da VPC privado do Amazon S3 para acessar de forma privada os dados do Amazon S3 a partir de um carregamento ou descarregamento de ETL. Para obter mais informações, consulte Endpoints para Amazon S3.
- Habilite “Encaminhamento aprimorado da VPC” para um cluster do Amazon Redshift, especificando um endpoint da VPC do Amazon S3 de destino. O tráfego gerado pelos comandos COPY, UNLOAD ou CREATE LIBRARY do Amazon Redshift é então roteado por meio do endpoint privado. Para obter mais informações, consulte Enhanced VPC routing.

# Gerenciamento de Identidade e Acesso no Amazon Redshift

O acesso ao Amazon Redshift requer credenciais que a AWS pode usar para autenticar suas solicitações. Essas credenciais devem ter permissões para acessar os recursos da AWS, como um cluster do Amazon Redshift. As seções a seguir fornecem detalhes sobre como você pode usar o AWS Identity and Access Management (IAM) e o Amazon Redshift para ajudar a proteger seus recursos, controlando quem pode acessá-los:

- Autenticando com identidades
- Controle de acesso

> **Important**
>
> Este tópico contém um conjunto de práticas recomendadas para gerenciar permissões, identidades e acesso seguro. Recomendamos que se familiarize com as práticas recomendadas para usar o IAM com o Amazon Redshift. Isso inclui o uso de perfis do IAM para aplicar permissões. Ter uma boa compreensão dessas seções ajudará você a manter um data warehouse do Amazon Redshift mais seguro.

# Autenticando com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como o usuário raiz da Usuário raiz da conta da AWS, como um usuário do IAM ou assumindo um perfil do IAM.

Você pode fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. Os usuários do AWS IAM Identity Center (IAM Identity Center), a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

É possível fazer login no AWS Management Console ou no de acesso da AWS dependendo do tipo de usuário que você é. Para mais informações sobre como fazer login na AWS, consulte Como fazer login na Conta da AWS no Guia do Usuário do Início de Sessão da AWS.

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comandos (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinar solicitações de API da AWS no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça mais informações de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no GuiaAWS IAM Identity Center do usuário. Usar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

## Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os recursos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

## Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis.. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

## Perfis do IAM

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM

Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do Usuário do AWS IAM Identity Center.

- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas – É possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar um perfil como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso no Guia do usuário do IAM.
- Acesso entre serviços: alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada a serviço: uma função vinculada a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

## Controle de acesso

Você pode ter credenciais válidas para autenticar suas solicitações, mas a menos que tenha permissões, você não pode criar ou acessar recursos do Amazon Redshift. Por exemplo, você deve ter permissões para criar um cluster Amazon Redshift, criar um snapshot, adicionar uma assinatura de evento e assim por diante.

As seções a seguir descrevem como gerenciar permissões para Amazon Redshift. Recomendamos que você leia a visão geral primeiro.

- Visão geral do gerenciamento de permissões de acesso aos recursos do Amazon Redshift
- Usar políticas baseadas em identidade (políticas do IAM) para o Amazon Redshift

## Visão geral do gerenciamento de permissões de acesso aos recursos do Amazon Redshift

Todo recurso da AWS é de propriedade de uma conta da AWS, e as permissões para criar ou acessar os recursos são regidas por políticas de permissões. Um administrador de conta pode anexar políticas de permissões a identidades do IAM (ou seja, usuários, grupos e perfis), e alguns serviços (como o AWS Lambda) também aceitam a anexação de políticas de permissões a recursos.

> **Note**
>
> Um administrador da conta (ou usuário administrador) é um usuário com privilégios de administrador. Para obter mais informações, consulte Melhores práticas do IAM no IAM User Guide.

Ao conceder permissões, você decide quem recebe as permissões, para quais recursos as permissões são concedidas e as ações específicas que você deseja permitir nesses recursos.

## Recursos e operações do Amazon Redshift

O Amazon Redshift fornece recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Permissões de acesso ao Amazon Redshift, Amazon Redshift sem servidor, à API DATA do Amazon Redshift e ao Editor de Consultas do Amazon Redshift v2

Ao configurar Controle de acesso, você escreve políticas de permissão que podem ser anexadas a uma identidade do IAM (políticas baseadas em identidade). Para obter informações de referência detalhadas, consulte os seguintes tópicos na Referência de autorização do serviço:

- Para o Amazon Redshift, consulte Ações, recursos e chaves de condição do Amazon Redshift que usam o prefixo `redshift:`.
- Para o Amazon Redshift sem servidor, consulte Ações, recursos e chaves de condição do Amazon Redshift sem servidor que usam o prefixo `redshift-serverless:`.
- Para a API DATA do Amazon Redshift, consulte Ações, recursos e chaves de condição da API DATA do Amazon Redshift que usam o prefixo `redshift-data:`.
- Para o Editor de Consultas do Amazon Redshift v2, consulte Ações, recursos e chaves de condição do AWS SQL Workbench (Editor de Consultas do Amazon Redshift v2) que usam o prefixo `sqlworkbench:`.

  O editor de consultas v2 inclui ações somente de permissão que não correspondem diretamente a uma operação de API. Essas ações são indicadas na Referência de autorização de serviço com `[permission only]`.

A Referência de autorização de serviço contém informações sobre quais operações de API podem ser usadas em uma política do IAM. Também inclui o recurso da AWS para o qual você pode

conceder as permissões e as chaves de condição que você pode incluir para controle de acesso detalhado. Para obter mais informações sobre as condições, consulte Uso de condições de política do IAM para controle de acesso refinado.

Você especifica as ações no campo `Action` da política, o valor de recurso no campo `Resource` da política e as condições no campo `Condition` da política. Para especificar uma ação para o Amazon RedShift, use o prefixo `redshift:` seguido do nome da operação da API (por exemplo, `redshift:CreateCluster`).

### Informações sobre propriedade de recursos

Um proprietário do recurso é a conta da AWS que criou um recurso. Ou seja, o proprietário do recurso é a conta da AWS da entidade principal (a conta raiz, um usuário do IAM ou uma função do IAM) que autentica a solicitação que cria o recurso. Os seguintes exemplos mostram como isso funciona:

- Se você usar as credenciais da conta raiz de sua conta da AWS para criar um cluster de banco de dados, sua conta da AWS é a proprietária do recurso Amazon Redshift.
- Se você criar uma função IAM em sua conta da AWS com permissões para criar recursos do Amazon Redshift, qualquer pessoa que possa assumir a função pode criar recursos do Amazon Redshift. Sua conta da AWS, à qual a função pertence, possui os recursos do Amazon Redshift.
- Se você criar um usuário do IAM em sua conta da AWS e conceder permissões para criar recursos do Amazon Redshift para esse usuário, o usuário pode criar recursos do Amazon Redshift. No entanto, sua conta da AWS, à qual o usuário pertence, possui os recursos do Amazon Redshift. Na maioria dos casos, esse método não é recomendado. Recomendamos criar um perfil do IAM e anexar permissões ao perfil e, depois, atribuir o perfil a um usuário.

### Gerenciamento de acesso aos recursos

A política de permissões descreve quem tem acesso a quê. A seção a seguir explica as opções disponíveis para a criação das políticas de permissões.

> **Note**
>
> Esta seção discute o uso de IAM no contexto do Amazon Redshift. Não são fornecidas informações detalhadas sobre o serviço IAM. Para ver a documentação completa do IAM, consulte What is IAM? no IAM User Guide. Para obter informações sobre a sintaxe e as

descrições da política do IAM, consulte a referência da política do IAM da AWS no Guia do usuário do IAM.

As políticas anexadas a uma identidade do IAM são conhecidas como políticas baseadas em identidade (políticas do IAM;) e as políticas anexadas a um recurso são conhecidas como políticas baseadas em recurso. O Amazon Redshift oferece suporte apenas a políticas baseadas em identidade (políticas do IAM).

Políticas baseadas em identidade (políticas do IAM)

É possível atribuir permissões anexando políticas a um perfil do IAM e, depois, atribuindo esse perfil a um usuário ou grupo. Segue-se um exemplo de política que contém permissões para criar, excluir, modificar e reinicializar clusters do Amazon Redshift para sua conta da AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowManageClusters",
      "Effect":"Allow",
      "Action": [
        "redshift:CreateCluster",
        "redshift:DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource":"*"
    }
  ]
}
```

Para obter mais informações sobre o uso de políticas baseadas em identidade com o Amazon Redshift, consulte Usar políticas baseadas em identidade (políticas do IAM) para o Amazon Redshift. Para obter mais informações sobre usuários, grupos, funções e permissões, consulte Identidades (usuários, grupos e funções) no Manual do usuário do IAM.

Políticas baseadas em recursos

Outros serviços, como o Amazon S3, também aceitam políticas de permissões baseadas em recurso. Por exemplo: você pode anexar uma política a um bucket do S3 para gerenciar permissões

de acesso a esse bucket. O Amazon Redshift não oferece suporte a políticas baseadas em recursos.

## Especificar elementos da política: ações, efeitos, recursos e entidades principais

Para cada recurso do Amazon Redshift (consulte Recursos e operações do Amazon Redshift), o serviço define um conjunto de operações de API (consulte Ações). Para conceder permissões para essas operações de API, o Amazon Redshift define um conjunto de ações que você pode especificar em uma política. A execução de uma operação de API pode exigir permissões para mais de uma ação.

Estes são os elementos de política básicos:

- Recurso: em uma política, você usa um nome do recurso da Amazon (ARN) para identificar o recurso a que a política se aplica. Para obter mais informações, consulte Recursos e operações do Amazon Redshift.
- Ação: você usa palavras-chave de ação para identificar operações de recursos que deseja permitir ou negar. Por exemplo, a permissão `redshift:DescribeClusters` concede ao usuário permissões para realizar a operação `DescribeClusters` do Amazon Redshift.
- Efeito - Você especifica o efeito quando o usuário solicita a ação específica, que pode ser permitir ou negar. Se você não conceder (permitir) explicitamente acesso a um recurso, o acesso estará implicitamente negado. Você também pode negar explicitamente o acesso a um recurso, para ter certeza de que um usuário não consiga acessá-lo, mesmo que uma política diferente conceda acesso.
- Entidade principal: em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é a entidade principal implícita. Para as políticas baseadas em recursos, você especifica quais usuários, contas, serviços ou outras entidades deseja que recebam permissões (isso se aplica somente a políticas baseadas em recursos). O Amazon Redshift não oferece suporte a políticas baseadas em recursos.

Para saber mais sobre a sintaxe e as descrições da política do IAM, consulte a Referência da política do AWS IAM no Manual do usuário do IAM.

Para obter uma tabela que mostra todas as ações da API do Amazon Redshift e os recursos aos quais se aplicam, consulte Permissões de acesso ao Amazon Redshift, Amazon Redshift sem servidor, à API DATA do Amazon Redshift e ao Editor de Consultas do Amazon Redshift v2.

## Especificar condições em uma política

Ao conceder permissões, você pode usar a linguagem da política de acesso para especificar as condições quando uma política deve entrar em vigor. Por exemplo, é recomendável aplicar uma política somente após uma data específica. Para obter mais informações sobre como especificar condições em uma linguagem de política de acesso, consulte Elementos de política do IAM JSON: Condição no Manual do usuário do IAM.

Para identificar as condições em que as políticas de permissões se aplicam, inclua um elemento `Condition` em sua política de permissões do IAM. Por exemplo, você pode criar uma política que permita a um usuário criar um cluster usando a ação `redshift:CreateCluster` e você pode adicionar um elemento `Condition` para restringir o usuário a criar o cluster somente em uma região específica. Para obter detalhes, consulte Uso de condições de política do IAM para controle de acesso refinado. Para obter uma lista que mostra todas as chaves-valor de condição e as ações e recursos do Amazon Redshift aos quais se aplicam, consulte Permissões de acesso ao Amazon Redshift, Amazon Redshift sem servidor, à API DATA do Amazon Redshift e ao Editor de Consultas do Amazon Redshift v2.

Uso de condições de política do IAM para controle de acesso refinado

No Amazon Redshift, você pode usar chaves de condição para restringir o acesso a recursos com base nas etiquetas desses recursos. A seguir estão as chaves de condição comuns do Amazon Redshift.

| Chave de condição | Descrição |
| --- | --- |
| `aws:RequestTag` | Requer que os usuários incluam uma chave de tag (nome) e valor sempre que criarem um recurso. Para obter mais informações, consulte aws:RequestTag no Manual do usuário do IAM. |
| `aws:ResourceTag` | Restringe o acesso de usuário a recursos com base em chaves de tag e valores específicos. Para obter mais informações, consulte aws:ResourceTag no Manual do usuário do IAM. |
| `aws:TagKeys` | Use essa chave para comparar as chaves de tag em uma solicitação com as chaves especificadas na política. Para obter mais informações, consulte aws:TagKeys no Manual do usuário do IAM. |

Para obter informações sobre tags, consulte Visão geral da marcação.

Para uma lista de ações de API compatíveis com as chaves de condição `redshift:RequestTag` e `redshift:ResourceTag`, consulte Permissões de acesso ao Amazon Redshift, Amazon Redshift sem servidor, à API DATA do Amazon Redshift e ao Editor de Consultas do Amazon Redshift v2.

As chaves de condição a seguir podem ser usadas com a ação GetClusterCredentials do Amazon Redshift

| Chave de condição | Descrição |
| --- | --- |
| `redshift:DurationSeconds` | Limita o número de segundos que pode ser especificado como duração. |
| `redshift:DbName` | Restringe os nomes de banco de dados que podem ser especificados. |
| `redshift:DbUser` | Restringe os nomes de usuário de banco de dados que podem ser especificados. |

Exemplo 1: restrição de acesso usando a chave de condição aws:ResourceTag

Use a seguinte política do IAM para permitir que um usuário modifique um cluster do Amazon Redshift apenas para uma conta da AWS específica na região da `us-west-2` com uma tag nomeada `environment` com um valor de tag de `test`.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "AllowModifyTestCluster",
        "Effect": "Allow",
        "Action": "redshift:ModifyCluster",
        "Resource": "arn:aws:redshift:us-west-2:123456789012:cluster:*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/environment": "test"
            }
        }
    }
}
```

Exemplo 2: restrição de acesso usando a chave de condição aws:RequestTag

Use a seguinte política de IAM para permitir que um usuário crie um cluster do Amazon Redshift apenas se o comando para criar o cluster incluir uma tag nomeada `usage` e um valor de tag de `production`. A condição com `aws:TagKeys` e o modificador `ForAllValues` especifica que somente as chaves `costcenter` e `usage` podem ser especificadas na solicitação.

```
{
    "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"
                ]
            }
        }
    }
}
```

## Usar políticas baseadas em identidade (políticas do IAM) para o Amazon Redshift

Este tópico fornece exemplos de políticas baseadas em identidade em que um administrador de conta pode anexar políticas de permissões a identidades do IAM (ou seja, usuários, grupos e funções).

> **Important**
>
> Recomendamos que você primeiro analise os tópicos introdutórios que explicam os conceitos básicos e as opções disponíveis para você gerenciar o acesso aos seus recursos do Amazon Redshift. Para obter mais informações, consulte Visão geral do gerenciamento de permissões de acesso aos recursos do Amazon Redshift.

A seguir, um exemplo de uma política de permissões. A política permite que um usuário crie, exclua, modifique e reinicialize todos os clusters, depois nega permissão para excluir ou alterar qualquer cluster cujo identificador de cluster comece com `production` na Região da AWS `us-west-2` e na Conta da 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"
    }
  ]
```

```
}
```

A política tem duas instruções:

- A primeira instrução concede permissões para um usuário para criar, excluir, modificar e reinicializar clusters. A instrução especifica um caractere curinga (*) como o valor `Resource` para que a política se aplique a todos os recursos do Amazon Redshift de propriedade da conta da AWS raiz.
- A segunda instrução nega a permissão para excluir ou modificar um cluster. A instrução especifica um nome de recurso da Amazon (ARN) do cluster para o valor `Resource` que inclui um caractere curinga (*). Como resultado, esta declaração se aplica a todos os clusters do Amazon Redshift pertencentes à conta da AWS raiz com o qual o identificador de cluster começa com `production`.

## Políticas gerenciadas pela AWS para o Amazon Redshift

A AWS aborda muitos casos de uso comuns fornecendo políticas autônomas do IAM que são criadas e administradas pela AWS. As políticas gerenciadas concedem permissões necessárias para casos de uso comuns, de maneira que você possa evitar a necessidade de investigar quais permissões são necessárias. Para obter mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Você também pode criar suas próprias políticas do IAM personalizadas para conceder permissões para operações e recursos da API do Amazon Redshift. É possível anexar essas políticas personalizadas a grupos ou perfis do IAM que exijam essas permissões.

As seguintes seções descrevem políticas gerenciadas pela AWS, que podem ser anexadas aos usuários de sua conta e são específicas do Amazon Redshift.

### AmazonRedshiftReadOnlyAccess

Concede acesso de somente leitura a todos os recursos do Amazon Redshift da conta da AWS.

Você pode encontrar a política AmazonRedshiftReadOnlyAccess no console do IAM e a política AmazonRedshiftReadOnlyAccess no Guia de referência de políticas gerenciadas pela AWS.

### AmazonRedshiftFullAccess

Concede acesso total a todos os recursos do Amazon Redshift da conta da AWS. Além disso, esta política concede acesso completo a todos os recursos do Amazon Redshift Serverless.

Você pode encontrar a política AmazonRedshiftFullAccess no console do IAM e a política AmazonRedshiftFullAccess no Guia de referência de políticas gerenciadas pela AWS.

### AmazonRedshiftQueryEditor

Concede acesso total ao editor de consultas no console do Amazon Redshift.

Você pode encontrar a política AmazonRedshiftQueryEditor no console do IAM e a política AmazonRedshiftQueryEditor no Guia de referência de políticas gerenciadas pela AWS.

### AmazonRedshiftDataFullAccess

Concede acesso total às operações e recursos da API de dados do Amazon Redshift para a conta da AWS.

Você pode encontrar a política AmazonRedshiftDataFullAccess no console do IAM e a política AmazonRedshiftDataFullAccess no Guia de referência de políticas gerenciadas pela AWS.

### AmazonRedshiftQueryEditorV2FullAccess

Concede acesso total às operações e recursos do editor de consultas v2 do Amazon Redshift. Essa política também concede acesso a outros serviços necessários.

Você pode encontrar a política AmazonRedshiftQueryEditorV2FullAccess no console do IAM e a política AmazonRedshiftQueryEditorV2FullAccess no Guia de referência de políticas gerenciadas pela AWS.

### AmazonRedshiftQueryEditorV2NoSharing

Concede a capacidade de trabalhar com o editor de consultas v2 do Amazon Redshift sem compartilhar recursos. Essa política também concede acesso a outros serviços necessários. A entidade principal que usa essa política não pode etiquetar seus recursos (como consultas) para compartilhá-los com outras entidades principais na mesma Conta da AWS.

Você pode encontrar a política AmazonRedshiftQueryEditorV2NoSharing no console do IAM e a política AmazonRedshiftQueryEditorV2NoSharing no Guia de referência de políticas gerenciadas pela AWS.

### AmazonRedshiftQueryEditorV2ReadSharing

Concede a capacidade de trabalhar com o editor de consultas v2 do Amazon Redshift com compartilhamento limitado de recursos. Essa política também concede acesso a outros serviços

necessários. A entidade principal que usa essa política pode etiquetar seus recursos (como consultas) para compartilhá-los com outras entidades principais na mesma Conta da AWS. A entidade principal concedida pode ler os recursos compartilhados com sua equipe, mas não pode atualizá-los.

Você pode encontrar a política AmazonRedshiftQueryEditorV2ReadSharing no console do IAM e a política AmazonRedshiftQueryEditorV2ReadSharing no Guia de referência de políticas gerenciadas pela AWS.

### AmazonRedshiftQueryEditorV2ReadWriteSharing

Concede a capacidade de trabalhar com o editor de consultas v2 do Amazon Redshift com compartilhamento de recursos. Essa política também concede acesso a outros serviços necessários. A entidade principal que usa essa política pode etiquetar seus recursos (como consultas) para compartilhá-los com outras entidades principais na mesma Conta da AWS. A entidade principal concedida pode ler e atualizar os recursos compartilhados com sua equipe.

Você pode encontrar a política AmazonRedshiftQueryEditorV2ReadWriteSharing no console do IAM e a política AmazonRedshiftQueryEditorV2ReadWriteSharing no Guia de referência de políticas gerenciadas pela AWS.

### AmazonRedshiftServiceLinkedRolePolicy

Não é possível anexar AmazonRedshiftServiceLinkedRolePolicy a suas entidades do IAM. Essa política é anexada a uma função vinculada a serviços que permite que o Amazon Redshift acesse recursos da conta. Para obter mais informações, consulte Usar funções vinculadas a serviço do Amazon Redshift.

Você pode encontrar a política AmazonRedshiftServiceLinkedRolePolicy no console do IAM e a política AmazonRedshiftServiceLinkedRolePolicy no Guia de referência de políticas gerenciadas pela AWS.

### AmazonRedshiftAllCommandsFullAccess

Concede a capacidade de usar a função do IAM criada a partir do console do Amazon Redshift e defini-la como padrão para que o cluster execute os comandos COPY do Amazon S3, UNLOAD, CREATE EXTERNAL SCHEMA, CREATE EXTERNAL FUNCTION e CREATE MODEL. A política também concede permissões para executar instruções SELECT para serviços relacionados, como Amazon S3, CloudWatch Logs, Amazon SageMaker ou AWS Glue.

Você pode encontrar a política AmazonRedshiftAllCommandsFullAccess no console do IAM e a política AmazonRedshiftAllCommandsFullAccess no Guia de referência de políticas gerenciadas pela AWS.

Você também pode criar suas próprias políticas do IAM personalizadas para conceder permissões para operações e recursos da API do Amazon Redshift. É possível anexar essas políticas personalizadas a grupos ou perfis do IAM que exijam essas permissões.

## Atualizações do Amazon Redshift para políticas gerenciadas pela AWS

Visualize detalhes sobre atualizações de políticas gerenciadas pela AWS para Amazon Redshift desde que este serviço começou a rastrear essas mudanças. Para alertas automáticos sobre mudanças nesta página, assine o RSS feed na página de histórico de documentos do Amazon Redshift.

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2FullAccess: atualizar para uma política existente | Adicionada a permissão para as ações `redshift-serverless:ListNamespaces` e `redshift-serverless:ListWorkgroups` à política gerenciada. Adicioná-las concede permissão para listar namespaces e grupos de trabalho sem servidor no data warehouse do Amazon Redshift. | 21 de fevereiro de 2024 |
| AmazonRedshiftQueryEditorV2NoSharing: atualização para uma política existente | Adicionada a permissão para as ações `redshift-serverless:ListNamespaces` e `redshift-serverless:ListWor` | 21 de fevereiro de 2024 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | `kgroups` à política gerenciada. Adicioná-las concede permissão para listar namespaces e grupos de trabalho sem servidor no data warehouse do Amazon Redshift. | |
| AmazonRedshiftQueryEditorV2ReadSharing: atualização para uma política existente | Adicionada a permissão para as ações `redshift-serverless:ListNamespaces` e `redshift-serverless:ListWorkgroups` à política gerenciada. Adicioná-las concede permissão para listar namespaces e grupos de trabalho sem servidor no data warehouse do Amazon Redshift. | 21 de fevereiro de 2024 |
| AmazonRedshiftQueryEditorV2ReadWriteSharing: atualização para uma política existente | Adicionada a permissão para as ações `redshift-serverless:ListNamespaces` e `redshift-serverless:ListWorkgroups` à política gerenciada. Adicioná-las concede permissão para listar namespaces e grupos de trabalho sem servidor no data warehouse do Amazon Redshift. | 21 de fevereiro de 2024 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftReadOnlyAccess: atualização para uma política existente | Adicionada a permissão para ação `redshift:ListRecommendations` à política gerenciada. Isso concede permissão para listar as recomendações do Amazon Redshift Advisor. | 7 de fevereiro de 2024 |
| AmazonRedshiftServiceLinkedRolePolicy: atualização para uma política existente | Adicionada a permissão para as ações `ec2:AssignIpv6Addresses` e `ec2:UnassignIpv6Addresses` à política gerenciada. Adicioná-los concede permissão para atribuir e desatribuir endereços IP. | 31 de outubro de 2023 |
| AmazonRedshiftQueryEditorV2NoSharing: atualização para uma política existente | Adicionada a permissão para as ações `sqlworkbench:GetAutocompletionMetadata` e `sqlworkbench:GetAutocompletionResource` à política gerenciada. Adicioná-los concede permissão para gerar e recuperar informações do banco de dados para preenchimento automático de SQL durante a edição de consultas. | 16 de agosto de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2ReadSharing: atualização para uma política existente | Adicionada a permissão para as ações `sqlworkbench:GetAutocompletionMetadata` e `sqlworkbench:GetAutocompletionResource` à política gerenciada. Adicioná-los concede permissão para gerar e recuperar informações do banco de dados para preenchimento automático de SQL durante a edição de consultas. | 16 de agosto de 2023 |
| AmazonRedshiftQueryEditorV2ReadWriteSharing: atualização para uma política existente | Adicionada a permissão para as ações `sqlworkbench:GetAutocompletionMetadata` e `sqlworkbench:GetAutocompletionResource` à política gerenciada. Adicioná-los concede permissão para gerar e recuperar informações do banco de dados para preenchimento automático de SQL durante a edição de consultas. | 16 de agosto de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftServiceLinkedRolePolicy: atualização para uma política existente | As permissões para ações no AWS Secrets Manager a fim de criar e gerenciar segredos são adicionadas à política gerenciada. As permissões adicionadas são as seguintes:<br>• `secretsmanager:GetRandomPassword`<br>• `secretsmanager:DescribeSecret`<br>• `secretsmanager:PutSecretValue`<br>• `secretsmanager:UpdateSecret`<br>• `secretsmanager:UpdateSecretVersionStage`<br>• `secretsmanager:RotateSecret`<br>• `secretsmanager:DeleteSecret` | 14 de agosto de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftServiceLinkedRolePolicy: atualização para uma política existente | Permissões para ações no Amazon EC2 para criar e gerenciar grupos de segurança e regras de roteamento são removidas da política gerenciada. Essas permissões se referiam à criação de sub-redes e VPCs. As permissões removidas são as seguintes:<br>• `ec2:AuthorizeSecurityGroupEgress`<br>• `ec2:AuthorizeSecurityGroupIngress`<br>• `ec2:UpdateSecurityGroupRuleDescriptionsEgress`<br>• `ec2:ReplaceRouteTableAssociation`<br>• `ec2:CreateRouteTable`<br>• `ec2:AttachInternetGateway`<br>• `ec2:UpdateSecurityGroupRuleDescriptionsIngress`<br>• `ec2:AssociateRouteTable`<br>• `ec2:RevokeSecurityGroupIngress`<br>• `ec2:CreateRoute` | 8 de maio de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • `ec2:CreateSecurityGroup`<br>• `ec2:RevokeSecurityGroupEgress`<br>• `ec2:ModifyVpcAttribute`<br>• `ec2:CreateSubnet`<br>• `ec2:CreateInternetGateway`<br>• `ec2:CreateVpc`<br><br>Elas foram associadas à tag de recurso Purpose:RedshiftMigrateToVpc. A tag limitou o escopo das permissões para tarefas de migração do Amazon EC2 Classic para a VPC do Amazon EC2. Para obter mais informações sobre etiquetas de recursos, consulte Controle de acesso aos recursos da AWS usando etiquetas de recursos. | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftDataFullAccess: atualização para uma política existente | Adicionada a permissão para ação `redshift:GetClusterCredentialsWithIAM` à política gerenciada. Essa adição concede permissão para obter credenciais temporárias avançadas para acessar um banco de dados do Amazon Redshift pela Conta da AWS especificada. | 7 de abril de 2023 |
| AmazonRedshiftServiceLinkedRolePolicy: atualização para uma política existente | Permissões para ações no Amazon EC2 para criação e gerenciamento de regras de grupos de segurança são adicionadas à política gerenciada. Essas regras e grupos de segurança estão especificamente associados à etiqueta de recurso `aws:RequestTag/Redshift` do Amazon Redshift. Isso limita o escopo das permissões para recursos específicos do Amazon Redshift. | 6 de abril de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2NoSharing: atualização para uma política existente | Adicionada a permissão para ação `sqlworkbench:GetSchemaInference` à política gerenciada. Essa adição concede permissão para obter as colunas e os tipos de dados inferidos de um arquivo. | 21 de março de 2023 |
| AmazonRedshiftQueryEditorV2ReadSharing: atualização para uma política existente | Adicionada a permissão para ação `sqlworkbench:GetSchemaInference` à política gerenciada. Essa adição concede permissão para obter as colunas e os tipos de dados inferidos de um arquivo. | 21 de março de 2023 |
| AmazonRedshiftQueryEditorV2ReadWriteSharing: atualização para uma política existente | Adicionada a permissão para ação `sqlworkbench:GetSchemaInference` à política gerenciada. Essa adição concede permissão para obter as colunas e os tipos de dados inferidos de um arquivo. | 21 de março de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2NoSharing: atualização para uma política existente | Adicionada a permissão para ação `sqlworkbench:AssociateNotebookWithTab` à política gerenciada. Adicioná-lo concede permissão para criar e atualizar guias vinculadas ao próprio caderno de um usuário. | 2 de fevereiro de 2023 |
| AmazonRedshiftQueryEditorV2ReadSharing: atualização para uma política existente | Adicionada a permissão para ação `sqlworkbench:AssociateNotebookWithTab` à política gerenciada. Adicioná-lo concede permissão para criar e atualizar guias vinculadas ao próprio caderno de um usuário ou a um caderno compartilhado com ele. | 2 de fevereiro de 2023 |
| AmazonRedshiftQueryEditorV2ReadWriteSharing: atualização para uma política existente | Adicionada a permissão para ação `sqlworkbench:AssociateNotebookWithTab` à política gerenciada. Adicioná-lo concede permissão para criar e atualizar guias vinculadas ao próprio caderno de um usuário ou a um caderno compartilhado com ele. | 2 de fevereiro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2NoSharing: atualização para uma política existente | Para conceder permissão para usar blocos de anotações, o Amazon Redshift adicionou permissão para as seguintes ações:<br>• `sqlworkbench:ListNotebooks`<br>• `sqlworkbench:CreateNotebook`<br>• `sqlworkbench:DuplicateNotebook`<br>• `sqlworkbench:CreateNotebookFromVersion`<br>• `sqlworkbench:ImportNotebook`<br>• `sqlworkbench:GetNotebook`<br>• `sqlworkbench:UpdateNotebook`<br>• `sqlworkbench:DeleteNotebook`<br>• `sqlworkbench:CreateNotebookCell`<br>• `sqlworkbench:DeleteNotebookCell`<br>• `sqlworkbench:UpdateNotebookCellContent` | 17 de outubro de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • sqlworkbench:UpdateNotebookCellLayout<br>• sqlworkbench:BatchGetNotebookCell<br>• sqlworkbench:ListNotebookVersions<br>• sqlworkbench:CreateNotebookVersion<br>• sqlworkbench:GetNotebookVersion<br>• sqlworkbench:DeleteNotebookVersion<br>• sqlworkbench:RestoreNotebookVersion<br>• sqlworkbench:ExportNotebook | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2ReadSharing: atualização para uma política existente | Para conceder permissão para usar blocos de anotações, o Amazon Redshift adicionou permissão para as seguintes ações:<br>• `sqlworkbench:ListNotebooks`<br>• `sqlworkbench:CreateNotebook`<br>• `sqlworkbench:DuplicateNotebook`<br>• `sqlworkbench:CreateNotebookFromVersion`<br>• `sqlworkbench:ImportNotebook`<br>• `sqlworkbench:GetNotebook`<br>• `sqlworkbench:UpdateNotebook`<br>• `sqlworkbench:DeleteNotebook`<br>• `sqlworkbench:CreateNotebookCell`<br>• `sqlworkbench:DeleteNotebookCell`<br>• `sqlworkbench:UpdateNotebookCellContent` | 17 de outubro de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • sqlworkbench:UpdateNotebookCellLayout<br>• sqlworkbench:BatchGetNotebookCell<br>• sqlworkbench:ListNotebookVersions<br>• sqlworkbench:CreateNotebookVersion<br>• sqlworkbench:GetNotebookVersion<br>• sqlworkbench:DeleteNotebookVersion<br>• sqlworkbench:RestoreNotebookVersion<br>• sqlworkbench:ExportNotebook | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2ReadWriteSharing: atualização para uma política existente | Para conceder permissão para usar blocos de anotações, o Amazon Redshift adicionou permissão para as seguintes ações:<br>• `sqlworkbench:ListNotebooks`<br>• `sqlworkbench:CreateNotebook`<br>• `sqlworkbench:DuplicateNotebook`<br>• `sqlworkbench:CreateNotebookFromVersion`<br>• `sqlworkbench:ImportNotebook`<br>• `sqlworkbench:GetNotebook`<br>• `sqlworkbench:UpdateNotebook`<br>• `sqlworkbench:DeleteNotebook`<br>• `sqlworkbench:CreateNotebookCell`<br>• `sqlworkbench:DeleteNotebookCell`<br>• `sqlworkbench:UpdateNotebookCellContent` | 17 de outubro de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • `sqlworkbench:UpdateNotebookCellLayout`<br>• `sqlworkbench:BatchGetNotebookCell`<br>• `sqlworkbench:ListNotebookVersions`<br>• `sqlworkbench:CreateNotebookVersion`<br>• `sqlworkbench:GetNotebookVersion`<br>• `sqlworkbench:DeleteNotebookVersion`<br>• `sqlworkbench:RestoreNotebookVersion`<br>• `sqlworkbench:ExportNotebook` | |
| AmazonRedshiftServiceLinkedRolePolicy: atualização para uma política existente | O Amazon Redshift adicionou o namespace `AWS/Redshift` para permitir a publicação de métricas no CloudWatch. | 7 de setembro de 2022 |
| AmazonRedshiftQueryEditorV2NoSharing: atualização para uma política existente | O Amazon Redshift adicionou permissão às ações `sqlworkbench:ListQueryExecutionHistory` e `sqlworkbench:GetQueryExecutionHistory`. Isso concede permissão para ver o histórico de consultas. | 30 de agosto de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2ReadSharing: atualização para uma política existente | O Amazon Redshift adicionou permissão às ações `sqlworkbench:ListQueryExecutionHistory` e `sqlworkbench:GetQueryExecutionHistory`. Isso concede permissão para ver o histórico de consultas. | 30 de agosto de 2022 |
| AmazonRedshiftQueryEditorV2ReadWriteSharing: atualização para uma política existente | O Amazon Redshift adicionou permissão às ações `sqlworkbench:ListQueryExecutionHistory` e `sqlworkbench:GetQueryExecutionHistory`. Isso concede permissão para ver o histórico de consultas. | 30 de agosto de 2022 |
| AmazonRedshiftFullAccess: atualização para uma política existente | Permissões para o Amazon Redshift Serverless são adicionadas à política gerenciada AmazonRedshiftFullAccess existente. | 22 de julho de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftDataFullAccess: atualização para uma política existente | O Amazon Redshift atualizou a condição de escopo padrão `redshift-serverless:GetCredentials` da permissão da tag `aws:ResourceTag/RedshiftDataFullAccess` do `StringEquals` para `StringLike` para conceder acesso a recursos marcados com chave de tag `RedshiftDataFullAccess` e qualquer valor da tag. | 11 de julho de 2022 |
| AmazonRedshiftDataFullAccess: atualização para uma política existente | O Amazon Redshift adicionou novas permissões para permitir `redshift-serverless:GetCredentials` para obter credenciais temporárias do Amazon Redshift Serverless. | 8 de julho de 2022 |
| AmazonRedshiftQueryEditorV2NoSharing: atualização para uma política existente | O Amazon Redshift adicionou permissão à ação `sqlworkbench:GetAccountSettings` . Essa ação concede permissão para obter configurações da conta. | 15 de junho de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2ReadSharing: atualização para uma política existente | O Amazon Redshift adicionou permissão à ação `sqlworkbench:GetAccountSettings` . Essa ação concede permissão para obter configurações da conta. | 15 de junho de 2022 |
| AmazonRedshiftQueryEditorV2ReadWriteSharing: atualização para uma política existente | O Amazon Redshift adicionou permissão à ação `sqlworkbench:GetAccountSettings` . Essa ação concede permissão para obter configurações da conta. | 15 de junho de 2022 |
| AmazonRedshiftServiceLinkedRolePolicy: atualização para uma política existente | Para habilitar o acesso público a novos endpoints do Amazon Redshift Serverless, o Amazon Redshift aloca e associa endereços IP elásticos à interface de rede elástica do endpoint da VPC na conta do cliente. Ele faz isso por meio de permissões fornecidas por meio da função vinculada ao serviço. Para habilitar esse caso de uso, são adicionadas ações para alocar e liberar um endereço IP elástico à função vinculada ao serviço do Amazon Redshift Serverless. | 26 de maio de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2FullAccess: atualização para uma política existente | Permissões para a ação `sqlworkbench:ListTaggedResources` . Ela tem o escopo específico para os recursos do editor de consultas v2 do Amazon Redshift. Esta atualização de política concede o direito de chamar `tag:GetResources` somente por meio do editor de consultas v2. | 22 de fevereiro de 2022 |
| AmazonRedshiftQueryEditorV2NoSharing: atualização para uma política existente | Permissões para a ação `sqlworkbench:ListTaggedResources` . Ela tem o escopo específico para os recursos do editor de consultas v2 do Amazon Redshift. Esta atualização de política concede o direito de chamar `tag:GetResources` somente por meio do editor de consultas v2. | 22 de fevereiro de 2022 |
| AmazonRedshiftQueryEditorV2ReadSharing: atualização para uma política existente | Permissões para a ação `sqlworkbench:ListTaggedResources` . Ela tem o escopo específico para os recursos do editor de consultas v2 do Amazon Redshift. Esta atualização de política concede o direito de chamar `tag:GetResources` somente por meio do editor de consultas v2. | 22 de fevereiro de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2ReadWriteSharing: atualização para uma política existente | Permissões para a ação `sqlworkbench:ListTaggedResources` . Ela tem o escopo específico para os recursos do editor de consultas v2 do Amazon Redshift. Esta atualização de política concede o direito de chamar `tag:GetResources` somente por meio do editor de consultas v2. | 22 de fevereiro de 2022 |
| AmazonRedshiftQueryEditorV2ReadSharing: atualização para uma política existente | Adicionada a permissão para ação `sqlworkbench:AssociateQueryWithTab` à política gerenciada. Adicioná-la permite que os clientes criem guias do editor vinculadas a uma consulta compartilhada com eles. | 22 de fevereiro de 2022 |
| AmazonRedshiftServiceLinkedRolePolicy: atualização para uma política existente | O Amazon Redshift adicionou permissões para novas ações para permitir o gerenciamento de recursos de rede e VPC do Amazon Redshift. | 22 de novembro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftAllCommandsFullAccess: nova política | O Amazon RedShift adicionou uma nova política para permitir usar a função do IAM criada a partir do console do Amazon Redshift e defini-la como padrão para que o cluster execute os comandos COPY do Amazon S3, UNLOAD, CREATE EXTERNAL SCHEMA, CREATE EXTERNAL FUNCTION, CREATE MODEL ou CREATE LIBRARY. | 18 de novembro de 2021 |
| AmazonRedshiftServiceLinkedRolePolicy: atualização para uma política existente | O Amazon Redshift adicionou permissões para novas ações para permitir o gerenciamento de grupos de log e fluxos de log do CloudWatch do Amazon Redshift, inclusive exportação de log de auditoria. | 15 de novembro de 2021 |
| AmazonRedshiftFullAccess: atualização para uma política existente | O Amazon Redshift adicionou novas permissões para permitir explicabilidade do modelo, DynamoDB, Redshift Spectrum e federação do Amazon RDS. | 07 de outubro de 2021 |
| AmazonRedshiftQueryEditorV2FullAccess: nova política | O Amazon Redshift adicionou uma nova política para permitir acesso total ao editor de consultas v2 do Amazon Redshift. | 24 de setembro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRedshiftQueryEditorV2NoSharing: nova política | O Amazon Redshift adicionou uma nova política para permitir o uso do editor de consultas v2 do Amazon Redshift sem compartilhar recursos. | 24 de setembro de 2021 |
| AmazonRedshiftQueryEditorV2ReadSharing: nova política | O Amazon Redshift adicionou uma nova política para permitir o compartilhamento de leitura no editor de consultas v2 do Amazon Redshift. | 24 de setembro de 2021 |
| AmazonRedshiftQueryEditorV2ReadWriteSharing: nova política | O Amazon Redshift adicionou uma nova política para permitir o compartilhamento de leitura e atualização no editor de consultas v2 do Amazon Redshift. | 24 de setembro de 2021 |
| AmazonRedshiftFullAccess: atualização para uma política existente | O Amazon Redshift adicionou novas permissões para permitir `sagemaker:*Job*` . | 18 de agosto de 2021 |
| AmazonRedshiftDataFullAccess: atualização para uma política existente | O Amazon Redshift adicionou novas permissões para permitir `AuthorizeDataShare` . | 12 de agosto de 2021 |
| AmazonRedshiftDataFullAccess: atualização para uma política existente | O Amazon Redshift adicionou novas permissões para permitir `BatchExecuteStatement` . | 27 de julho de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| O Amazon Redshift começou a monitorar alterações | O Amazon Redshift começou a monitorar alterações para suas políticas gerenciadas pela AWS. | 27 de julho de 2021 |

## Permissões necessárias para usar Redshift Spectrum

O Amazon Redshift Spectrum requer permissões para outros serviços da AWS para acessar recursos. Para obter detalhes sobre as permissões em políticas do IAM para Redshift Spectrum, consulte Políticas do IAM para Amazon Redshift Spectrum no Guia do desenvolvedor de database do Amazon Redshift.

## Permissões necessárias para usar o console do Amazon Redshift

Para que um usuário trabalhe com o console do Amazon Redshift, esse usuário deve ter um conjunto mínimo de permissões que permita ao usuário descrever os recursos do Amazon Redshift para sua conta da AWS. Essas permissões também devem permitir que o usuário descreva outras informações relacionadas, incluindo segurança do Amazon EC2, Amazon CloudWatch, Amazon SNS e informações de rede.

Se você criar uma política do IAM que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para os usuários com essa política do IAM. Para garantir que esses usuários ainda possam usar o console do Amazon Redshift, anexe também a política gerenciada pelo `AmazonRedshiftReadOnlyAccess` ao usuário. Como fazer isso é descrito em Políticas gerenciadas pela AWS para o Amazon Redshift.

Para obter informações para conceder ao usuário acesso ao editor de consulta no console do Amazon Redshift, consulte Permissões necessárias para usar o editor de consulta do console do Amazon Redshift.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do Amazon Redshift.

## Permissões necessárias para usar o editor de consulta do console do Amazon Redshift

Para que um usuário trabalhe com o editor de consultas do Amazon Redshift, esse usuário deve ter um conjunto mínimo de permissões para as operações da API de dados do Amazon Redshift e do Amazon Redshift. Para se conectar a um banco de dados usando um segredo, você também deve ter permissões do Secrets Manager.

Para conceder a um usuário acesso ao editor de consultas no console do Amazon Redshift, anexe as políticas `AmazonRedshiftQueryEditor` e `AmazonRedshiftReadOnlyAccess` gerenciadas pela AWS. A política `AmazonRedshiftQueryEditor` permite que o usuário recupere os resultados de apenas suas próprias instruções SQL. Ou seja, instruções apresentadas pelo mesmo `aws:userid`, como mostrado nesta seção da política `AmazonRedshiftQueryEditor` gerenciada pela AWS.

```
{
    "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}"
        }
    }
}
```

Para permitir que um usuário recupere os resultados das instruções SQL de outras pessoas na mesma função do IAM, crie sua própria política sem a condição de limitar o acesso ao usuário atual. Limite também o acesso para alterar uma política para um administrador.

## Permissões necessárias para usar o editor de consultas v2

Para trabalhar com o editor de consultas do Amazon Redshift v2, o usuário deve ter um conjunto mínimo de permissões para o Amazon Redshift, as operações do editor de consultas v2 e outros

produtos da AWS como AWS Key Management Service, AWS Secrets Manager e serviço de marcação.

Para conceder ao usuário acesso total ao editor de consultas v2, anexe a política `AmazonRedshiftQueryEditorV2FullAccess` gerenciada pela AWS. A política `AmazonRedshiftQueryEditorV2FullAccess` permite que o usuário compartilhe recursos do editor de consultas v2, como consultas, com outras pessoas na mesma equipe. Para obter detalhes sobre como o acesso aos recursos do editor de consulta v2 é controlado, consulte a definição da política gerenciada específica para o editor de consultas v2 no console do IAM.

Algumas políticas do editor de consultas v2 do Amazon Redshift gerenciadas pela AWS usam etiquetas da AWS dentro de condições para definir escopo de acesso aos recursos. No editor de consultas v2, o compartilhamento de consultas baseia-se na chave e no valor da tag `"aws:ResourceTag/sqlworkbench-team": "${aws:PrincipalTag/sqlworkbench-team}"` na política do IAM anexada à entidade principal (o perfil do IAM). As entidades principais na mesma Conta da AWS com o mesmo valor de etiqueta (por exemplo, `accounting-team`) estão na mesma equipe no editor de consultas v2. Só é possível ter associação a uma equipe por vez. Um usuário com permissões administrativas pode configurar equipes no console do IAM fornecendo a todos os membros da equipe o mesmo valor para a etiqueta `sqlworkbench-team`. Se o valor da etiqueta `sqlworkbench-team` for alterado para um usuário do IAM ou uma função do IAM, poderá haver um atraso até que a alteração seja refletida nos recursos compartilhados. Se o valor da etiqueta de um recurso (como uma consulta) for alterado, poderá haver novamente um atraso até que a alteração seja refletida. Os membros da equipe também devem ter a permissão `tag:GetResources` para compartilhar.

Exemplo: para adicionar a etiqueta **`accounting-team`** para uma função do IAM

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console, escolha Roles (Funções) e, em seguida, escolha o nome da função que deseja editar.
3. Escolha a guia Tags (Etiquetas) e escolha Add tags (Gerenciar etiquetas).
4. Adicione a chave da etiqueta sqlworkbench-team e o valor `accounting-team`.
5. Escolha Salvar alterações.

   Agora, quando uma entidade principal do IAM (com essa função do IAM anexada) compartilha uma consulta com a equipe, outras entidades principais com o mesmo valor de etiqueta `accounting-team` pode exibir a consulta.

Para obter mais informações sobre como anexar uma etiqueta a uma entidade principal, inclusive funções do IAM e usuários do IAM, consulte Recursos de etiquetas do IAM no Guia do usuário do IAM.

Você também pode configurar equipes no nível da sessão usando um provedor de identidades (IdP). Isso permite que vários usuários que usam a mesma função do IAM tenham uma equipe diferente. A política de confiança da função do IAM deve permitir a operação `sts:TagSession`. Para obter mais informações, consulte Permissões necessárias adicionar etiquetas de sessão no Guia do usuário do IAM. Adicione o atributo de etiqueta da entidade principal à declaração do SAML fornecida pelo IdP.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:sqlworkbench-
team">
    <AttributeValue>accounting-team</AttributeValue>
</Attribute>
```

Siga as instruções para que seu provedor de identidades (IdP) preencha o atributo SAML com o conteúdo proveniente do diretório. Para obter mais informações sobre provedores de identidade (IdPs) e o Amazon Redshift, consulte Usar a autenticação do IAM para gerar credenciais do usuário do banco de dados e Provedores de identidade e federação no Guia do usuário do IAM.

O `sqlworkbench:CreateNotebookVersion` concede permissão para obter o conteúdo atual de células de bloco de anotações e criar uma versão de bloco de anotações em sua conta. Ou seja, no momento da criação da versão, o conteúdo atual do bloco de anotações é igual ao conteúdo da versão. Posteriormente, o conteúdo das células na versão não será modificado à medida que o bloco de anotações atual for atualizado. O`sqlworkbench:GetNotebookVersion` concede permissão para obter uma versão do bloco de anotações. Um usuário que não tem a permissão `sqlworkbench:BatchGetNotebookCell`, mas tem as permissões `sqlworkbench:CreateNotebookVersion` e `sqlworkbench:GetNotebookVersion` em um bloco de anotações, tem acesso às células do bloco de anotações na versão. Esse usuário sem a permissão `sqlworkbench:BatchGetNotebookCell` ainda pode recuperar o conteúdo das células de um bloco de anotações criando uma versão e obtendo essa versão criada.

## Permissões necessárias para usar o programador do Amazon Redshift

Ao usar o programador Amazon Redshift, você configura uma função IAM com uma relação de confiança com o programador Amazon Redshift (**`scheduler.redshift.amazonaws.com`**) para permitir que o programador assuma permissões em seu nome. Você também anexa uma política (permissões) à função para as operações da API do Amazon Redshift que deseja programar.

O exemplo a seguir mostra o documento de política no formato JSON para configurar uma relação de confiança com o programador Amazon Redshift e o Amazon Redshift.

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

Para obter mais informações sobre entidades confiáveis, consulte Criar uma função para delegar permissões a um serviço da AWS no Manual do usuário do IAM.

Você também deve adicionar permissão para as operações do Amazon Redshift que deseja programar.

Para que o programador use a operação `ResizeCluster`, adicione uma permissão que seja semelhante à seguinte à sua política do IAM. Dependendo do seu ambiente, você pode desejar tornar a política mais restritiva.

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

Para obter as etapas para criar uma função para o programador do Amazon Redshift, consulte Criar uma função para um serviço da AWS (console) no Manual do usuário do IAM. Faça estas escolhas ao criar uma função no console do IAM:

- Em Choose the service that will use this role (Escolher o serviço que usará esta função): escolha Redshift.
- Em Select your use case (Selecionar seu caso de uso), escolha Redshift - programador.
- Crie ou anexe uma política à função que permite que uma operação do Amazon Redshift seja programada. Escolha Create policy (Criar política) ou modifique a função para anexar uma política. Insira a política JSON para a operação que está para ser programada.
- Depois de criar a função, edite o Trust Relationship (Relacionamento de confiança) da função do IAM para incluir o serviço `redshift.amazonaws.com`.

A função do IAM que você cria em entidades confiáveis de `scheduler.redshift.amazonaws.com` e `redshift.amazonaws.com`. Ele também tem uma política anexada que permite uma ação de API do Amazon Redshift compatível, como `"redshift:ResizeCluster"`.

## Permissões necessárias para usar o programador do Amazon EventBridge

Ao usar o programador do Amazon EventBridge, você configura uma função do IAM com uma relação de confiança com o programador do EventBridge (**`events.amazonaws.com`**) para permitir que o programador assuma permissões em seu nome. Você também anexa uma política (permissões) à função para as operações da API de dados do Amazon Redshift que deseja programar e uma política para operações do Amazon EventBridge.

Use o programador EventBridge ao criar consultas programadas com o editor de consulta do Amazon Redshift no console.

Você pode criar uma função do IAM para executar consultas programadas no console do IAM. Nesta função do IAM, anexe `AmazonEventBridgeFullAccess` e `AmazonRedshiftDataFullAccess`.

O exemplo a seguir mostra o documento de política no formato JSON para configurar um relacionamento de confiança com o programador do EventBridge.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com",
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Para obter mais informações sobre entidades confiáveis, consulte Criar uma função para delegar permissões a um serviço da AWS no Manual do usuário do IAM.

Para obter as etapas para criar uma função para o programador do EventBridge, consulte Criar uma função para um serviço da AWS (console) no Manual do usuário do IAM. Faça estas escolhas ao criar uma função no console do IAM:

- Em Escolha o serviço que usará esta função, escolha CloudWatch Events.
- Em Selecionar o caso de uso: escolha CloudWatch Events.
- Anexe as seguintes políticas de permissão: `AmazonEventBridgeFullAccess` e `AmazonRedshiftDataFullAccess`.

A função do IAM que você cria tem uma entidade confiável de `events.amazonaws.com`. Ele também tem uma política anexada que permite ações compatíveis da API de dados do Amazon Redshift, como `"redshift-data:*"`.

## Permissões necessárias para usar o machine learning (ML) do Amazon Redshift

A seguir, você encontra uma descrição das permissões necessárias para usar o machine learning (ML) do Amazon Redshift para diferentes casos de uso.

Para que seus usuários utilizem o Amazon Redshift ML com o Amazon SageMaker, crie uma função do IAM com uma política mais restritiva do que a padrão. Você pode usar a política a seguir. Você também pode modificar essa política para atender às suas necessidades.

A política a seguir mostra as permissões necessárias para executar o SageMaker Autopilot com explicabilidade do modelo do 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"
                    ]
                }
            }
        }
    ]
}
```

A política a seguir mostra todas as permissões mínimas para acesso à federação do Amazon DynamoDB, Redshift Spectrum e 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"
                    ]
                }
            }
        }
    ]
}
```

Opcionalmente, para usar uma chave do AWS KMS para criptografia, adicione as permissões a seguir à política.

```
{
    "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>"
    ]
}
```

Para permitir que o Amazon Redshift e o SageMaker assumam a função do IAM precedente para interagir com outros serviços, adicione a política de confiança a seguir à função.

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

Na precedente, o bucket do Amazon S3 `redshift-downloads/redshift-ml/` é o local onde os dados de exemplo usados para outras etapas e exemplos são armazenados. Você pode remover esse bucket se não precisar carregar dados do Amazon S3. Ou substitua-o por outros buckets do Amazon S3 que você usa para carregar dados no Amazon Redshift.

Os valores **`your-account-id`**, **`your-role`** e **`your-s3-bucket`** são o ID da conta, a função e o bucket especificados no comando CREATE MODEL.

Opcionalmente, use as chaves do AWS KMS da política de exemplo se você especificar uma chave do AWS KMS ao usar o Amazon Redshift ML. O valor **`your-kms-key`** é a chave que você usa como parte do comando CREATE MODEL.

Ao especificar uma Virtual Private Cloud (VPC) privada para o trabalho de ajuste de hiperparâmetros, adicione as permissões a seguir.

```
{
            "Effect": "Allow",
            "Action": [
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeVpcs",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups"
            ]
}
```

Para trabalhar com explicação do modelo, verifique se você tem as permissões para chamar as operações da API do SageMaker. Recomendamos usar a política gerenciada `AmazonSageMakerFullAccess`. Para criar uma função do IAM com uma política mais restritiva, use a política a seguir.

```
{
  "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": "*"
    }
  ]
}
```

Para obter mais informações sobre a política gerenciada `AmazonSageMakerFullAccess`, consulte AmazonSageMakerFullAccess no Guia do desenvolvedor do Amazon SageMaker.

Se você quiser criar modelos do Forecast, recomendamos que use a política gerenciada `AmazonForecastFullAccess`. Se você quiser usar uma política mais restritiva, adicione a política a seguir ao seu perfil do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "forecast:CreateAutoPredictor",
                "forecast:CreateDataset",
                "forecast:CreateDatasetGroup",
                "forecast:CreateDatasetImportJob",
                "forecast:CreateForecast",
                "forecast:CreateForecastExportJob",
                "forecast:DeleteResourceTree",
                "forecast:DescribeAutoPredictor",
                "forecast:DescribeDataset",
                "forecast:DescribeDatasetGroup",
                "forecast:DescribeDatasetImportJob",
                "forecast:DescribeForecast",
                "forecast:DescribeForecastExportJob",
                "forecast:StopResource",
                "forecast:TagResource",
                "forecast:UpdateDatasetGroup"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Para obter mais informações sobre o Amazon Redshift ML, consulte Usar o machine learning no Amazon Redshift ou CREATE MODEL.

## Permissões para ingestão de streaming

A ingestão de streaming funciona com dois serviços: o Kinesis Data Streams e o Amazon MSK.

Permissões necessárias para usar a ingestão de streaming com o Kinesis Data Streams

Há um procedimento com um exemplo de política gerenciada disponível em Conceitos básicos da ingestão de streaming do Amazon Kinesis Data Streams.

Permissões necessárias para usar a ingestão de streaming com o Amazon MSK

Há um procedimento com um exemplo de política gerenciada disponível em Conceitos básicos da ingestão de streaming do Amazon Managed Streaming for Apache Kafka.

## Permissões necessárias para usar as operações de API de compartilhamento de dados

Para controlar o acesso às operações de API de compartilhamento de dados, use as políticas baseadas em ações do IAM. Para obter mais informações sobre como gerenciar políticas do IAM, consulte Gerenciar políticas do IAM no Manual do usuário do IAM.

Em particular, suponha que um administrador de cluster de produtor precise usar a chamada `AuthorizeDataShare` para autorizar a saída de uma unidade de compartilhamento de dados fora de uma conta da Conta da AWS. Nesse caso, você configura uma política baseada em ação do IAM para conceder essa permissão. Use a chamada `DeauthorizeDataShare` para revogar a saída.

Ao usar políticas baseadas em ações do IAM, você também pode especificar um recurso do IAM na política, como `DataShareARN`. Veja a seguir o formato e um exemplo de `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
```

Você pode restringir o acesso `AuthorizeDataShare` a um datashare específico especificando o nome do datashare na política do IAM.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/SalesShare"
      ],
      "Effect": "Deny"
    }
  ]
}
```

Você também pode restringir a política do IAM a todos os conjuntos de dados de propriedade de um cluster de produtores específico. Para fazer isso, substitua o valor **`datashare-name`** na política com um curinga ou um asterisco. Mantenha o valor de cluster `namespace-guid`.

```
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/
*
```

A seguir está a política do IAM que impede que uma entidade chame `AuthorizeDataShare` nas unidades de compartilhamento de dados detidas por um cluster de produtor específico.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

O DataShareARN restringe o acesso com base no nome da unidade de compartilhamento de dados e no ID global exclusivo (GUID) para o namespace do cluster proprietário. Ele faz isso especificando o nome como um asterisco.

## Políticas de recursos de GetClusterCredentials

Para se conectar a um banco de dados de cluster usando uma conexão JDBC ou ODBC com credenciais de banco de dados do IAM ou chamar de modo programático a ação GetClusterCredentials, você precisará de um conjunto mínimo de permissões. No mínimo, você precisará de permissão para chamar a ação redshift:GetClusterCredentials com acesso a um recurso dbuser.

Se você usar uma conexão JDBC ou ODBC, em vez de especificar server e port, você poderá especificar cluster_id e region; mas, para fazer isso, sua política deve permitir a ação redshift:DescribeClusters com acesso ao recurso cluster.

Se chamar GetClusterCredentials com os parâmetros opcionais Autocreate, DbGroups e DbName, verifique se permitiu as ações e o acesso aos recursos listados na tabela a seguir.

| Parâmetro de GetClusterCredentials | Ação | Recurso |
|---|---|---|
| Autocreate | redshift:CreateClusterUser | dbuser |
| DbGroups | redshift:JoinGroup | dbgroup |
| DbName | N/D | dbname |

Para obter mais informações sobre recursos, consulte Recursos e operações do Amazon Redshift.

Você também pode incluir as seguintes condições na política:

- redshift:DurationSeconds

- `redshift:DbName`
- `redshift:DbUser`

Para obter mais informações sobre as condições, consulte Especificar condições em uma política.

## Exemplos de política gerenciada pelo cliente

Nesta seção, você pode encontrar exemplos de políticas de usuário que concedem permissões para várias ações do Amazon Redshift. Essas políticas funcionam quando você está usando a API do Amazon Redshift, AWS SDKs ou a AWS CLI.

> **Note**
>
> Todos os exemplos usam a Região do Oeste dos EUA (Oregon) (`us-west-2`) e contêm IDs de conta fictícios.

Exemplo 1: permitir ao usuário acesso total a todas as ações e recursos do Amazon Redshift

A política a seguir permite acesso a todas as ações do Amazon Redshift em todos os recursos.

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

O valor `redshift:*` no elemento `Action` indica todas as ações no Amazon Redshift.

Exemplo 2: negar a um usuário o acesso a um conjunto de ações do Amazon Redshift

Por padrão, todas as permissões são negadas. Contudo, às vezes você precisa negar explicitamente o acesso a uma ação ou conjunto de ações específico. A política a seguir permite o acesso a todas

as ações do Amazon Redshift e nega explicitamente o acesso a qualquer ação do Amazon Redshift em que o nome comece com `Delete`. Essa política se aplica a todos os recursos do Amazon Redshift em `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:*"
   }
  ]
}
```

Exemplo 3: permitir que um usuário gerencie clusters

A seguinte política permite que um usuário crie, exclua, modifique e reinicialize todos os clusters e, então, nega permissão para excluir ou alterar qualquer cluster cujo nome de cluster inicie com `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"
    }
  ]
}
```

Exemplo 4: permitir que um usuário autorize e revogue acesso ao snapshot

A seguinte política permite que um usuário, por exemplo o Usuário A, faça o seguinte:

- Autorize o acesso a qualquer snapshot criado a partir de um cluster chamado `shared`.
- Revogue o acesso a snapshot para qualquer snapshot criado a partir do cluster `shared` cujo nome de snapshot inicie com `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"
    }
  ]
}
```

Se o Usuário A tiver permitido que o Usuário B acesse um snapshot, o Usuário B deve ter uma política como a seguinte para permitir que o Usuário B restaure um cluster do snapshot. A seguinte política permite que o Usuário B descreva e restaure snapshots e crie clusters. O nome desses clusters deve iniciar com `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"
    }
  ]
}
```

Exemplo 5: permitir que um usuário copie um snapshot de cluster e restaure um cluster de um snapshot

A seguinte política permite que um usuário copie qualquer snapshot criado a partir de um cluster chamado `big-cluster-1` e restaure qualquer snapshot cujo nome inicie com `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"
    }
  ]
}
```

Exemplo 6: permitir que um usuário acesse o Amazon Redshift e ações e recursos comuns para serviços da AWS relacionados

A política de exemplo a seguir permite acesso a todas as ações e recursos para Amazon Redshift, Amazon Simple Notification Service (Amazon SNS) e Amazon CloudWatch. Ele também permite ações especificadas em todos os recursos relacionados do Amazon EC2 na conta.

> **Note**
>
> As permissões em nível de recurso não são compatíveis com as ações do Amazon EC2 especificadas nesta política de exemplo.

```
{
  "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": [
        "*"
      ]
    }
  ]
}
```

Exemplo 7: permitir que um usuário marque recursos com o console do Amazon Redshift

O exemplo a seguir permite que um usuário marque recursos no console do Amazon Redshift usando o console do Amazon Redshift usando AWS Resource Groups. Essa política pode ser anexada a uma função de usuário que invoca o console novo ou original do Amazon Redshift. Para obter mais informações sobre marcação, consulte Marcação de recursos no Amazon Redshift.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Tagging permissions",
            "Effect": "Allow",
            "Action": [
                "redshift:DeleteTags",
                "redshift:CreateTags",
                "redshift:DescribeTags",
                "tag:UntagResources",
                "tag:TagResources"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

## Política de exemplo para usar GetClusterCredentials

A política a seguir usa esses valores de parâmetro de exemplo:

- Região: `us-west-2`
- Conta da AWS: `123456789012`
- Nome do cluster: `examplecluster`

A política a seguir permite as ações `GetCredentials`, `CreateClusterUser` e `JoinGroup`. A política usa chaves de condição para permitir as ações `GetClusterCredentials` e `CreateClusterUser` somente quando o ID do usuário da AWS corresponde a `"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"`. O acesso ao IAM é solicitado somente para o banco de dados `"testdb"`. A política também permite que os usuários ingressem em um grupo chamado `"common_group"`.

```
{
"Version": "2012-10-17",
  "Statement": [
    {
     "Sid": "GetClusterCredsStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:GetClusterCredentials"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
${redshift:DbUser}",
        "arn:aws:redshift:us-west-2:123456789012:dbname:examplecluster/testdb",
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
      ],
        "Condition": {
           "StringEquals": {
           "aws:userid":"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
           }
        }
    },
    {
      "Sid": "CreateClusterUserStatement",
```

```
      "Effect": "Allow",
      "Action": [
        "redshift:CreateClusterUser"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
${redshift:DbUser}"
      ],
      "Condition": {
        "StringEquals": {
          "aws:userid":"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
        }
      }
    },
    {
      "Sid": "RedshiftJoinGroupStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:JoinGroup"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
      ]
    }
  ]
}
```

## Federação de um provedor de identidades (IdP) nativo para o Amazon Redshift

O gerenciamento de identidades e permissões para o Amazon Redshift é facilitado com a federação do provedor de identidades nativo porque ela utiliza o provedor de identidades existente para simplificar a autenticação e o gerenciamento de permissões. Para isso, ela possibilita o compartilhamento de metadados de identidade de seu provedor de identidades com o Redshift. Para a primeira iteração desse recurso, o provedor de identidades compatível é o Microsoft Azure Active Directory (Azure AD).

Para configurar o Amazon Redshift para que ele possa autenticar identidades do provedor de identidades de terceiro, inscreva o provedor de identidades no Amazon Redshift. Isso permite que o Redshift autentique usuários e funções definidos pelo provedor de identidades. Assim, você pode evitar a necessidade de executar o gerenciamento granular de identidades tanto no provedor de

identidades de terceiro quanto no Amazon Redshift, porque as informações de identidade são compartilhadas.

Para obter informações sobre o uso de perfis de sessão que são transferidos de grupos de provedores de identidades (IdP), consulte PG_GET_SESSION_ROLES no Guia do desenvolvedor de banco de dados do Amazon Redshift.

## Configurar o provedor de identidades no Amazon Redshift

Esta seção mostra as etapas de configuração do provedor de identidades e do Amazon Redshift para estabelecer comunicação para federação do provedor de identidades nativo. Você precisa ter uma conta ativa junto ao seu provedor de identidades. Antes de configurar o Amazon Redshift, você inscreve o Redshift como aplicação em seu provedor de identidades, concedendo consentimento ao administrador.

Conclua as seguintes etapas no Amazon Redshift:

1. Você executa uma instrução SQL para inscrever o provedor de identidades, incluindo descrições dos metadados da aplicação do Azure. Para criar o provedor de identidades no Amazon Redshift, execute o comando a seguir depois de substituir os valores dos parâmetros issuer, client_id, client_secret e audience. Esses parâmetros são específicos do Microsoft Azure AD. Substitua o nome do provedor de identidades por um nome de sua escolha e o namespace por um nome exclusivo para conter usuários e funções do diretório do provedor de identidades.

   ```
   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"]
   }'
   ```

   O tipo `azure` indica que o provedor facilita especificamente a comunicação com o Microsoft Azure AD. Atualmente, esse é o único provedor de identidades de terceiro compatível.

   - issuer: o ID do emissor para confiar no token que é recebido. O identificador exclusivo para tenant_id é anexado ao emissor.
   - client_id: o identificador público exclusivo da aplicação inscrito no provedor de identidades. Ele pode ser chamado de ID da aplicação.

- client_secret: um identificador secreto, ou senha, conhecido apenas pelo provedor de identidades e pela aplicação inscrita.
- audience: o ID da aplicação atribuído à aplicação no Azure.

Em vez de usar um segredo de cliente compartilhado, você pode definir parâmetros para especificar um certificado, uma chave privada e uma senha da chave privada ao criar o provedor de identidades.

```
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"}';
```

A senha da chave privada, client_pk_password, é opcional.

2. Opcional: execute comandos SQL no Amazon Redshift para criar previamente usuários e funções. Isso facilita a concessão de permissões com antecedência. O nome da função no Amazon Redshift é semelhante ao seguinte: <Namespace>:<GroupName on Azure AD>. Por exemplo, quando você cria um grupo no Microsoft Azure AD chamado `rsgroup` e um namespace chamado `aad`, o nome da função é `aad:rsgroup`. Os nomes de usuário e função no Amazon Redshift são definidos a partir desses nomes de usuário e associações de grupo no namespace do provedor de identidades.

   O mapeamento de funções e usuários inclui a verificação do valor `external_id` para garantir que esteja atualizado. A ID externa mapeia para o identificador do grupo ou usuário no provedor de identidades. Por exemplo, a ID externa de uma função mapeia para a ID de grupo do Azure AD correspondente. Da mesma forma, a ID externa de cada usuário é mapeada para sua ID no provedor de identidades.

   ```
   create role "aad:rsgroup";
   ```

3. Conceda permissões relevantes às funções de acordo com seus requisitos. Por exemplo:

```
GRANT SELECT on all tables in schema public to role "aad:rsgroup";
```

4. Você também pode conceder permissões a usuários específicos.

```
GRANT SELECT on table foo to aad:alice@example.com
```

Observe que a associação do perfil de um usuário externo federado está disponível somente na sessão desse usuário. Isso tem implicações na criação de objetos de banco de dados. Quando um usuário externo federado cria um visualização ou procedimento armazenado, por exemplo, o mesmo usuário não pode delegar permissão desses objetos a outros usuários e perfis.

Uma explicação sobre os namespaces

Um namespace mapeia um usuário ou uma função para um provedor de identidades específico. Por exemplo, o prefixo para usuários criados no AWS IAM é `iam:`. Esse prefixo evita colisões de nomes de usuário e possibilita o suporte a vários armazenamentos de identidades. Se o usuário alice@example.com da origem de identidade inscrita com o namespace aad fizer login, o usuário `aad:alice@example.com` será criado no Redshift se ele ainda não existir. Observe que um namespace de usuário e função tem uma função diferente de um namespace de cluster no Amazon Redshift, que é um identificador exclusivo associado a um cluster.

## Como o login funciona com a federação do provedor de identidades (IdP) nativo

Para concluir a configuração preliminar entre o provedor de identidades e o Amazon Redshift, execute algumas etapas: primeiro, inscreva o Amazon Redshift como uma aplicação de terceiro em seu provedor de identidades, solicitando as permissões de API necessárias. Em seguida, crie usuários e grupos no provedor de identidades. Por último, inscreva o provedor de identidades no Amazon Redshift usando instruções SQL, as quais definem parâmetros de autenticação exclusivos do provedor de identidades. Como parte da inscrição do provedor de identidades no Redshift, atribua um namespace para garantir que os usuários e as funções sejam agrupados corretamente.

Quando o provedor de identidades é inscrito no Amazon Redshift, a comunicação entre o Redshift e o provedor de identidades é estabelecida. Um cliente pode então passar tokens e realizar a autenticação no Redshift como uma entidade de provedor de identidades. O Amazon Redshift usa as informações de associação de grupo de IdP a fim de fazer o mapeamento para funções do Redshift. Se o usuário ainda não existir no Redshift, ele será criado. Serão criadas funções mapeadas para grupos de provedores de identidade se elas não existirem. O administrador do Amazon Redshift

concede permissão nas funções, e os usuários podem executar consultas e outras tarefas de banco de dados.

As seguintes etapas descrevem como funciona a federação do provedor de identidades nativo quando um usuário faz login:

1. Quando um usuário faz login usando a opção de IdP nativo, por meio do cliente, o token do provedor de identidades é enviado do cliente ao driver.
2. O usuário é autenticado. Se o usuário ainda não existir no Amazon Redshift, será criado um novo usuário. O Redshift mapeia os grupos de provedores de identidade do usuário para funções do Redshift.
3. As permissões são atribuídas com base nas funções do Redshift do usuário. Elas são concedidas a usuários e funções por um administrador.
4. O usuário pode consultar o Redshift.

## Usar ferramentas de cliente para desktop para se conectar ao Amazon Redshift

Para obter instruções sobre como usar a federação do provedor de identidades nativo para se conectar ao Amazon Redshift com o Power BI, consulte a publicação de blog Integrate Amazon Redshift native IdP federation with Microsoft Azure Active Directory (AD) and Power BI (Integração da federação do IdP nativo do Amazon Redshift com o Microsoft Azure Active Directory (AD) e Power BI). Ela descreve uma implementação detalhada da configuração de IdP nativo do Amazon Redshift com o Azure AD. Além disso, detalha as etapas para configurar a conexão do cliente para o Power BI Desktop ou o serviço Power BI. As etapas incluem registro de aplicações, configuração de permissões e configuração de credenciais.

Para saber como integrar a federação de IdP nativa do Amazon Redshift com o Azure AD, usando o Power BI Desktop e o JDBC Client-SQL Workbench/J, assista ao seguinte vídeo:

Para obter instruções sobre como usar a federação do provedor de identidades nativo para se conectar ao Amazon Redshift com um cliente SQL, especificamente DBeaver ou SQL Workbench/J, consulte a publicação de blog Integrate Amazon Redshift native IdP federation with Microsoft Azure AD using a SQL client (Integração da federação do IdP nativo do Amazon Redshift com o Microsoft Azure AD usando um cliente SQL).

# Conectar o Redshift ao IAM Identity Center para proporcionar aos usuários uma experiência de logon único

É possível gerenciar o acesso de usuário e grupo aos data warehouses do Amazon Redshift por meio da propagação de identidade confiável. Isso funciona por meio de uma conexão entre o Redshift e o AWS IAM Identity Center, que proporciona aos usuários uma experiência de logon único. Isso faz com que você possa trazer usuários e grupos do diretório e atribuir diretamente permissões a eles. Posteriormente, essa conexão dará suporte à vinculação de ferramentas e serviços adicionais. Para ilustrar um caso de ponta a ponta, é possível usar um painel do Amazon QuickSight ou o editor de consultas do Amazon Redshift v2 para acessar o Redshift. Nesse caso, o acesso se baseia em grupos do IAM Identity Center. O Redshift pode determinar quem é um usuário e as associações do grupo. O IAM Identity Center também possibilita a você conectar e gerenciar identidades por meio de um provedor de identidades (IdP) de terceiros, como Okta ou PingOne.

Depois de configurar a conexão entre o Redshift e o IAM Identity Center, o administrador poderá configurar um acesso refinado com base em grupos de provedores de identidade para autorizar o acesso do usuário aos dados.

## Os benefícios da integração do Redshift com o AWS IAM Identity Center

O uso do IAM Identity Center com o Redshift pode beneficiar a organização das seguintes maneiras:

- Os autores do painel no Amazon QuickSight podem se conectar a fontes de dados do Redshift sem precisar inserir senhas novamente ou exigir que um administrador configure perfis do IAM com permissões complexas.
- O IAM Identity Center oferece um local central para os usuários da força de trabalho na AWS. É possível criar diretamente usuários e grupos no IAM Identity Center ou conectar usuários e grupos existentes gerenciados por você em um provedor de identidade baseado em padrões, como Okta, PingOne ou Microsoft Entra ID (Azure AD). O IAM Identity Center direciona a autenticação para a fonte confiável escolhida para usuários e grupos e mantém um diretório de usuários e grupos para acesso pelo Redshift. Para obter mais informações, consulte Manage your identity source e Supported identity providers no Guia de usuário do AWS IAM Identity Center.
- É possível compartilhar uma instância do IAM Identity Center com vários clusters e grupos de trabalho do Redshift usando um recurso simples de descoberta automática e conexão. Isso agiliza a adição de clusters sem o esforço extra de configurar a conexão do IAM Identity Center para cada um, além de garantir que todos os clusters e grupos de trabalho tenham uma visão consistente de usuários, atributos e grupos. A instância do IAM Identity Center da organização deve estar na

mesma região de qualquer unidade de compartilhamento de dados do Redshift a que você esteja se conectando.

- Como as identidades de usuário são conhecidas e registradas com acesso a dados, é mais fácil para você atender aos regulamentos de conformidade por meio da auditoria do acesso do usuário no AWS CloudTrail.

## Configuração da integração do IAM Identity Center com o Amazon Redshift

O administrador de cluster do Amazon Redshift ou o administrador do Amazon Redshift Serverless deve realizar várias etapas para configurar o Redshift como um aplicativo habilitado para o IAM Identity Center. Isso faz com que o Redshift possa descobrir e se conectar automaticamente ao IAM Identity Center para receber serviços de logon e diretório de usuários. Depois disso, quando criar um cluster ou um grupo de trabalho, o administrador do Redshift poderá permitir que o novo data warehouse use o IAM Identity Center para gerenciar o acesso ao banco de dados.

O objetivo de habilitar o Redshift como uma aplicação gerenciada pelo IAM Identity Center é para que você possa controlar as permissões de usuário e grupo dentro do IAM Identity Center ou de um provedor de identidades de terceiros integrado. Quando os usuários do banco de dados fazem logon em um banco de dados do Redshift, por exemplo, um analista ou um cientista de dados compara os grupos no IAM Identity Center e se eles coincidem com os nomes de função no Redshift. Assim, um grupo que define o nome de uma função do banco de dados do Redshift pode acessar um conjunto de tabelas para análise de vendas, por exemplo. As seções a seguir mostram como configurar isso.

### Pré-requisitos

Estes são os pré-requisitos para integrar o IAM Identity Center ao Amazon Redshift:

- Configuração da conta: você deve configurar o IAM Identity Center na conta de gerenciamento da organização AWS se pretende ter casos de uso entre contas ou se usa clusters do Redshift em contas diferentes com a mesma instância do IAM Identity Center. Isso inclui a configuração da origem da identidade. Para obter mais informações, consulte Getting Started, workforce identities e supported identity providers no Guia de usuário do AWS IAM Identity Center. Você deve se certificar de ter criado usuários ou grupos no IAM Identity Center ou sincronizado usuários e grupos da fonte de identidade para poder atribuí-los aos dados no Redshift.

> **Note**
>
> Você tem a opção de usar uma instância da conta do Centro de Identidade do IAM, desde que o Redshift e o Centro de Identidade do IAM estejam na mesma conta. Você pode criar essa instância usando um widget ao criar e configurar um cluster ou um grupo de trabalho do Redshift.

- Configuração de um emissor de tokens confiáveis: em alguns casos, talvez você precise usar um emissor de tokens confiáveis, que é uma entidade capaz de emitir e verificar tokens confiáveis. Para isso, etapas preliminares são necessárias para o administrador do Redshift que configura a integração do IAM Identity Center selecionar o emissor de tokens confiáveis e adicionar os atributos necessários para concluir a configuração. Isso pode incluir a configuração de um provedor de identidades externo para servir como um emissor de tokens confiáveis e a adição dos atributos no console do IAM Identity Center. Para concluir essas etapas, consulte Setting up a trusted token issuer.

  > **Note**
  >
  > A configuração de um emissor de tokens confiáveis não é obrigatória para todas as conexões externas. A conexão com o banco de dados do Redshift com o editor de consultas do Amazon Redshift v2 não exige a configuração do emissor de tokens confiáveis. Porém, ela pode ser aplicada a aplicações de terceiros, como painéis ou aplicações personalizadas, que se autenticam com o provedor de identidades.

- Configuração de um perfil do IAM ou funções: as seções a seguir mencionam permissões que devem ser configuradas. Você precisará adicionar permissões segundo as melhores práticas do IAM. As permissões específicas são detalhadas nos procedimentos a seguir.

Para obter mais informações, consulte Getting Started with IAM Identity Center.

Configuração do provedor de identidades para trabalhar com o IAM Identity Center

A primeira etapa do controle do gerenciamento de identidades de usuário e grupo é se conectar ao IAM Identity Center e configurar o provedor de identidades. É possível usar o próprio IAM Identity Center como o provedor de identidades ou conectar um repositório de identidades de terceiros, como o Okta, por exemplo. Para obter mais informações sobre como configurar a conexão e o provedor de identidades, consulte Connect to an external identity provider no Guia de usuário do IAM Identity

Center. Verifique se, ao final desse processo, você tem uma pequena coleção de usuários e grupos adicionados ao IAM Identity Center, para fins de teste.

Permissões administrativas

Permissões necessárias para o gerenciamento do ciclo de vida da aplicação do Redshift/Centro de Identidade do IAM

Você deve criar uma identidade do IAM, que o administrador do Redshift usa a fim de configurar o Redshift para uso com o Centro de Identidade do IAM. Normalmente, você criaria um perfil do IAM com permissões e o atribuiria a outras identidades conforme necessário. Ele deve ter as permissões listadas para executar as ações a seguir.

Criar a aplicação do Redshift/Centro de Identidade do IAM

- `sso:PutApplicationAssignmentConfiguration`: para segurança.
- `sso:CreateApplication`: usado para criar uma aplicação IAM Identity Center.
- `sso:PutApplicationAuthenticationMethod`: concede acesso à autenticação do Redshift.
- `sso:PutApplicationGrant`: usado para alterar as informações do emissor de tokens confiáveis.
- `sso:PutApplicationAccessScope`: para configuração da aplicação Redshift IAM Identity Center. Isso se aplica ao AWS Lake Formation e a Concessões de Acesso do Amazon S3.
- `redshift:CreateRedshiftIdcApplication`: usado para criar a aplicação Redshift IDC.

Descrever a aplicação do Redshift/Centro de Identidade do IAM

- `sso:GetApplicationGrant`: usado para listar as informações do emissor de tokens confiáveis.
- `sso:ListApplicationAccessScopes`: para que a configuração da aplicação Redshift do Centro de Identidade do IAM liste integrações subsequentes, como para o AWS Lake Formation e a funcionalidade Concessões de Acesso do S3.
- `redshift:DescribeRedshiftIdcApplications`: usado para descrever as aplicações existentes do Centro de Identidade do IAM.

Alterar a aplicação do Redshift/Centro de Identidade do IAM

- `redshift:ModifyRedshiftIdcApplication`: usado para alterar uma aplicação Redshift existente.

- `sso:UpdateApplication`: usado para atualizar uma aplicação IAM Identity Center.
- `sso:GetApplicationGrant`: obtém as informações do emissor de tokens de confiança.
- `sso:ListApplicationAccessScopes`: para configuração da aplicação Redshift IAM Identity Center.
- `sso:DeleteApplicationGrant`: exclui as informações do emissor de tokens confiáveis.
- `sso:PutApplicationGrant`: usado para alterar as informações do emissor de tokens confiáveis.
- `sso:PutApplicationAccessScope`: para configuração da aplicação Redshift IAM Identity Center. Isso se aplica ao AWS Lake Formation e a Concessões de Acesso do Amazon S3.
- `sso:DeleteApplicationAccessScope`: para excluir a configuração da aplicação Redshift do Centro de Identidade do IAM. Isso se aplica ao AWS Lake Formation e a Concessões de Acesso do Amazon S3.

Excluir a aplicação do Redshift/Centro de Identidade do IAM

- `sso:DeleteApplication`: usado para excluir uma aplicação IAM Identity Center.
- `redshift:DeleteRedshiftIdcApplication`: dá a possibilidade de excluir uma aplicação Redshift IDC existente.

Permissões necessárias para o gerenciamento do ciclo de vida da aplicação Redshift/editor de consultas v2

Você deve criar uma identidade do IAM, que o administrador do Redshift usa a fim de configurar o Redshift para uso com o Centro de Identidade do IAM. Normalmente, você criaria um perfil do IAM com permissões e o atribuiria a outras identidades conforme necessário. Ele deve ter as permissões listadas para executar as ações a seguir.

Criar a aplicação do editor de consultas v2 (QEV2)

- `redshift:CreateQev2IdcApplication`: usado para criar a aplicação do QEV2.
- `sso:CreateApplication`: usado para criar uma aplicação do Centro de Identidade do IAM.
- `sso:PutApplicationAuthenticationMethod`: concede acesso à autenticação do Redshift.
- `sso:PutApplicationGrant`: usado para alterar as informações do emissor de tokens confiáveis.

- `sso:PutApplicationAccessScope`: para configuração da aplicação Redshift IAM Identity Center. Isso inclui o editor de consultas v2.
- `sso:PutApplicationAssignmentConfiguration`: para segurança.

Descrever a aplicação do editor de consultas v2

- `redshift:DescribeQev2IdcApplications`: usado para descrever a aplicação QEV2 do Centro de Identidade do IAM.

Alterar a aplicação do editor de consultas v2

- `redshift:ModifyQev2IdcApplication`: usado para alterar a aplicação QEV2 do Centro de Identidade do IAM.
- `sso:UpdateApplication`: usado para alterar a aplicação QEV2 do Centro de Identidade do IAM.

Excluir a aplicação do editor de consultas v2

- `redshift:DeleteQev2IdcApplication`: usado para excluir a aplicação do QEV2.
- `sso:DeleteApplication`: usado para excluir a aplicação do QEV2.

> **Note**
>
> No SDK do Amazon Redshift, as seguintes APIs não estão disponíveis:
>
> - CreateQev2IdcApplication
> - DescribeQev2IdcApplications
> - ModifyQev2IdcApplication
> - DeleteQev2IdcApplication
>
> Essas ações são específicas para realizar a integração do Centro de Identidade do IAM com o QEV2 do Redshift no Console da AWS. Para obter mais informações, consulte Actions defined by Amazon Redshift.

Permissões necessárias para o administrador do banco de dados conectar novos recursos no console

Essas permissões são necessárias para conectar novos clusters provisionados ou grupos de trabalho do Amazon Redshift sem servidor durante o processo de criação. Se você tiver essas permissões, uma seleção vai ser exibida no console para optar por se conectar à aplicação gerenciada pelo Centro de Identidade do IAM para Redshift.

- `redshift:DescribeRedshiftIdcApplications`
- `sso:ListApplicationAccessScopes`
- `sso:GetApplicationAccessScope`
- `sso:GetApplicationGrant`

Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.

Configuração do Redshift como uma aplicação gerenciada pela AWS com o Centro de Identidade do IAM

Para o IAM Identity Center gerenciar identidades para um cluster provisionado do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor, o administrador do Redshift deve concluir as etapas para fazer do Redshift uma aplicação gerenciada pelo Centro de Identidade do IAM:

1. Selecione Integração com Centro de Identidade do IAM no menu do console do Amazon Redshift ou do Amazon Redshift sem servidor e, em seguida, selecione Conectar-se ao Centro de Identidade do IAM. A partir daí, você passa por uma série de seleções para preencher as propriedades da integração do Centro de Identidade do IAM.
2. Escolha um nome de exibição e um nome exclusivo para a aplicação gerenciada pela IDC do Redshift.
3. Especifique o namespace da organização. Trata-se normalmente de uma versão abreviada do nome da organização. Ela é adicionada como um prefixo para as funções e os usuários gerenciados pela IDC no banco de dados do Redshift.
4. Selecione um perfil do IAM a ser usado. Esse perfil do IAM deve ser à parte de outros usados no Redshift, e recomendamos que não seja usado com outras finalidades. As permissões da política específica necessárias são as seguintes:

- `sso:DescribeApplication`: necessária para criar uma entrada do provedor de identidades (IdP) no catálogo.
- `sso:DescribeInstance`: usada para criar manualmente funções ou usuários federados do IdP.

5. Configure conexões cliente e emissores de tokens confiáveis. A configuração de emissores de tokens confiáveis facilita a propagação de identidade confiável ao estabelecer um relacionamento com um provedor de identidades externo. A propagação de identidade possibilita que um usuário, por exemplo, faça logon em uma aplicação e acesse dados específicos em outra aplicação. Isso permite aos usuários coletar dados de locais diferentes com mais facilidade. Nesta etapa, no console, você define atributos para cada emissor de tokens confiáveis. Entre os atributos estão o nome e a declaração do público (ou aud claim), que talvez você precise obter dos atributos de configuração da ferramenta ou do serviço. Talvez você também precise fornecer o nome da aplicação do JSON Web Token (JWT) da ferramenta de terceiros.

   > **Note**
   >
   > O `aud claim` exigido de cada ferramenta ou serviço de terceiros pode variar, com base no tipo de token, que pode ser um token de acesso emitido por um provedor de identidades ou outro tipo, como um token de ID. Cada fornecedor pode ser diferente. Quando você está implementando a propagação de identidade confiável e a integração com o Redshift, é necessário fornecer o valor aud correto para o tipo de token com o qual a ferramenta de terceiros envia para AWS. Verifique as recomendações do fornecedor de ferramentas ou serviços.

   Para obter informações detalhadas sobre a propagação de identidade confiável, consulte How trusted identity propagation works. Além disso, consulte a documentação beta do Centro de Identidade do IAM que acompanha esta documentação.

Depois que o administrador do Redshift concluir as etapas e salvar a configuração, as propriedades do Centro de Identidade do IAM vão ser exibidas no console do Redshift. Também é possível consultar a exibição de sistema SVV_IDENTITY_PROVIDERS para verificar as propriedades da aplicação. Isso inclui o nome e o namespace da aplicação. Você usa o namespace como prefixo para objetos de banco de dados do Redshift associados à aplicação. A conclusão dessas tarefas

torna o Redshift uma aplicação compatível com o Centro de Identidade do IAM. As propriedades no console incluem o status da integração. Ele indica Habilitado quando a integração está concluída. Depois desse processo, a integração do Centro de Identidade do IAM poderá ser habilitada em cada novo cluster.

Depois da configuração, você poderá incluir usuários e grupos do Centro de Identidade do IAM no Redshift escolhendo a guia Usuários ou Grupos e escolhendo Atribuir.

Habilitação da integração do Centro de Identidade do IAM para um novo cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor

O administrador do banco de dados configura novos recursos do Redshift para trabalhar em alinhamento com o Centro de Identidade do IAM a fim de facilitar o logon e o acesso aos dados. Isso é realizado como parte das etapas para criar um cluster provisionado ou um grupo de trabalho de tecnologia sem servidor. Qualquer pessoa com permissões para criar recursos do Redshift pode realizar essas tarefas de integração do Centro de Identidade do IAM. Ao criar um cluster provisionado, você começa escolhendo Criar cluster no console do Amazon Redshift. As etapas a seguir mostram como habilitar o gerenciamento do Centro de Identidade do IAM para um banco de dados. (Isso não inclui todas as etapas para criar um cluster.)

1. Escolha Habilitar para **<**your cluster name**>** na seção Integração com Centro de Identidade do IAM nas etapas de criação do cluster.
2. Há uma etapa no processo quando você habilita a integração. Você faz isso escolhendo Habilitar integração com Centro de Identidade do IAM no console.
3. Para o novo cluster ou grupo de trabalho, crie funções de banco de dados no Redshift usando comandos SQL. Este é o comando.

   ```
   CREATE ROLE <idcnamespace:rolename>;
   ```

   O namespace e o nome da função são os seguintes:

   - Prefixo do namespace do Centro de Identidade do IAM: este é o namespace definido por você ao configurar a conexão entre o Centro de Identidade do IAM e o Redshift.
   - Nome da função: esta função do banco de dados do Redshift deve coincidir com o nome do grupo no Centro de Identidade do IAM.

   O Redshift se conecta ao Centro de Identidade do IAM e busca as informações necessárias para criar e mapear a função do banco de dados para o grupo do Centro de Identidade do IAM.

Quando um novo data warehouse é criado, o perfil do IAM especificado para a integração do IDC é automaticamente anexado ao cluster provisionado ou ao grupo de trabalho do Amazon Redshift Serverless. Depois de inserir os metadados de cluster necessários e criar o recurso, você poderá verificar o status da integração do Centro de Identidade do IAM nas propriedades. Se os nomes de grupo no Centro de Identidade do IAM tiverem espaços, será necessário usar aspas no SQL ao criar a função correspondente.

Depois de habilitar o banco de dados do Redshift e criar funções, estará tudo pronto para você se conectar ao banco de dados usando o editor de consultas do Amazon Redshift v2 ou Amazon QuickSight. Os detalhes serão explicados mais detalhadamente nas seções a seguir.

Configuração do **`RedshiftIdcApplication`** padrão usando a API

A configuração é realizada pelo administrador de identidades. Usando a API, você cria e preenche um `RedshiftIdcApplication`, que representa a aplicação Redshift no Centro de Identidade do IAM.

1. Para começar, é possível criar usuários e adicioná-los a grupos no Centro de Identidade do IAM. Você faz isso no console da AWS do Centro de Identidade do IAM (IDC).
2. Chame `create-redshift-idc-application` para criar uma aplicação IDC e torná-la compatível com o uso do Redshift. Você cria a aplicação preenchendo os valores necessários. O nome de exibição é o nome a ser mostrado no painel IDC. O ARN do perfil do IAM é um ARN com permissões para o Centro de Identidade do IAM e que também pode ser assumido pelo Redshift.

   ```
   aws redshift create-redshift-idc-application
   --idc-instance-arn 'arn:aws:sso:::instance/ssoins-1234a01a1b12345d'
   --identity-namespace 'MyIdcIdentityNamespace'
   --idc-display-name 'TEST-NEW-APPLICATION'
   --iam-role-arn 'arn:aws:redshift:us-east-1:012345678901:role/TestRedshiftRole'
   --redshift-idc-application-name 'myredshiftidcapplication'
   ```

   O exemplo a seguir mostra uma resposta `RedshiftIdcApplication` de exemplo retornada pela chamada para `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": "AWSIDC",
                "IdcDisplayName": "Redshift-Idc-Application",
                "IamRoleArn": "arn:aws:redshift:us-east-1:012345678901:role/
TestRedshiftRole",
                "IdcManagedApplicationArn": "arn:aws:sso::012345678901:application/
ssoins-1234a01a1b12345d/apl-12345678910",
                "IdcOnboardStatus": "arn:aws:redshift:us-
east-1:123461817589:redshiftidcapplication",
                "RedshiftIdcApplicationArn": "Completed",
                "AuthorizedTokenIssuerList": [
                      "TrustedTokenIssuerArn": ...,
                      "AuthorizedAudiencesList": [...]...
                ]}
```

3. É possível usar `create-application-assignment` para atribuir grupos específicos ou usuários individuais à aplicação gerenciada no Centro de Identidade do IAM. Fazendo isso, você pode especificar grupos para gerenciamento por meio do Centro de Identidade do IAM. Se o administrador do banco de dados criar funções de banco de dados no Redshift, os nomes de grupo no Centro de Identidade do IAM serão mapeados para nomes de função no Redshift. As funções controlam as permissões no banco de dados. Para obter mais informações, consulte Assign user access to applications in the IAM Identity Center console.
4. Depois de habilitar a aplicação, chame `create-cluster` e inclua o ARN da aplicação gerenciada pelo Redshift do Centro de Identidade do IAM. Isso associa o cluster à aplicação gerenciada no Centro de Identidade do IAM.

Associação de uma aplicação do Centro de Identidade do IAM a um cluster ou grupo de trabalho existente

Se tiver um cluster ou grupo de trabalho existente que gostaria de habilitar para a integração do Centro de Identidade do IAM, você poderá fazer isso executando um comando SQL. Você executa o comando a seguir para habilitar a integração. É necessário que um administrador do banco de dados execute a consulta e que a conexão entre o Redshift e o Centro de Identidade do IAM já tenha sido configurada. Quando você define `ENABLE`, ele permite que o Centro de Identidade do IAM ofereça gerenciamento de identidades para o cluster ou o grupo de trabalho.

```
ALTER IDENTITY PROVIDER
<idp_name> | NAMESPACE <namespace> | IAM_ROLE default | 'arn:aws:iam::<AWS account-
id-1>:role/<role-name>' | [DISABLE | ENABLE]
```

É possível remover um provedor de identidades existente. O exemplo a seguir mostra como CASCADE exclui funções e usuários anexados ao provedor de identidades.

```
DROP IDENTITY PROVIDER
<provider_name> [ CASCADE ]
```

Configuração das permissões de usuário

Um administrador configura permissões para recursos variados, com base nos atributos de identidade dos usuários e nas associações de grupo, dentro do provedor de identidades ou diretamente no Centro de Identidade do IAM. Por exemplo, o administrador do provedor de identidades pode adicionar um engenheiro de banco de dados a um grupo indicado para a função. Esse nome de grupo é mapeado para um nome de função de banco de dados do Redshift. A função dá ou restringe acesso a tabelas ou exibições específicas no Redshift.

### Personas de administrador para conectar aplicações

Estas são as personas-chave para conectar aplicações de análise à aplicação gerenciada pelo Centro de Identidade do IAM para Redshift:

- Administrador da aplicação: cria uma aplicação e configura com quais serviços ela permitirá trocas de tokens de identidade. Esse administrador também especifica quais usuários ou grupos têm acesso à aplicação.
- Administrador de dados: configura acesso refinado aos dados. Usuários e grupos no Centro de Identidade do IAM podem ser mapeados para permissões específicas.

## Conexão com o Amazon Redshift usando o Centro de Identidade do IAM por meio do Amazon QuickSight

A seguir, como usar o Amazon QuickSight para se autenticar com o Redshift quando ele está conectado e o acesso é gerenciado por meio do Centro de Identidade do IAM: Autorização de conexões pelo Amazon QuickSight com clusters do Amazon Redshift. Essas etapas também se aplicam ao Amazon Redshift sem servidor.

## Conexão com o Amazon Redshift usando o Centro de Identidade do IAM por meio do editor de consultas do Amazon Redshift v2

Ao concluir as etapas para configurar uma conexão do Centro de Identidade do IAM com o Redshift, o usuário pode acessar o banco de dados e os objetos indicados no banco de dados por meio da

identidade de namespace prefixado com base no Centro de Identidade do IAM. Para obter mais informações sobre como se conectar aos bancos de dados do Redshift com logon no editor de consultas v2, consulte Working with query editor v2.

## Consulta de dados por meio de AWS Lake Formation

O uso de AWS Lake Formation facilita controlar e proteger de maneira centralizada o data lake, além de oferecer acesso aos dados. A configuração da propagação de identidade para o Lake Formation por meio do Centro de Identidade do IAM e do Redshift possibilita ao administrador permitir acesso refinado a um data lake do Amazon S3, com base nos grupos de provedores de identidades (IdP) da organização. Esses grupos são gerenciados por meio do Centro de Identidade do IAM. Esta seção mostra como configurar alguns casos de uso, consultando um data lake e um compartilhamento de dados, que demonstram como aproveitar o Centro de Identidade do IAM com o Redshift para se conectar aos recursos controlados pelo Lake Formation.

Uso de uma conexão do Centro de Identidade do IAM e do Redshift para consultar um data lake

Essas etapas abordam um caso de uso no qual você usa o Centro de Identidade do IAM conectado ao Redshift para consultar um data lake controlado pelo Lake Formation.

Pré-requisitos

Este procedimento tem diversas etapas de pré-requisito:

1. O Centro de Identidade do IAM deve ser configurado para dar suporte à autenticação e ao gerenciamento de identidades com o Redshift. É possível habilitar o Centro de Identidade do IAM pelo console e selecionar uma fonte do provedor de identidades (IdP). Depois disso, sincronize um conjunto dos usuários IdP com o Centro de Identidade do IAM. Você também deve configurar uma conexão entre o Centro de Identidade do IAM e o Redshift seguindo as etapas detalhadas anteriormente neste documento.
2. Crie um novo cluster do Amazon Redshift e habilite o gerenciamento de identidades por meio do Centro de Identidade do IAM nas etapas de configuração.
3. Crie uma aplicação gerenciada do Centro de Identidade do IAM para Lake Formation e a configure. Depois disso, vem a configuração da conexão entre o Centro de Identidade do IAM e o Redshift. As etapas são as seguintes:
   a. Na AWS CLI, use o comando `modify-redshift-idc-application` para habilitar a integração do serviço Lake Formation com a aplicação gerenciada do Centro de Identidade do

IAM para Redshift. Essa chamada inclui o parâmetro `service-integrations`, que é definido como um valor de string da configuração que permite a autorização para o Lake Formation.

b. Configure o Lake Formation usando o comando `create-lake-formation-identity-center-configuration`. Isso cria uma aplicação Centro de Identidade do IAM para Lake Formation, visível no portal do Centro de Identidade do IAM. O administrador deve definir o argumento `--cli-input-json`, cujo valor é o caminho para um arquivo JSON que usa o formato padrão para todas as chamadas de API da CLI da AWS. Você deve incluir valores para o seguinte:

- `CatalogId`: o ID do catálogo do Lake Formation.
- `InstanceArn`: o valor ARN da instância do Centro de Identidade do IAM.

Depois que o administrador concluir a configuração de pré-requisito, o administrador do banco de dados poderá criar um esquema externo com a finalidade de consultar o data lake.

1. O administrador cria o esquema externo: o administrador do banco de dados do Redshift se conecta ao banco de dados e cria um esquema externo usando a seguinte instrução SQL:

```
CREATE EXTERNAL SCHEMA if not exists my_external_schema from DATA CATALOG database
 'my_lf_integrated_db' catalog_id '12345678901234';
```

   A especificação de um perfil do IAM não é necessária nesse caso, porque o acesso é gerenciado por meio do Centro de Identidade do IAM.

2. O administrador concede permissões: o administrador concede uso a um grupo do Centro de Identidade do IAM, que concede permissões em recursos do Redshift. Isso é feito executando uma instrução SQL como a seguinte:

```
GRANT USAGE ON SCHEMA "my_external_schema" to "IDCCO:sales";
```

   Posteriormente, o administrador concederá permissões do Lake Formation em objetos, com base nos requisitos da organização, usando a CLI da AWS:

```
aws lakeformation grant-permissions ...
```

3. Os usuários executam consultas: neste momento, um usuário do Centro de Identidade do IAM que faz parte do grupo de vendas, para fins ilustrativos, pode fazer logon por meio do editor de

consultas v2 no banco de dados do Redshift. Eles podem acabar executando uma consulta que acessa uma tabela no esquema externo, como no seguinte exemplo:

```
SELECT * from my_external_schema.table1;
```

Uso de uma conexão do Centro de Identidade do IAM e do Redshift para se conectar a uma unidade de compartilhamento de dados

É possível acessar uma unidade de compartilhamento de dados por meio de um data warehouse do Redshift diferente quando o acesso é gerenciado por meio do Centro de Identidade do IAM. Para isso, você executa uma consulta para configurar um banco de dados externo. Antes de concluir essas etapas, presume-se que você tenha uma conexão configurada entre o Redshift e o Centro de Identidade do IAM e tenha criado a aplicação AWS Lake Formation, conforme detalhado no procedimento anterior.

1. Criação do banco de dados externo: o administrador cria um banco de dados externo para compartilhamento de dados, referenciando-o por meio do ARN. Este é um exemplo que mostra como fazer isso:

   ```
   CREATE DATABASE "redshift_external_db" FROM ARN 'arn:aws:glue:us-
   east-1:123456789012:database/redshift_external_db-iad' WITH NO DATA CATALOG SCHEMA;
   ```

   Nesse caso de uso, quando você está usando o Centro de Identidade do IAM com Redshift para gerenciamento de identidades, o perfil do IAM não está incluído.

2. O administrador configura permissões: depois de criar um banco de dados, o administrador vai conceder uso a um grupo do Centro de Identidade do IAM. Isso concede permissões em recursos do Redshift:

   ```
   GRANT USAGE ON DATABASE "my_external_db" to "IDCCO:sales";
   ```

   O administrador também concede permissões do Lake Formation em objetos usando a CLI da AWS:

   ```
   aws lakeformation grant-permissions ...
   ```

3. Os usuários executam consultas: um usuário do grupo de vendas pode consultar uma tabela no banco de dados, com base nas permissões atribuídas:

```
select * from redshift_external_db.public.employees;
```

Para obter mais informações sobre como conceder permissões em um data lake e conceder permissões em compartilhamentos de dados, consulte Granting permissions to users and groups. Para obter mais informações sobre como conceder uso a um esquema ou a um banco de dados, consulte GRANT.

## Integração da aplicação ou da ferramenta com o OAuth usando um emissor de tokens confiáveis

Se for um fornecedor de ferramentas, você poderá adicionar a funcionalidade para se conectar ao Redshift por meio da conexão do Centro de Identidade do IAM.

Plug-in para uso do Redshift com o Centro de Identidade do IAM

Este plug-in, usado na autenticação com o Centro de Identidade do IAM, oferece propriedades de conexão adicionais para facilitar a autenticação:

| Nome do plug-in | Descrição | Valor |
| --- | --- | --- |
| `IdpTokenAuthPlugin` | Um plug-in de autenticação que aceita um token do Centro de Identidade do IAM (IDC) ou um OIDC JWT de qualquer provedor de identidade da web vinculado ao IDC. | `com.amazon.redshift.plugin.IdpTokenAuthPlugin` |

O nome do plug-in correspondente para ODBC e Python é IdpTokenAuthPlugin. Além disso, ODBC e Python não usam o nome de classe totalmente qualificado para plug-ins. Só o JDBC o usa. Na ferramenta, use a propriedade `plugin_name` para inserir o valor do nome. Em ferramentas baseadas em Python, essa propriedade é chamada de `credentials_provider`.

O plug-in tem as seguintes opções de conexão associadas:

- IDC_Region: a região da AWS onde a instância do Centro de Identidade do IAM está localizada.

- Identity_Namespace: o namespace de identidade a ser usado durante a autenticação usando o IdpTokenAuthPlugin. Isso ajuda o Redshift a determinar qual instância do IAM Identity Center usar.

Você insere esses valores nas propriedades de conexão da ferramenta desenvolvida e usada por você para se conectar. Para obter mais informações sobre opções do JDBC, consulte Options for JDBC driver version 2.1 configuration. Para obter mais informações sobre opções do ODBC, consulte Configuring ODBC driver options.

### Limitações

Estas limitações são aplicáveis:

- A autenticação de ferramentas baseadas em JDBC, ODBC e Python não é compatível por meio do Redshift conectado ao Centro de Identidade do IAM. Você precisaria personalizar o driver da ferramenta. Ele só dá suporte a conexões do Amazon QuickSight e do editor de consultas v2.
- As configurações de segurança e privacidade do navegador da internet, especialmente aquelas que controlam as configurações seguras de cookies, como o recurso Proteção total contra cookies do Firefox, podem resultar em tentativas de conexão bloqueadas do editor de consultas v2 com o banco de dados do Redshift. Para corrigir o problema, você pode adicionar o URL do site do console do editor de consultas v2 à lista de exceções de proteção contra rastreamento do navegador. Para fazer isso no Firefox, clique no escudo na barra de endereço do navegador e alterne o botão para desativar a proteção contra rastreamento para o editor de consultas v2. No Chrome, se você estiver usando o modo de navegação anônima, clique no ícone de olho na barra de endereço para permitir cookies de terceiros no editor de consultas v2.

## Uso de funções vinculadas ao serviço para o Amazon Redshift

O Amazon Redshift usa funções do AWS Identity and Access Management (IAM) vinculadas ao serviço.. Uma função vinculada a serviço é um tipo exclusivo de função do IAM que está vinculada diretamente ao Amazon Redshift. As funções vinculadas ao serviço são predefinidas pelo Amazon Redshift e incluem todas as permissões exigidas pelo serviço para chamar os serviços da AWS em nome do cluster do Amazon Redshift.

Uma função vinculada ao serviço facilita a configuração do Amazon Redshift porque você não precisa adicionar manualmente as permissões necessárias. A função está vinculada aos casos de uso do Amazon Redshift e tem permissões predefinidas. Apenas o Amazon Redshift pode assumir a função, e apenas a função vinculada ao serviço pode usar a política de permissões predefinida.

O Amazon Redshift cria uma função vinculada ao serviço em sua conta na primeira vez que você criar um cluster. Você pode excluir a função vinculada ao serviço somente depois de excluir todos os clusters do Amazon Redshift em sua conta. Isso protege os recursos do Amazon Redshift porque você não pode remover inadvertidamente as permissões necessárias para acessar os recursos.

O Amazon Redshift oferece suporte ao uso de funções vinculadas a serviços em todas as regiões onde o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

Para obter informações sobre outros produtos compatíveis com funções vinculadas a serviços, consulte Serviços da AWS que funcionam com o IAM e procure serviços que tenham Yes (Sim) na coluna Service-Linked Role (Função vinculada a serviço). Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

## Permissões de função vinculadas ao serviço para Amazon Redshift

O Amazon Redshift usa a função vinculada ao serviço chamada AWSServiceRoleForRedshift — Permite que o Amazon Redshift chame serviços da AWS da em seu nome. Essa função vinculada ao serviço é anexada à seguinte política gerenciada: `AmazonRedshiftServiceLinkedRolePolicy`. Para atualizações dessa política, consulte Políticas gerenciadas pela AWS (predefinidas) pelo Amazon Redshift.

A função vinculada ao serviço AWSServiceRoleForRedshift confia apenas em **`redshift.amazonaws.com`** para assumir a função.

A política de permissões de função vinculada ao serviço AWSServiceRoleForRedshift permite que o Amazon Redshift conclua o seguinte em todos os recursos relacionados:

- `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

Permissões para recursos de rede

As permissões a seguir possibilitam ações no Amazon EC2 para criação e gerenciamento de regras de grupos de segurança. Essas regras e grupos de segurança estão especificamente associados à etiqueta de recurso aws:RequestTag/Redshift do Amazon Redshift. Isso limita o escopo das permissões para recursos específicos do Amazon Redshift.

- ec2:CreateSecurityGroup
- ec2:AuthorizeSecurityGroupEgress
- ec2:AuthorizeSecurityGroupIngress
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress
- ec2:ModifySecurityGroupRules
- ec2:DeleteSecurityGroup

Ações para registro de auditoria

As ações listadas com o prefixo logs pertence ao registro de auditoria e aos recursos relacionados. Especificamente, a criação e o gerenciamento de grupos de logs e fluxos de logs.

- logs:CreateLogGroup

- `logs:PutRetentionPolicy`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogStreams`
- `logs:GetLogEvents`

O JSON a seguir mostra ações e o escopo de recursos, para o Amazon Redshift, para registro de auditoria.

```
[
    {
        "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:*"
        ]
    }
]
```

Para obter mais informações sobre funções vinculadas a serviço e a finalidade delas na AWS, consulte Usar funções vinculadas a serviço. Para obter mais informações sobre ações específicas e outros recursos do IAM para o Amazon Redshift, consulte Ações, recursos e chaves de condição do Amazon Redshift.

Ações para gerenciar credenciais de administrador com AWS Secrets Manager

As ações listadas com o prefixo `secretsmanager` dizem respeito ao uso do Amazon Redshift para gerenciar as credenciais de administrador. Essas ações permitem que o Amazon Redshift use AWS Secrets Manager para criar e gerenciar os segredos de credencial de administrador.

O JSON a seguir mostra ações e o escopo de recursos, para o Amazon Redshift, para gerenciamento das credenciais de administrador com o 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": "*"
    }
]
```

Como permitir que uma entidade do IAM crie perfis vinculados ao serviço AWSServiceRoleForRedshift

```
{
```

```
    "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"}}
}
```

Como permitir que uma entidade do IAM exclua perfis vinculados ao serviço AWSServiceRoleForRedshift

Adicione a seguinte declaração de política às permissões dessa entidade 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"}}
}
```

Como alternativa, você pode usar uma política gerenciada pela AWS para fornecer acesso total ao Amazon Redshift.

## Criar uma função vinculada a serviço para Amazon Redshift

Você não precisa criar manualmente uma função vinculada ao serviço AWSServiceRoleForRedshift. O Amazon Redshift cria a função serviço vinculada a serviço para você. Se a função vinculada ao serviço AWSServiceRoleForRedshift foi excluída de sua conta, o Amazon Redshift cria a função quando você inicia um novo cluster do Amazon Redshift.

> **Important**
>
> Se você usou o serviço Amazon Redshift antes de 18 de setembro de 2017, quando ele começou a oferecer suporte a funções vinculadas a serviços, o Amazon Redshift criou a função AWSServiceRoleForRedshift em sua conta. Para saber mais, consulte Uma nova função apareceu na minha conta do IAM.

### Editar uma função vinculada a serviço para Amazon Redshift

O Amazon Redshift não permite que você edite a função vinculada ao serviço AWSServiceRoleForRedshift. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você pode editar a descrição da função usando o console do IAM, a AWS Command Line Interface (AWS CLI), ou a API do IAM. Para obter mais informações, consulte Modificar uma função noManual do usuário do IAM.

### Excluir uma função vinculada a serviço para Amazon Redshift

Se você não precisar mais usar um recurso ou serviço que exija uma função vinculada a um serviço, recomendamos que você exclua essa função. Dessa forma, você não terá uma entidade não utilizada que não seja ativamente monitorada ou mantida.

Para que você possa excluir uma função vinculada a serviço para uma conta, será necessário desligar e excluir todos os clusters da conta. Para obter mais informações, consulte Desativação e exclusão de clusters.

Também é possível usar o console do IAM, a AWS CLI ou a API do IAM para excluir uma função vinculada ao serviço. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

## Usar a autenticação do IAM para gerar credenciais do usuário do banco de dados

Você pode gerar credenciais de banco de dados temporárias com base em permissões concedidas por meio de uma política de permissões do AWS Identity and Access Management (IAM) para gerenciar o acesso que seus usuários têm ao banco de dados Amazon Redshift.

Normalmente, os usuários do banco de dados do Amazon Redshift efetuam login no banco de dados fornecendo um nome de usuário e uma senha do banco de dados. No entanto, você não precisa manter nomes de usuário e senhas em seu banco de dados do Amazon Redshift. Como alternativa, é possível configurar o sistema para permitir que os usuários criem credenciais de usuário e façam login no banco de dados com base em suas credenciais do IAM.

Para obter mais informações, consulte Provedores de identidade e federação no Guia do usuário do IAM.

Tópicos

- Visão geral
- Criar credenciais temporárias do IAM
- Opções para fornecer credenciais do IAM


## Visão geral

O Amazon Redshift fornece a operação de API GetClusterCredentials para gerar credenciais de usuário de banco de dados temporárias. Você pode configurar seu cliente SQL com drivers JDBC ou ODBC do Amazon Redshift que gerenciam o processo de chamada da operação `GetClusterCredentials`. Eles fazem isso recuperando as credenciais do usuário do banco de dados e estabelecendo uma conexão entre seu cliente SQL e seu banco de dados do Amazon Redshift. Você também pode usar o aplicativo de banco de dados para chamar a ação `GetClusterCredentials`, recuperar credenciais de usuário de base de dados e conectar-se ao banco de dados de modo programático.

Se você já gerencia identidades de usuário fora da AWS, pode usar um provedor de identidade (IdP) compatível com Security Assertion Markup Language (SAML) 2.0 para gerenciar o acesso aos recursos do Amazon Redshift. Configure o IdP para permitir o acesso de usuários federados à função do IAM. Com essa função do IAM, você pode gerar credenciais de banco de dados temporárias e fazer login em bancos de dados do Amazon Redshift.

O cliente SQL precisa de permissão para chamar a operação `GetClusterCredentials` para você. Para gerenciar essas permissões, crie uma função do IAM e anexe a política de permissões do IAM que concede ou restringe o acesso à operação `GetClusterCredentials` e às ações relacionadas. Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.

A política também concede ou restringe o acesso a recursos específicos, como clusters, bancos de dados, nomes de usuário de banco de dados e nomes de grupo de usuários do Amazon Redshift.

> **Note**
>
> Recomendamos o uso dos drivers JDBC ou ODBC do Amazon Redshift para gerenciar o processo de chamada da operação `GetClusterCredentials` e logon no banco de dados. Para simplificar, partimos do pressuposto de que você está usando um cliente SQL com drivers JDBC ou ODBC durante todo este tópico.

Para obter detalhes específicos e exemplos de uso da operação `GetClusterCredentials` ou do comando paralelo da CLI `get-cluster-credentials`, consulte GetClusterCredentials e get-cluster-credentials.

Para gerenciar a autenticação e a autorização de forma centralizada, o Amazon Redshift oferece suporte à autenticação do banco de dados com IAM, permitindo a autenticação do usuário por meio da federação empresarial. Em vez de criar um usuário, é possível usar identidades existentes do AWS Directory Service, do diretório de usuário da sua empresa ou de um provedor de identidade da web. Eles são conhecidos como usuários federados. A AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um IdP.

Para fornecer acesso federado a um usuário ou aplicação cliente em sua organização para chamar operações de API do Amazon Redshift, você também pode usar o driver JDBC ou ODBC com suporte SAML 2.0 para solicitar autenticação do IdP de sua organização. Nesse caso, os usuários da sua organização não têm acesso direto ao Amazon Redshift.

## Criar credenciais temporárias do IAM

Nesta seção, você pode encontrar como configurar o sistema para gerar credenciais de usuário de banco de dados temporárias baseadas no IAM e fazer login no banco de dados usando as novas credenciais.

Basicamente, o fluxo do processo é o seguinte:

1. Etapa 1: Criar um perfil do IAM para acesso por autenticação única do IAM

   (Opcional) Você pode autenticar usuários para acesso a um banco de dados do Amazon Redshift integrando a autenticação IAM e um provedor de identidade de terceiros (IdP).

2. Etapa 2: configurar declarações de SAML para o IdP

   (Opcional) Para usar a autenticação do IAM usando um IdP, é necessário definir uma regra de reivindicação no aplicativo do IdP que mapeie usuários ou grupos da organização para a função do IAM. Opcionalmente, você pode incluir elementos de atributo para definir parâmetros de `GetClusterCredentials`.

3. Etapa 3: criar um perfil do IAM com permissões para chamar GetClusterCredentials

A aplicação cliente SQL assume o usuário quando ele chama a operação `GetClusterCredentials`. Se você tiver criado uma função do IAM para acesso do provedor de identidade, poderá adicionar a permissão necessária a essa função.

4. Etapa 4: criar um usuário de banco de dados e grupos de bancos de dados

   (Opcional) Por padrão, `GetClusterCredentials` retorna credenciais para criar um novo usuário se o nome de usuário não existir. Você também pode especificar grupos de usuários aos quais os usuários poderão se associar no logon. Por padrão, os usuários de banco de dados se associam ao grupo PUBLIC.

5. Etapa 5: configurar uma conexão JDBC ou ODBC para usar credenciais do IAM

   Para se conectar ao seu banco de dados Amazon Redshift, você configura seu cliente SQL para usar um driver JDBC ou ODBC do Amazon Redshift.

Etapa 1: Criar um perfil do IAM para acesso por autenticação única do IAM

Se você não usa um provedor de identidade para acesso de logon único, ignore esta etapa.

Se você já gerencia identidades de usuário fora da AWS, pode autenticar usuários para acesso a um banco de dados do Amazon Redshift integrando a autenticação IAM e um provedor de identidade SAML-2.0 de terceiros (IdP).

Para obter mais informações, consulte Provedores de identidade e federação no Guia do usuário do IAM.

Antes de usar a autenticação IdP do Amazon Redshift, crie um provedor de identidade SAML AWS. Crie um IdP no console do IAM para informar a AWS sobre o IdP e sua configuração. Isso estabelece a confiança entre a conta da AWS e o IdP. Para obter as etapas de criação de uma função, consulte Criar uma função para federação SAML 2.0 (console) no Manual do usuário do IAM.

Etapa 2: configurar declarações de SAML para o IdP

Após criar a função do IAM, defina uma regra de reivindicação no aplicativo do IdP para mapear usuários ou grupos da organização para a função do IAM. Para obter mais informações, consulte Configurando declarações de SAML para a resposta de autenticação no Manual do usuário do IAM.

Se você optar por usar os parâmetros opcionais de `GetClusterCredentials` `DbUser`, `AutoCreate` e `DbGroups`, terá duas opções. Você poderá definir os valores dos parâmetros com a

conexão JDBC ou ODBC ou definir os valores adicionando elementos de atributo de SAML ao IdP. Para obter mais informações sobre os parâmetros `DbGroups`, `DbUser` e `AutoCreate`, consulte Etapa 5: configurar uma conexão JDBC ou ODBC para usar credenciais do IAM.

> **Note**
>
> Se você usar uma variável de política do IAM `${redshift:DbUser}`, conforme descrito em Políticas de recursos de GetClusterCredentials, o valor para `DbUser` será substituído pelo valor recuperado pelo contexto da solicitação da operação de API. Os drivers do Amazon Redshift usam o valor da variável `DbUser` fornecida pelo URL de conexão, em vez do valor fornecido como um atributo SAML.
> Para ajudar a proteger essa configuração, recomendamos que você use uma condição em uma política do IAM para validar o valor `DbUser` usando o `RoleSessionName`. Você pode encontrar exemplos de como definir uma condição usando uma política do IAM em Política de exemplo para usar GetClusterCredentials.

Para configurar o IdP para definir os parâmetros `DbGroups`, `DbUser` e `AutoCreate`, inclua os seguintes elementos `Attribute`:

- Um elemento `Attribute` com o atributo `Name` definido para "https://redshift.amazon.com/SAML/Attributes/DbUser"

  Defina o elemento `AttributeValue` como o nome de um usuário que se conectará ao banco de dados do Amazon Redshift.

  O valor do elemento `AttributeValue` deve estar em minúsculas, começar com uma letra, conter somente caracteres alfanuméricos, sublinhado ("_"), sinal de adição ("+"), ponto ("."), arroba ("@") ou hífen ("-") e ter menos de 128 caracteres. Normalmente, o nome de usuário é um ID de usuário (por exemplo, bobsmith) ou um endereço de e-mail (por exemplo, bobsmith@example.com). O valor não pode incluir um espaço (por exemplo, o nome de exibição de um usuário, como Bob Smith).

  ```
  <Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbUser">
      <AttributeValue>user-name</AttributeValue>
  </Attribute>
  ```

- Um elemento Attribute com o atributo Name definido para "https://redshift.amazon.com/SAML/Attributes/AutoCreate"

Defina o elemento AttributeValue como true para criar um novo usuário de banco de dados caso não exista um. Defina o AttributeValue como false para especificar que o usuário do banco de dados deve existir no banco de dados do Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/AutoCreate">
    <AttributeValue>true</AttributeValue>
</Attribute>
```

- Um elemento `Attribute` com o atributo `Name` definido para "https://redshift.amazon.com/SAML/Attributes/DbGroups"

  Este elemento contém um ou mais elementos `AttributeValue`. Defina cada elemento `AttributeValue` com um nome de grupo de banco de dados ao qual o `DbUser` se junta durante a sessão ao se conectar ao banco de dados do Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbGroups">
    <AttributeValue>group1</AttributeValue>
    <AttributeValue>group2</AttributeValue>
    <AttributeValue>group3</AttributeValue>
</Attribute>
```

Etapa 3: criar um perfil do IAM com permissões para chamar GetClusterCredentials

Seu cliente SQL precisa de autorização para chamar a operação `GetClusterCredentials` em seu nome. Para fornecer essa autorização, crie um usuário ou um perfil e anexe uma política que conceda as permissões necessárias.

Para criar uma função do IAM com permissões para chamar GetClusterCredentials

1. Usando o serviço do IAM, crie um usuário ou um perfil. Você também pode utilizar um usuário ou uma função existente. Por exemplo, se você tiver criado uma função do IAM para acesso do provedor de identidade, poderá anexar as políticas do IAM necessária a essa função.
2. Anexe uma política de permissão com permissão para chamar a operação `redshift:GetClusterCredentials`. Dependendo de quais parâmetros opcionais forem especificados, você também poderá permitir ou restringir ações e recursos adicionais na política:

- Para permitir que seu cliente SQL recupere a ID, região da AWS e porta do cluster, inclua permissão para chamar a operação `redshift:DescribeClusters` com o recurso de cluster Redshift.
- Se você usar a opção `AutoCreate`, inclua uma permissão para chamar `redshift:CreateClusterUser` com o recurso `dbuser`. O nome do recurso da Amazon (ARN) a seguir especifica o `dbuser` do Amazon Redshift. Substitua *`region`*, *`account-id`* e *`cluster-name`* pelos valores da região, conta e cluster da AWS. Em *`dbuser-name`*, especifique o nome de usuário a ser usado para fazer login no banco de dados do cluster.

  ```
  arn:aws:redshift:region:account-id:dbuser:cluster-name/dbuser-name
  ```

- (Opcional) Adicione um ARN que especifica o recurso `dbname` do Amazon Redshift no formato a seguir. Substitua *`region`*, *`account-id`* e *`cluster-name`* pelos valores da região, conta e cluster da AWS. Em *`database-name`*, especifique o nome de um banco de dados no qual o usuário fará login.

  ```
  arn:aws:redshift:region:account-id:dbname:cluster-name/database-name
  ```

- Se você usar a opção `DbGroups`, inclua permissão para chamar a operação `redshift:JoinGroup` com o recurso `dbgroup` do Amazon Redshift no formato a seguir. Substitua *`region`*, *`account-id`* e *`cluster-name`* pelos valores da região, conta e cluster da AWS. Em *`dbgroup-name`*, especifique o nome de um grupo de usuários ao qual o usuário se associará no login.

  ```
  arn:aws:redshift:region:account-id:dbgroup:cluster-name/dbgroup-name
  ```

Para ter mais informações e exemplos, consulte Políticas de recursos de GetClusterCredentials.

O exemplo a seguir mostra uma política que permite que a função do IAM chame a operação `GetClusterCredentials`. Especificar o recurso `dbuser` do Amazon Redshift concede à função acesso ao nome de usuário do banco de dados `temp_creds_user` no cluster nomeado `examplecluster`.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
temp_creds_user"
  }
}
```

Você pode usar um curinga (*) para substituir, total ou parcialmente, o nome do cluster, o nome de usuário e os nomes de grupo de bancos de dados. O exemplo a seguir permite que qualquer nome de usuário comece com `temp_` em qualquer cluster na conta especificada.

> **Important**
>
> A instrução no exemplo a seguir especifica um caractere coringa (*) como parte do valor para o recurso, para que a política permita qualquer nome de recurso que comece com os caracteres especificados. Usar um caractere coringa em suas políticas de IAM pode ser excessivamente permissivo. Como uma prática recomendada, recomendamos o uso de políticas mais restritivas possíveis para seu aplicativo de negócios.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:*/temp_*"
  }
}
```

O exemplo a seguir mostra uma política que permite que a função do IAM chame a operação `GetClusterCredentials` com a opção de criar automaticamente um novo usuário e especificar grupos aos quais o usuário se associará no login. A cláusula `"Resource": "*"` concede à função acesso a qualquer recurso, incluindo clusters, usuários de banco de dados ou grupos de usuários.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
```

```
            "redshift:GetClusterCredentials",
            "redshift:CreateClusterUser",
  "redshift:JoinGroup"
          ],
    "Resource": "*"
  }
}
```

Para obter mais informações, consulte Amazon Redshift ARN syntax.

Etapa 4: criar um usuário de banco de dados e grupos de bancos de dados

Se desejar, é possível criar um usuário de banco de dados que você usará para fazer login no banco de dados do cluster. Se você criar credenciais de usuário temporárias para um usuário existente, poderá desabilitar a senha do usuário para forçar o usuário a fazer logon com a senha temporária. Como alternativa, você pode usar a opção Autocreate de `GetClusterCredentials` para criar automaticamente um novo usuário de banco de dados.

É possível criar grupos de usuários de banco de dados com as permissões às quais o usuário do banco de dados do IAM deve se associar no login. Quando você chamar a operação `GetClusterCredentials`, poderá especificar uma lista de nomes de grupo de usuários aos quais o novo usuário se associará no login. Essas associações de grupos são válidas somente para sessões criadas através das credenciais geradas com a solicitação específica.

Para criar um usuário de banco de dados e grupos de bancos de dados

1. Faça login em seu banco de dados Amazon Redshift e crie um usuário de banco de dados usando CREATE USER ou altere um usuário existente usando ALTER USER.
2. Se desejar, especifique a opção PASSWORD DISABLE para impedir que o usuário utilize uma senha. Quando a senha de um usuário é desabilitada, ele só pode fazer login usando as credenciais temporárias. Se a senha não for desabilitada, o usuário poderá fazer login com a senha ou usando as credenciais temporárias. Não é possível desabilitar a senha de um superusuário.

   Os usuários precisam de acesso programático se quiserem interagir com a AWS de fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando a AWS.

   Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| Identificação da força de trabalho<br><br>(Usuários gerenciados no Centro de Identidade do IAM) | Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções da interface que deseja utilizar.<br><br>• Para a AWS CLI, consulte Configuração da AWS CLI para usar o AWS IAM Identity Center no AWS Command Line Interface Guia do usuário da .<br>• Para os SDKs da AWS, ferramentas e APIs da AWS, consulte Autenticação do Centro de Identidade do IAM no Guia de referência de ferramentas e SDKs da AWS. |
| IAM | Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções em Como usar credenciais temporárias com recursos da AWS no Guia do usuário do IAM. |

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| IAM | (Não recomendado)<br>Use credenciais de longo prazo para assinar solicitaç ões programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções da interface que deseja utilizar.<br>• Para a AWS CLI, consulte Autenticação usando as credenciais de usuário do IAM no Guia do usuário da AWS Command Line Interface.<br>• Para as ferramentas e SDKs da AWS, consulte Autenticação usando as credenciais de longo prazo no Guia de referência de ferramentas e SDKs da AWS.<br>• Para as APIs da AWS, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM. |

O exemplo a seguir cria um usuário com a senha desabilitada.

```
create user temp_creds_user password disable;
```

O exemplo a seguir desabilita a senha de um usuário existente.

```
alter user temp_creds_user password disable;
```

3. Crie grupos de usuários de banco de dados usando CREATE GROUP.
4. Use o comando GRANT para definir os privilégios de acesso dos grupos.

### Etapa 5: configurar uma conexão JDBC ou ODBC para usar credenciais do IAM

Você pode configurar seu cliente SQL com um driver JDBC ou ODBC do Amazon Redshift. Este driver gerencia o processo de criação de credenciais de usuário de banco de dados e de estabelecimento de uma conexão entre seu cliente SQL e seu banco de dados Amazon Redshift.

Se você usa um provedor de identidade para autenticação, especifique o nome de um plug-in de provedor de credenciais. Os drivers JDBC e ODBC do Amazon Redshift incluem plug-ins para os seguintes provedores de identidade baseados em SAML:

- Active Directory Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure AD

  Para obter as etapas para configurar o Microsoft Azure AD como um provedor de identidade, consulte Configurar a autenticação única de JDBC ou ODBC com o Microsoft Azure AD.

Para configurar uma conexão JDBC para usar credenciais do IAM

1. Baixe o driver JDBC Amazon Redshift mais recente da página Configurar uma conexão para o driver JDBC versão 2.1 para o Amazon Redshift.
2. Crie um URL de JDBC com as opções de credenciais do IAM em um dos formatos a seguir. Para usar a autenticação do IAM, adicione `iam:` ao URL do JDBC do Amazon Redshift seguido por `jdbc:redshift:` conforme especificado no exemplo a seguir.

   ```
   jdbc:redshift:iam://
   ```

   Adicione `cluster-name`, `region`, `eaccount-id`. O driver JDBC usa as informações da sua conta IAM e o nome do cluster para recuperar o ID do cluster e a região da AWS. Para fazer isso, o usuário ou o perfil do IAM deve ter permissão para chamar a operação `redshift:DescribeClusters` com o cluster especificado. Se o seu usuário ou perfil não tiver permissão para chamar a operação `redshift:DescribeClusters`, inclua o ID do cluster, a região da AWS e a porta, conforme mostrado no exemplo a seguir. O número da porta é opcional.

```
jdbc:redshift:iam://examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com:5439/dev
```

3. Adicione opções JDBC para fornecer credenciais do IAM. Use combinações diferentes de opções JDBC para fornecer credenciais do IAM. Para obter detalhes, consulte Opções JDBC e ODBC para criar credenciais de usuário de banco de dados.

   O URL a seguir especifica o AccessKeyID e a SecretAccessKey para um usuário.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?
   AccessKeyID=AKIAIOSFODNN7EXAMPLE&SecretAccessKey=wJalrXUtnFEMI/K7MDENG/
   bPxRfiCYEXAMPLEKEY
   ```

   O exemplo a seguir especifica um perfil nomeado que contém as credenciais do IAM.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?Profile=user2
   ```

4. Adicione opções JDBC que o driver JDBC usa para chamar a operação `GetClusterCredentials` da API. Não inclua essas opções se você chamar a operação `GetClusterCredentials` da API de forma programática.

   O exemplo a seguir inclui as opções JDBC do `GetClusterCredentials`.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?
   plugin_name=com.amazon.redshift.plugin.AzureCredentialsProvider&UID=user&PWD=password&idp_t
   ```

Para configurar uma conexão ODBC para usar credenciais do IAM

No procedimento a seguir, você pode encontrar etapas somente para configurar a autenticação do IAM. Para que as etapas usem autenticação padrão, usando um nome de usuário de banco de dados e uma senha, consulte Configurar uma conexão ODBC.

1. Instale e configure o driver ODBC do Amazon Redshift mais recente para o seu sistema operacional. Para obter mais informações, consulte a página Configurar uma conexão ODBC.

   > **Important**
   >
   > O driver ODBC do Amazon Redshift deve ser a versão 1.3.6.1000 ou posterior.

2. Siga as etapas referentes ao seu sistema operacional para definir as configurações de conexão.

   Para obter mais informações, consulte um dos seguintes:

   - Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows
   - Use um gerenciador de driver ODBC para configurar o driver nos sistemas operacionais Linux e macOS X

3. Em sistemas operacionais Microsoft Windows, acesse a janela Configuração de DSN do driver ODBC do Amazon Redshift.

   a. Em Connection Settings, insira as seguintes informações:

      - Nome da fonte de dados
      - Server (opcional)
      - Port (opcional)
      - Database

      Se o usuário ou o perfil do IAM tiver permissão para chamar a operação `redshift:DescribeClusters`, somente Nome da fonte de dados e Banco de dados são obrigatórios. O Amazon Redshift usa ClusterId eRegião para obter o servidor e a porta chamando a operação `DescribeCluster`.

      Se o usuário ou o perfil não tiver permissão para chamar a operação `redshift:DescribeClusters`, especifique Servidor e Porta.

   b. Em Autenticação, escolha um valor para Auth Type (Tipo de autenticação).

      Para cada tipo de autenticação, insira valores conforme listado a seguir:

      Perfil do AWS

         Insira as seguintes informações:

         - ClusterID
         - Region
         - Profile name

Insira o nome de um perfil em um arquivo de configuração AWS que contém valores para as opções de conexão ODBC. Para obter mais informações, consulte Uso de um perfil de configuração.

(Opcional) Forneça detalhes para opções que o driver ODBC usa para chamar a operação `GetClusterCredentials` da API:

- DbUser
- User AutoCreate
- DbGroups

Para obter mais informações, consulte Opções JDBC e ODBC para criar credenciais de usuário de banco de dados.

Credenciais do IAM

Insira as seguintes informações:

- ClusterID
- Region
- AccessKeyID e SecretAccessKey

O ID da chave de acesso e a chave de acesso secreta do usuário ou perfil do IAM configurado para autenticação do banco de dados do IAM.

- SessionToken

SessionToken é obrigatório para uma função do IAM com credenciais temporárias. Para obter mais informações, consulte Credenciais de segurança temporárias.

Forneça detalhes para opções que o driver ODBC usa para chamar a operação `GetClusterCredentials` da API:

- DbUser (obrigatório)
- User AutoCreate (opcional)
- DbGroups (opcional)

Para obter mais informações, consulte Opções JDBC e ODBC para criar credenciais de usuário de banco de dados.

Provedor de identidade: AD FS

Para Autenticação Integrada do Windows com AD FS, deixe User and Password vazios.

Forneça os detalhes do IdP:

- IdP Host

  O nome do host corporativo do provedor de identidade. Este nome não deve conter barras (/).

- IdP Port (opcional)

  A porta usada pelo provedor de identidade. O padrão é 443.

- Preferred Role

  O nome do recurso da Amazon (ARN) de uma função do IAM nos elementos `AttributeValue` de vários valores do atributo `Role` na declaração de SAML. Trabalhe com o administrador do IdP para localizar o valor apropriado da função preferencial. Para obter mais informações, consulte Configurar declarações de SAML para o IdP.

(Opcional) Forneça detalhes para opções que o driver ODBC usa para chamar a operação `GetClusterCredentials` da API:

- DbUser
- User AutoCreate
- DbGroups

Para obter mais informações, consulte Opções JDBC e ODBC para criar credenciais de usuário de banco de dados.

Provedor de identidade: PingFederate

Em User (Usuário) e Password (Senha), insira o nome de usuário e a senha do IdP.

Forneça os detalhes do IdP:

- IdP Host

O nome do host corporativo do provedor de identidade. Este nome não deve conter barras (/).

- IdP Port (opcional)

  A porta usada pelo provedor de identidade. O padrão é 443.

- Preferred Role

  O nome do recurso da Amazon (ARN) de uma função do IAM nos elementos `AttributeValue` de vários valores do atributo `Role` na declaração de SAML. Trabalhe com o administrador do IdP para localizar o valor apropriado da função preferencial. Para obter mais informações, consulte Configurar declarações de SAML para o IdP.

(Opcional) Forneça detalhes para opções que o driver ODBC usa para chamar a operação `GetClusterCredentials` da API:

- DbUser
- User AutoCreate
- DbGroups

Para obter mais informações, consulte Opções JDBC e ODBC para criar credenciais de usuário de banco de dados.

Provedor de identidade: Okta

Em User (Usuário) e Password (Senha), insira o nome de usuário e a senha do IdP.

Forneça os detalhes do IdP:

- IdP Host

  O nome do host corporativo do provedor de identidade. Este nome não deve conter barras (/).

- IdP Port

  Esse valor não é usado pelo Okta.

- Preferred Role

O nome do recurso da Amazon (ARN) da função do IAM nos elementos `AttributeValue` do atributo `Role` na declaração de SAML. Trabalhe com o administrador do IdP para localizar o valor apropriado da função preferencial. Para obter mais informações, consulte Configurar declarações de SAML para o IdP.

- Okta App ID

  O ID de um aplicativo do Okta. O valor de App ID vem depois de "amazon_aws" no link de incorporação de aplicativo do Okta. Consulte o administrador do IdP para obter esse valor.

(Opcional) Forneça detalhes para opções que o driver ODBC usa para chamar a operação `GetClusterCredentials` da API:

- DbUser
- User AutoCreate
- DbGroups

Para obter mais informações, consulte Opções JDBC e ODBC para criar credenciais de usuário de banco de dados.

Provedor de identidade: Azure AD

Em User (Usuário) e Password (Senha), insira o nome de usuário e a senha do IdP.

Para o ID do cluster e a Região, insira o ID do cluster e a região da AWS do cluster do Amazon Redshift.

Para Banco de dados, insira o banco de dados que você criou para o cluster do Amazon Redshift.

Forneça os detalhes do IdP:

- IdP Tenant (Locatário IdP)

  O locatário usado para o Azure AD.

- Azure Client Secret (Segredo do cliente do Azure)

  O segredo do cliente da aplicação empresarial Amazon Redshift no Azure.

- Azure Client ID (ID do cliente do Azure)

A ID do cliente (ID do aplicativo) da aplicação empresarial Amazon Redshift no Azure.

(Opcional) Forneça detalhes para opções que o driver ODBC usa para chamar a operação `GetClusterCredentials` da API:

- DbUser
- User AutoCreate
- DbGroups

Para obter mais informações, consulte Opções JDBC e ODBC para criar credenciais de usuário de banco de dados.

## Opções para fornecer credenciais do IAM

Para fornecer credenciais do IAM para uma conexão JDBC ou ODBC, escolha uma das opções a seguir.

- Perfil da AWS

  Como alternativa ao fornecimento de valores de credenciais sob a forma de configurações JDBC ou ODBC, você pode colocar os valores em um perfil nomeado. Para obter mais informações, consulte Uso de um perfil de configuração.
- Credenciais do IAM

  Forneça valores para AccessKeyID, SecretAccessKey e, opcionalmente, SessionToken sob a forma de configurações JDBC ou ODBC. SessionToken é obrigatório somente em uma função do IAM com credenciais temporárias. Para obter mais informações, consulte Opções JDBC e ODBC para fornecer credenciais do IAM.
- Federação do provedor de identidade

  Ao usar a federação de provedor de identidade para permitir que usuários de um provedor de identidade se autentiquem no Amazon Redshift, especifique o nome de um plug-in de provedor de credencial. Para obter mais informações, consulte Usar um plug-in de provedor de credenciais.

  Os drivers JDBC e ODBC do Amazon Redshift incluem plug-ins para os seguintes provedores de credenciais de federação de identidade baseados em SAML:
  - Microsoft Active Identity Federation Services (AD FS)
  - PingOne

- Okta
- Microsoft Azure Active Directory (Azure AD)

Você pode fornecer o nome de plug-in e valores relacionados sob a forma de configurações JDBC ou ODBC ou usando um perfil. Para ter mais informações, consulte Opções para a configuração do driver JDBC versão 2.1 e Configurar as opções do driver ODBC.

Para obter mais informações, consulte Configurar uma conexão JDBC ou ODBC para usar credenciais do IAM.

Uso de um perfil de configuração

Você pode fornecer as opções `GetClusterCredentials` e opções de credenciais do IAM como configurações em perfis nomeados em seu arquivo de configuração da AWS. Para fornecer o nome do perfil, use a opção de perfil JDBC. A configuração é armazenada em um arquivo chamado `config` ou um arquivo chamado `credentials` em uma pasta chamada `.aws` no seu diretório inicial.

Para um plug-in de provedor de credencial baseado em SAML incluído com um driver Amazon Redshift JDBC ou ODBC, você pode usar as configurações descritas anteriormente em Usar um plug-in de provedor de credenciais. Se `plugin_name` não for usado, as outras opções serão ignoradas.

O exemplo a seguir mostra o arquivo ~/.aws/credentials com dois perfis.

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

[user2]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
session_token=AQoDYXdzEPT//////////
wEXAMPLEtc764bNrC9SAPBSM22wDOk4x4HIZ8j4FZTwdQWLWsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTflfKD8YUuwthAx7
qkPpKPi/kMcGd
QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5VSXDvp75YU
9HFvlRd8Tx6q6fE8YQcHNVXAkiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fPOLn9FX9KSYvKTr4rvx3iSIlTJabIQwj2ICCR/oLxBA==
```

Para suar as credenciais do exemplo `user2`, especifique `Profile=user2` no URL de JDBC.

Para obter mais informações sobre o uso de perfis, consulte Configurações de arquivos de configuração e credenciais no Guia do usuário do AWS Command Line Interface.

Para obter mais informações sobre o uso de perfis para o driver JDBC, consulte Especificar perfis.

Para obter mais informações sobre o uso de perfis para o driver ODBC, consulte Configurar a autenticação.

Opções JDBC e ODBC para fornecer credenciais do IAM

A tabela a seguir lista as opções JDBC e ODBC para fornecimento de credenciais do IAM.

| Opção | Descrição |
| --- | --- |
| `Iam` | Para uso somente em uma string de conexão ODBC. Defina como 1 para usar a autenticação do IAM. |
| `AccessKeyID`<br><br>`SecretAccessKey`<br><br>`SessionToken` | O ID da chave de acesso e a chave de acesso secreta para o usuário ou perfil do IAM configurado para autenticação de banco de dados do IAM. O `SessionToken` é necessário somente para um perfil do IAM com credenciais temporárias. SessionToken não é usado para um usuário. Para obter mais informações, consulte Credenciais de segurança temporárias. |
| `plugin_name` | O nome totalmente qualificado de uma classe que implementa um provedor de credenciais. O driver JDBC do Amazon Redshift inclui plug-ins de provedor de credenciais baseados em SAML. Se você fornecer o `plugin_name`, também poderá fornecer outras opções relacionadas. Para obter mais informações, consulte Usar um plug-in de provedor de credenciais. |
| `Profile` | O nome de um perfil em um arquivo de credenciais da AWS ou configuração que contém valores para as opções de conexão JDBC. Para obter mais informações, consulte Uso de um perfil de configuração. |

Usar um plug-in de provedor de credenciais

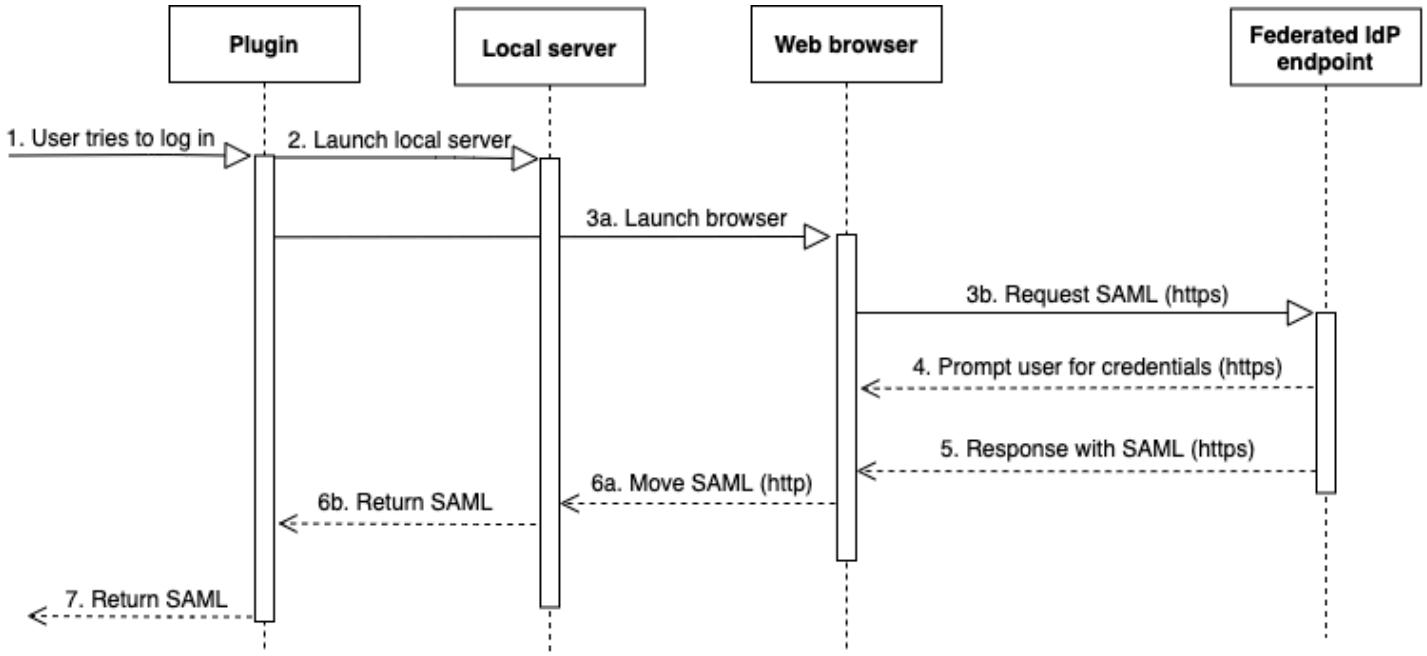
O Amazon Redshift usa plug-ins de provedor de credenciais para autenticação única.

Para comportar autenticação única, o Amazon Redshift fornece o plug-in do Azure AD para o Microsoft Azure Active Directory. Para obter informações sobre como configurar esse plugin, consulte Configurar a autenticação única de JDBC ou ODBC com o Microsoft Azure AD.

Configurar a autenticação multifator
Configurar a autenticação multifator

Para oferecer suporte à autenticação multifator (MFA), o Amazon Redshift fornece o plug-in do Azure AD para o Microsoft Azure Active Directory. Use o plug-in SAML do navegador para Okta, PingOne e o plug-in Azure AD do navegador para o Diretório Ativo do Microsoft Azure.

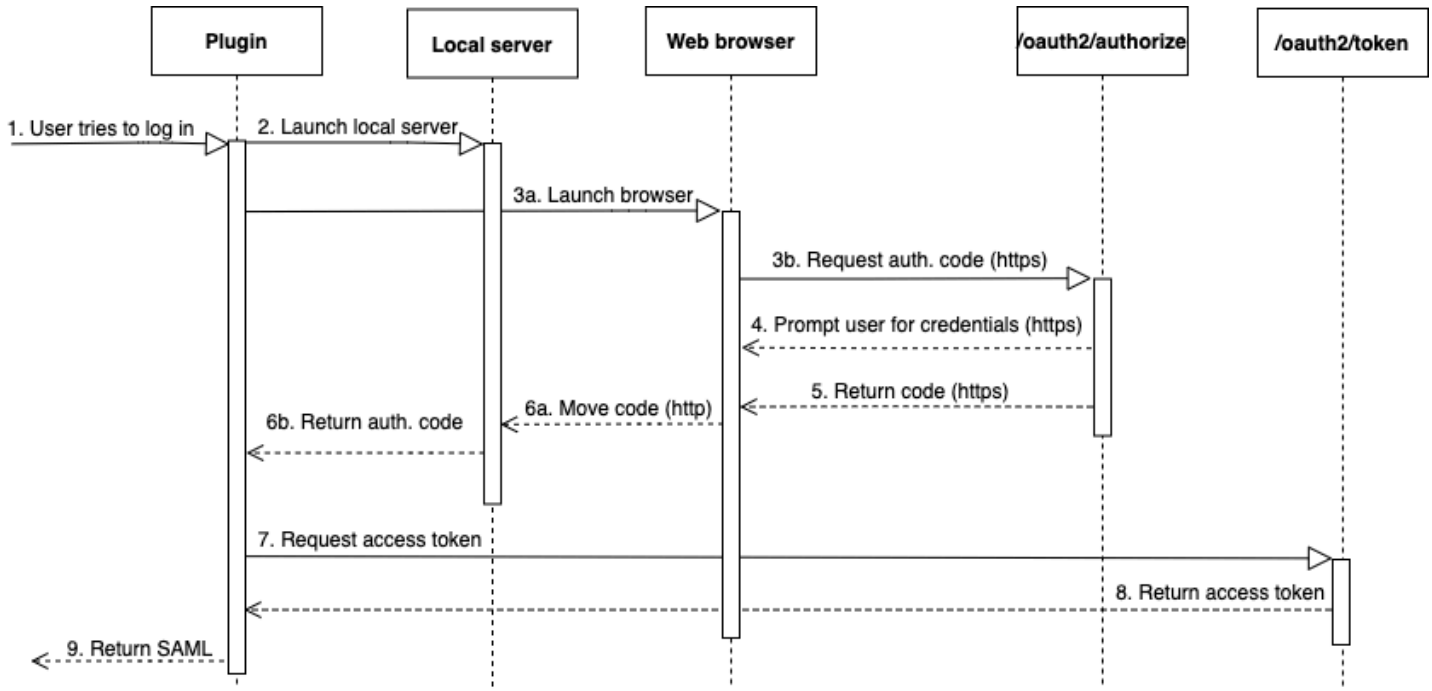
Com o plug-in de navegador de SAML, a autenticação de SAML flui assim:




1. Um usuário tenta fazer login.
2. O plug-in executa um servidor local para ouvir conexões de entrada no host local.
3. O plug-in inicia um navegador da web para solicitar uma resposta de SAML por HTTPS pelo endpoint do provedor de identidades federado do URL de login de autenticação única especificado.
4. O navegador da web segue o link e solicita que o usuário insira as credenciais.

5. Depois que o usuário autentica e concede consentimento, o endpoint do provedor de identidade federado retorna uma resposta de SAML por HTTPS para o URI indicado por `redirect_uri`.
6. O navegador da web move a mensagem de resposta com a resposta de SAML para o `redirect_uri` indicado.
7. O servidor local aceita a conexão de entrada e o plug-in recupera a resposta SAML e a passa para o Amazon Redshift.

Com o plug-in de navegador do Azure AD, a autenticação de SAML flui assim:




1. Um usuário tenta fazer login.
2. O plug-in executa um servidor local para ouvir conexões de entrada no host local.
3. O plug-in inicia um navegador da web para solicitar um código de autorização do endpoint `oauth2/authorize` do Azure AD.
4. O navegador da web segue o link gerado por HTTPS e solicita que o usuário insira as credenciais. O link é gerado com o uso de propriedades de configuração, como locatário e client_id.
5. Depois que o usuário autentica e concede consentimento, o endpoint `oauth2/authorize` do Azure AD retorna e envia uma resposta por HTTPS com o código de autorização para o `redirect_uri` indicado.
6. O navegador da web move a mensagem de resposta com a resposta de SAML para o `redirect_uri` indicado.

7. O servidor local aceita a conexão de entrada e as solicitações de plug-in e recupera o código de autorização e envia uma solicitação POST para o endpoint `oauth2/token` do Azure AD.
8. O endpoint `oauth2/token` do Azure AD retorna uma resposta com um token de acesso para o `redirect_uri` indicado.
9. O plug-in recupera a resposta SAML e a passa para o Amazon Redshift.

Consulte as seguintes seções:

- Active Directory Federation Services (AD FS)

  Para obter mais informações, consulte Configurar a autenticação única de JDBC ou ODBC com o AD FS.
- PingOne (Ping)

  O ping é compatível somente com o adaptador IdP predeterminado do PingOne usando a autenticação de formulários.

  Para obter mais informações, consulte Configurar a autenticação única de JDBC ou ODBC com o Ping Identity.
- Okta

  O Okta é compatível apenas com o aplicativo fornecido pelo Okta usado com o AWS Management Console.

  Para obter mais informações, consulte Configurar a autenticação única de JDBC ou ODBC com o Okta.
- Microsoft Azure Active Directory

  Para obter mais informações, consulte Configurar a autenticação única de JDBC ou ODBC com o Microsoft Azure AD.

### Configurar opções de plug-ins

Configurar opções de plug-ins

Para usar um plugin de provedor de credenciais baseado em SAML, especifique as seguintes opções em um perfil nomeado ou usando opções JBDC ou ODBC. Se `plugin_name` não for especificado, as outras opções serão ignoradas.

| Opção | Descrição |
| --- | --- |
| `plugin_name` | Para JDBC, o nome de classe que implementa um provedor de credenciais. Especifique um dos seguintes:<br>• Para o Active Directory Federation Services<br>`com.amazon.redshift.plugin.AdfsCredentialsProvider`<br>• Para o Okta<br>`com.amazon.redshift.plugin.OktaCredentialsProvider`<br>• Para o PingFederate<br>`com.amazon.redshift.plugin.PingCredentialsProvider`<br>• Para o Microsoft Azure Active Directory<br>`com.amazon.redshift.plugin.AzureCredentialsProvider`<br>• Para SAML MFA<br>`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`<br>• Para autenticação única do Microsoft Azure Active Directory com MFA<br>`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`<br>Para o ODBC, especifique um dos seguintes:<br>• Para o Active Directory Federation Services: `adfs`<br>• Para o Okta: `okta`<br>• Para o PingFederate: `ping`<br>• Para o Microsoft Azure Active Directory: `azure`<br>• Para SAML MFA: `browser saml` |

| Opção | Descrição |
| --- | --- |
| | • Para autenticação única do Microsoft Azure Active Directory com MFA: `browser azure ad` |
| `idp_host` | O nome do host corporativo do provedor de identidade. Este nome não deve conter barras (‘/’). Para um provedor de identidade Okta, o valor de `idp_host` deve terminar com `.okta.com` . |
| `idp_port` | A porta usada pelo provedor de identidade. O padrão é 443. Essa porta é ignorada para o Okta. |
| `preferred_role` | O nome do recurso da Amazon (ARN) da função nos elementos `AttributeValue` do atributo `Role` na declaração de SAML. Trabalhe com o administrador do IdP para localizar o valor apropriado da função preferencial. Para obter mais informações, consulte Configurar declarações de SAML para o IdP. |
| `user` | Um nome de usuário corporativo, incluindo domínio quando aplicável. Por exemplo, para o Active Directory, o nome de domínio precisa estar no formato domínio\nome de usuário. |
| password | A senha do usuário corporativo. É recomendável não usar esta opção. Em vez disso, use o cliente SQL para fornecer a senha. |
| `app_id` | O ID de um aplicativo do Okta. Usado somente com o Okta. O valor de `app_id` vem depois de `amazon_aws` no link de incorporação do aplicativo do Okta. Para obter esse valor, consulte o administrador do IdP. Este é um exemplo de um link de incorporação de aplicativo: `https://example.okta.com/home/amazon_aws/0oa2hylwrpM8UGehd1t7/272` |
| `idp_tenant` | Um locatário usado para o Azure AD. Usado apenas com o Azure. |
| `client_id` | Uma ID de cliente para a aplicação empresarial Amazon Redshift no Azure AD. Usado apenas com o Azure. |

### Configurar a autenticação única de JDBC ou ODBC com o Microsoft Azure AD

Você pode usar o Microsoft Azure AD como um provedor de identidade (IdP) para acessar seu cluster do Amazon Redshift. A seguir, encontra-se um procedimento que descreve como configurar uma relação de confiança para essa finalidade. Para obter mais informações sobre como configurar a AWS como um provedor de serviços para o IdP, consulte Configurar seu IdP SAML 2.0 com confiança de parte confiante e adicionar declarações no Guia do usuário do IAM.

> **Note**
>
> Para usar o Azure AD com JDBC, o driver Amazon Redshift JDBC deve ser a versão 1.2.37.1061 ou posterior. Para usar o Azure AD com ODBC, o driver ODBC do Amazon Redshift deve ser a versão 1.4.10.1000 ou posterior.

Assista ao vídeo a seguir para saber como federar o acesso do Amazon Redshift com o logon único do Microsoft Azure AD: Federar o acesso do Amazon Redshift com o logon único do Microsoft Azure AD.

Para configurar o Azure AD e sua conta da AWS para que confiem um no outro

1. Crie ou use um cluster existente do Amazon Redshift para os usuários do Azure AD se conectarem. Para configurar a conexão, certas propriedades deste cluster são necessárias, como o identificador de cluster. Para obter mais informações, consulte Criar um cluster.
2. Configure grupos e usuários do Diretório Ativo do Azure usados para a AWS no portal do Microsoft Azure.
3. Adicione o Amazon Redshift como uma aplicação empresarial no portal do Microsoft Azure para usar para logon único no AWS Console e logon federado no Amazon Redshift. Escolha Enterprise application (Aplicativo empresarial).
4. Escolha +New application (+Novo aplicativo). A página Adicionar um aplicativo é exibida.
5. Pesquise **`AWS`** no campo de pesquisa.
6. Escolha Amazon Web Services (AWS) e escolha Adicionar. Isso cria a aplicação da AWS.
7. Em Manage (Gerenciar), escolha Single sign-on (Logon único).
8. Escolha SAML. O Amazon Web Services (AWS) | A página de logon baseada em SAML é exibida.
9. Escolha Yes (Sim) para prosseguir para a página Configurar logon único com SAML. Esta página mostra a lista de atributos pré-configurados relacionados à autenticação única.

10. Em Basic SAML Configuration (Configuração básica de SAML), escolha o ícone de edição e Save (Salvar).
11. Quando você estiver configurando mais de um aplicativo, forneça um valor de identificador. Por exemplo, digite ***https://signin.aws.amazon.com/saml#2***. Observe que a partir do segundo aplicativo em diante, use esse formato com um sinal # para especificar um valor SPN exclusivo.
12. Na seção User Attributes and Claims (Atributos de usuário e reivindicações), escolha o ícone de edição.

    Por padrão, as reivindicações UID (Unique User Identifier), Role, RoleSessionName e SessionDuration são pré-configuradas.
13. Escolha + Add new claim (+ Adicionar nova reivindicação) para adicionar uma reivindicação aos usuários do banco de dados.

    Em Nome, digite **`DbUser`**.

    Em Namespace, insira **`https://redshift.amazon.com/SAML/Attributes`**.

    Em Origem, escolha Atributo.

    Em Source attribute (Atributo de origem), escolha user.userprincipalname. Selecione Salvar.
14. Escolha + Add new claim (+ Adicionar nova reivindicação) para adicionar uma reivindicação ao AutoCreate.

    Em Nome, digite **`AutoCreate`**.

    Em Namespace, insira **`https://redshift.amazon.com/SAML/Attributes`**.

    Em Origem, escolha Atributo.

    Em Source attribute (Atributo de origem), escolha "true". Selecione Salvar.

    Aqui, *`123456789012`* é a conta da AWS, *`AzureSSO`* é uma função do IAM que você criou e *`AzureADProvider`* é o provedor do IAM.

| Nome da reivindicação | Valor |
| --- | --- |
| Identificador de usuário exclusivo (ID de nome) | user.userprincipalname |
| https://aws.amazon.com/SAML/Attributes/SessionDuration | "900" |
| https://aws.amazon.com/SAML/Attributes/Role | arn:aws:iam::*123456789012* :role/*AzureSSO*,arn:aws:iam::*123456789012* :saml-provider/*AzureADProvider* |
| https://aws.amazon.com/SAML/Attributes/RoleSessionName | user.userprincipalname |
| https://redshift.amazon.com/SAML/Attributes/AutoCreate | "true" |
| https://redshift.amazon.com/SAML/Attributes/DbGroups | user.assignedroles |
| https://redshift.amazon.com/SAML/Attributes/DbUser | user.userprincipalname |

15. Em Registro de aplicativo > ***your-application-name*** > Autenticação, adicione Aplicativo móvel e desktop. Especifique o URL como http://localhost/redshift/.
16. Na seção SAML Signing Certificate (Certificado de assinatura SAML), escolha Download (Fazer download) para fazer download e salvar o arquivo XML de metadados de federação para usar ao criar um provedor de identidade SAML do IAM. Esse arquivo é usado para criar a identidade federada da autenticação única.
17. Crie um provedor de identidade SAML do IAM no console do IAM. O documento de metadados fornecido é o arquivo XML de metadados da federação que você salvou quando configurou o Azure Enterprise Application. Para obter etapas detalhadas, consulte Criar e gerenciar um provedor de identidade do IAM (console) no Manual do usuário do IAM.
18. Crie uma função do IAM para a federação do SAML 2.0 no console do IAM. Para obter etapas detalhadas, consulte Criar uma função para o SAML no Manual do usuário do IAM.

19. Crie uma política do IAM que você possa anexar à função do IAM criada para a federação do SAML 2.0 no console do IAM. Para obter etapas detalhadas, consulte Criar políticas do IAM (console) no Manual do usuário do IAM.

    Modifique a seguinte política (no formato JSON) para o seu ambiente:

    - Substitua a região da AWS do seu cluster por *us-west-1*.
    - Substitua a conta da AWS por *123456789012*.
    - Substitua seu identificador de cluster (ou * para todos os clusters) por *cluster-identifier*.
    - Substitua seu banco de dados (ou * para todos os bancos de dados) por *dev*.
    - Substitua o identificador exclusivo de sua função do IAM por *AROAJ2UCCR6DPCEXAMPLE*.
    - Substitua o domínio de e-mail do locatário ou da empresa por *example.com*.
    - Substitua o grupo de banco de dados ao qual você planeja atribuir o usuário por *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": "*"
        }
    ]
}
```

Esta política concede permissões da seguinte forma:

- A primeira seção concede permissão à operação de API do `GetClusterCredentials` para obter credenciais temporárias para o cluster especificado. Neste exemplo, o recurso é *`cluster-identifier`* com banco de dados *`dev`*, na conta *`123456789012`* e na região da AWS *`us-west-1`*. A cláusula `${redshift:DbUser}` permite que apenas os usuários que correspondam ao valor de `DbUser` especificado no Azure AD se conectem.
- A cláusula de condição impõe que apenas determinados usuários obtêm credenciais temporárias. Esses são os usuários da função especificada pelo ID exclusivo de função *`AROAJ2UCCR6DPCEXAMPLE`* na conta do IAM identificada por um endereço de e-mail no domínio de e-mail da empresa. Para obter mais informações sobre IDs exclusivos, consulte IDs exclusivos no Manual do usuário do IAM.

  Sua configuração com seu IdP (neste caso, Azure AD) determina como a cláusula de condição é gravada. Se o e-mail do seu funcionário for `johndoe@example.com`, primeiro defina `${redshift:DbUser}` para o campo super que corresponde ao nome de usuário do funcionário `johndoe`. Então, para fazer essa condição funcionar, defina o campo `RoleSessionName` do AWS SAML como o supercampo que corresponde ao e-mail do funcionário `johndoe@example.com`. Ao adotar essa abordagem, considere o seguinte:

  - Se você definir `${redshift:DbUser}` para ser o e-mail do funcionário, em seguida, remova o `@example.com` no JSON do exemplo para corresponder com o `RoleSessionName`.
  - Se você definir o `RoleSessionId` para ser apenas o nome de usuário do funcionário, remova o `@example.com` no exemplo para corresponder ao `RoleSessionName`.
  - No JSON de exemplo, tanto `${redshift:DbUser}` como `RoleSessionName` são definidos como o e-mail do funcionário. Este exemplo JSON usa o nome de usuário do banco de dados Amazon Redshift com `@example.com` para conectar o usuário para acessar o cluster.
- A segunda seção concede permissão para criar um nome `dbuser` no cluster especificado. Neste JSON de exemplo, ele restringe a criação de `${redshift:DbUser}`.
- A terceira seção concede permissão para especificar a qual `dbgroup` um usuário pode ingressar. Neste JSON de exemplo, um usuário pode ingressar no grupo `my_dbgroup` no cluster especificado.
- A quarta seção concede permissão para ações que o usuário pode fazer em todos os recursos. Neste JSON de exemplo, ele permite que os usuários chamem `redshift:DescribeClusters` para obter informações do cluster, como o endpoint do cluster, região da AWS e porta. Também permite que os usuários chamem `iam:ListRoles` para verificar quais funções um usuário pode assumir.

Como configurar o JDBC para autenticação no Microsoft Azure AD

- Configure seu cliente de banco de dados para se conectar ao cluster por meio do JDBC usando o logon único do Azure AD.

  Você pode usar qualquer cliente que use um driver JDBC para se conectar usando o logon único do Azure AD ou usar uma linguagem, como Java, para se conectar usando um script. Para obter informações sobre instalação e configuração, consulte Configurar uma conexão para o driver JDBC versão 2.1 para o Amazon Redshift.

  Por exemplo, você pode usar SQLWorkbench/J como o cliente. Ao configurar o SQLWorkbench/j, a URL do seu banco de dados usa o seguinte formato.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Se você usar o SQLWorkbench/j como o cliente, execute as seguintes etapas:

a. Inicie o SQL Workbench/J. Na página Selecionar perfil de conexão adicione um Grupo de perfis chamado **`AzureAuth`**.

b. Em Connection Profile (Perfil de conexão), insira **`Azure`**.

c. Escolha Manage Drivers (Gerenciar drivers) e escolha Amazon Redshift. Escolha o ícone Open Folder (Abrir pasta) ao lado de Library (Biblioteca), e escolha o arquivo.jar JDBC apropriado.

d. Na página Select Connection Profile (Selecionar perfil de conexão), adicione informações ao perfil de conexão da seguinte maneira:

- Em User (Usuário), insira seu nome de usuário do Microsoft Azure. Este é o nome de usuário da conta do Microsoft Azure que você está usando para o logon único que tem permissão para o cluster que você está tentando autenticar.
- Em Password (Senha), digite sua senha do Microsoft Azure.
- Em Drivers, escolha Amazon Redshift (com.amazon.redshift.jdbc.Driver).
- Para URL, insira **`jdbc:redshift:iam://`*`your-cluster-identifier`*`:`*`your-cluster-region`*`/`*`your-database-name`*.

e. Escolha Extended Properties (Propriedades estendidas) para adicionar informações adicionais às propriedades de conexão, conforme descrito a seguir.

Para a configuração de autenticação única do Azure AD, adicione outras informações da seguinte forma:

- Para plugin_name, insira **`com.amazon.redshift.plugin.AzureCredentialsProvider`**. Esse valor especifica para o driver usar o logon único do Azure AD como o método de autenticação.
- Para idp_tenant, insira ***`your-idp-tenant`***. Usado apenas para o Microsoft Azure AD. Este é o nome do locatário da sua empresa configurado no Azure AD. Esse valor pode ser o nome do locatário ou o ID exclusivo do locatário com hífens.
- Para client_secret, insira ***`your-azure-redshift-application-client-secret`***. Usado apenas para o Microsoft Azure AD. Este é o segredo do seu cliente da aplicação Amazon Redshift que você criou ao definir a configuração do Azure Single Sign-On. Isso só é aplicável ao plug-in com.amazon.redshift.plugin.AzureCredentialsProvider.
- Para client_id, insira ***`your-azure-redshift-application-client-id`***. Usado apenas para o Microsoft Azure AD. Esta é a ID do cliente (com hifens) da aplicação Amazon Redshift que você criou ao definir sua configuração do Azure Single Sign-On.

Para a configuração de autenticação única do Azure AD com MFA, adicione outras informações às propriedades de conexão da seguinte forma:

- Para plugin_name, insira **`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`**. Isso especifica para o driver usar o método de autenticação única do Azure com MFA.
- Para idp_tenant, insira ***`your-idp-tenant`***. Usado apenas para o Microsoft Azure AD. Este é o nome do locatário da sua empresa configurado no Azure AD. Esse valor pode ser o nome do locatário ou o ID exclusivo do locatário com hífens.
- Para client_id, insira ***`your-azure-redshift-application-client-id`***. Essa opção é usada apenas para o Microsoft Azure AD. Este é o ID do cliente (com hifens) da aplicação Amazon Redshift que você criou ao definir a configuração de autenticação única do Azure com MFA.
- Em listen_port, insira ***`your-listen-port`***. Esta é a porta que o servidor local está escutando. O padrão é 7890.
- Em idp_response_timeout, insira ***`the-number-of-seconds`***. Este é o número de segundos a aguardar antes do tempo limite quando o servidor IdP envia de volta uma resposta. O número mínimo de segundos deve ser 10. Se o tempo para estabelecer a conexão for maior do que esse limite, a conexão é cancelada.

Como configurar o ODBC para autenticação no Microsoft Azure AD

- Configure seu cliente de banco de dados para se conectar ao cluster por meio de ODBC usando seu logon único do Azure AD.

  O Amazon Redshift fornece drivers ODBC para sistemas operacionais Linux, Windows e macOS. Antes de instalar um driver de ODBC, será necessário determinar se a ferramenta do cliente SQL é de 32 ou 64 bits. Instale o driver de ODBC que corresponde aos requisitos da ferramenta de cliente SQL.

  Além disso, instale e configure o driver ODBC Amazon Redshift mais recente para o seu sistema operacional da seguinte maneira:

  - No Windows, consulte Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows.

- Para macOS, consulte Instalar o driver ODBC do Amazon Redshift no macOS X.
- Para Linux, consulte Instalar o driver ODBC do Amazon Redshift no Linux.

No Windows, na página Amazon Redshift ODBC Driver DSN Setup (Configuração do DSN do driver ODBC do Amazon Redshift), em Connection Settings (Configurações de conexão), insira as seguintes informações:

- Para Data Source Name (Nome da fonte de dados), insira ***your-DSN***. Isto especifica o nome da fonte de dados usado como o nome do perfil de ODBC.
- Em Auth type (Tipo de autenticação) para a configuração de autenticação única do Azure AD, escolha **`Identity Provider: Azure AD`**. Este é o método de autenticação que o driver de ODBC usa para autenticar usando o logon único do Azure.
- Em Auth type (Tipo de autenticação) para a configuração de autenticação única do Azure AD com MFA, escolha **`Identity Provider: Browser Azure AD`**. Este é o método de autenticação que o driver de ODBC usa para autenticar usando o logon único do Azure com MFA.
- Para Cluster ID (ID do cluster), insira ***your-cluster-identifier***.
- Para Region (Região), insira ***your-cluster-region***.
- Para Database (Banco de dados), insira ***your-database-name***.
- Em User (Usuário), insira ***your-azure-username***. Este é o nome de usuário da conta do Microsoft Azure que está sendo usada para logon único que tem permissão para o cluster que você está tentando autenticar. Use isso somente quando Auth Type (Tipo de autenticação) for Identity Provider: Azure AD (Provedor de identidade: Azure AD).
- Em Password (Senha), insira ***your-azure-password***. Use isso somente quando Auth Type (Tipo de autenticação) for Identity Provider: Azure AD (Provedor de identidade: Azure AD).
- Para IdP Tenant (Locatário IdP), insira ***your-idp-tenant***. Este é o nome do locatário da sua empresa configurado no seu IdP (Azure). Esse valor pode ser o nome do locatário ou o ID exclusivo do locatário com hífens.
- Para Azure Client Secret (Segredo do cliente do Azure), insira ***your-azure-redshift-application-client-secret***. Este é o segredo do cliente da aplicação Amazon Redshift que você criou ao definir sua configuração de logon único do Azure.
- Para Azure Client ID (ID do cliente do Azure), insira ***your-azure-redshift-application-client-id***. Este é o ID do cliente (com hífens) da aplicação Amazon Redshift que você criou ao definir sua configuração do Azure Single Sign-On.

- Em Porta de escuta, insira ***your-listen-port***. Esta é a porta de escuta padrão que o servidor local está escutando. O padrão é 7890. Isso se aplica somente ao plug-in do Browser Azure AD.
- Em Response Timeout (Tempo limite de resposta), insira ***the-number-of-seconds***. Este é o número de segundos a aguardar antes do tempo limite quando o servidor IdP envia de volta uma resposta. O número mínimo de segundos deve ser 10. Se o tempo para estabelecer a conexão for maior do que esse limite, a conexão é cancelada. Esta opção se aplica apenas ao plug-in do Azure AD do navegador.

No macOS e no Linux, edite o arquivo `odbc.ini` da seguinte forma:

> **Note**
>
> Nenhuma entrada diferencia letras maiúsculas de minúsculas.

- Para clusterid, insira ***your-cluster-identifier***. Esse é o nome do cluster criado pelo Amazon Redshift.
- Para region (região), insira ***your-cluster-region***. Esta é a Região da AWS do cluster do Amazon Redshift criado.
- Para database (banco de dados), insira ***your-database-name***. Este é o nome do banco de dados que você está tentando acessar no cluster do Amazon Redshift.
- Para locale (localidade), insira **`en-us`**. Este é o idioma em que as mensagens de erro são exibidas.
- Para IAM, insira **`1`**. Esse valor especifica ao driver para autenticar usando credenciais do IAM.
- Em plugin_name para a configuração de autenticação única do Azure AD, insira **`AzureAD`**. Isso especifica ao driver para usar o Azure Single Sign-On como o método de autenticação.
- Em plugin_name para a configuração de autenticação única do Azure AD com MFA, insira **`BrowserAzureAD`**. Isso especifica para o driver usar o logon único do Azure com MFA como o método de autenticação.
- Em uid, insira ***your-azure-username***. Este é o nome de usuário da conta do Microsoft Azure que você está usando para logon único, que tem permissão para o cluster que você está tentando autenticar. Use isso somente quando plugin_name for AzureAD.

- Em pwd, insira ***your-azure-password***. Use isso somente quando plugin_name for AzureAD.
- Para idp_tenant, insira ***your-idp-tenant***. Este é o nome do locatário da sua empresa configurado no seu IdP (Azure). Esse valor pode ser o nome do locatário ou o ID exclusivo do locatário com hífens.
- Para client_secret, insira ***your-azure-redshift-application-client-secret***. Este é o segredo do cliente da aplicação Amazon Redshift que você criou ao definir sua configuração de logon único do Azure.
- Para client_id, insira ***your-azure-redshift-application-client-id***. Este é o ID do cliente (com hífens) da aplicação Amazon Redshift que você criou ao definir sua configuração do Azure Single Sign-On.
- Em listen_port, insira ***your-listen-port***. Esta é a porta que o servidor local está escutando. O padrão é 7890. Isso se aplica ao plug-in do Browser Azure AD.
- Em idp_response_timeout, insira ***the-number-of-seconds***. Este é o período especificado em segundos para aguardar a resposta do Azure. Esta opção se aplica ao plug-in do Azure AD do navegador.

No macOS e no Linux, edite também as configurações de perfil para adicionar as exportações a seguir.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Como solucionar problemas com o plug-in Browser Azure AD

1. Para usar o plug-in Browser Azure AD, você deve definir o URL de resposta especificado na solicitação para corresponder ao URL de resposta configurado para seu aplicativo.

   Navegue até a página Configurar o logon único com SAML no portal do Microsoft Azure. Verifique se o URL de resposta está definido como http://localhost/redshift/.
2. Se você receber um erro de locatário IdP, verifique se o nome do Locatário IdP corresponde ao nome de domínio usado inicialmente para configurar o Active Directory no Microsoft Azure.

No Windows, navegue até a seção Configurações de conexão da página Configuração do DSN do driver ODBC do Amazon Redshift. Verifique se o nome do locatário da empresa configurada no seu IdP (Azure) corresponde ao nome de domínio usado inicialmente para configurar o Active Directory no Microsoft Azure.

No macOS e no Linux, localize o arquivo odbc.ini. Verifique se o nome do locatário da empresa configurada no seu IdP (Azure) corresponde ao nome de domínio usado inicialmente para configurar o Active Directory no Microsoft Azure.

3. Se você receber um erro informando que o URL de resposta especificado na solicitação não corresponde aos URLs de resposta configurados para seu aplicativo, verifique se os URIs de redirecionamento são os mesmos que o URL de resposta.

   Navegue até a página de Registro de aplicativo do seu aplicativo no portal do Microsoft Azure. Verifique se os URIs de redirecionamento correspondem ao URL de resposta.

4. Se receber a resposta inesperada: erro não autorizado, verifique se você concluiu a configuração de Aplicativos móveis e de desktop.

   Navegue até a página de Registro de aplicativo do seu aplicativo no portal do Microsoft Azure. Navegue até Autenticação e verifique se você configurou Aplicativos móveis e de desktop para usar http://localhost/redshift/ como URIs de redirecionamento.

### Configurar a autenticação única de JDBC ou ODBC com o AD FS

É possível usar o AD FS como um provedor de identidade (IdP) para acessar seu cluster do Amazon Redshift. A seguir, encontra-se um procedimento que descreve como configurar uma relação de confiança para essa finalidade. Para obter mais informações sobre como configurar a AWS como um provedor de serviços para AD FS, consulte Configurar seu IdP SAML 2.0 com confiança de parte confiante e adicionar declarações no Manual do usuário do IAM.

Para configurar o AD FS e sua conta da AWS para que confiem um no outro

1. Crie ou use um cluster existente do Amazon Redshift para os usuários do AD FS se conectarem. Para configurar a conexão, certas propriedades deste cluster são necessárias, como o identificador de cluster. Para obter mais informações, consulte Criar um cluster.
2. Configure o AD FS para controlar o acesso do Amazon Redshift no console de gerenciamento Microsoft:

1. Escolha ADFS 2.0 e Add Relying Party Trust (Adicionar confiança da parte dependente). Na página Add Relying Party Trust Wizard (Assistente para adicionar confiança da parte dependente) escolha Start (Iniciar).
2. Na página Select Data Source (Selecionar fonte de dados), escolha Import data about the relying party published online or on a local network (Importar dados sobre a parte dependente publicados online ou em uma rede local).
3. Em Federation metadata address (host name or URL) (Endereço de metadados de federação [nome do host ou URL]), insira **`https://signin.aws.amazon.com/saml-metadata.xml`**. O arquivo XML de metadados é um documento de metadados SAML padrão que descreve a AWS como uma parte confiável.
4. Na página Specify Display Name (Especificar nome de exibição), insira um valor para Display name (Nome de exibição).
5. Na página Choose Issuance Authorization Rules (Escolher regras de autorização de emissão), escolha uma regra de autorização de emissão para permitir ou negar que todos os usuários acessem essa parte dependente.
6. Na página Ready to Add Trust (Pronto para adicionar confiança) revise as configurações.
7. Na página Finish (Concluir), escolha Open the Edit Claim Rules dialog for this relying party trust when the wizard closes (Abrir a caixa de diálogo Editar regras de reivindicação para esta parte dependente quando o assistente for encerrado).
8. No menu de contexto (clique com o botão direito do mouse), escolha Relying Party Trusts (Confianças de parte dependente).
9. Para sua parte dependente, abra o menu de contexto (clique com o botão direito do mouse) e escolha Edit Claim Rules (Editar regras de reivindicação). Na página Edit Claim Rules (Editar regras de reivindicação), escolha Add Rule (Adicionar regra).
10. Em Claim rule template (Modelo de regra de reivindicação), escolha Transform an Incoming Claim (Transformar uma reivindicação de entrada) e na página Edit Rule – NameId (Editar regra – NameId), faça o seguinte:
    - Em Claim rule name (Nome da regra de reivindicação), insira NameId.
    - Em Incoming claim name (Nome da reivindicação de entrada), escolha Windows Account Name (Nome da conta do Windows).
    - Em Outgoing claim name (Nome da reivindicação de saída), escolha Name ID (ID do nome).

- Em Outgoing name ID format (Formato de ID de nome de saída), escolha Persistent Identifier (Identificador persistente).
- Escolha Pass through all claim values (Transmitir todos os valores de reivindicação).

11. Na página Edit Claim Rules (Editar regras de reivindicação), escolha Add Rule (Adicionar regra). Na página Select Rule Template (Selecionar modelo de regra), em Claim rule template (Modelo de regra de reivindicação), escolha Send LDAP Attributes as Claims (Enviar atributos LDAP como reivindicações).
12. Na página Configure Rule (Configurar regra), faça o seguinte:
    - Em Claim rule name (Nome da regra de reivindicação), insira RoleSessionName.
    - Em Attribute store (Armazenamento de atributos), escolha Active Directory.
    - Em LDAP Attribute (Atributo LDAP), escolha Email Addresses (Endereços de e-mail).
    - Para o Tipo de declaração de saída, escolha https://aws.amazon.com/SAML/Attributes/RoleSessionName.
13. Na página Edit Claim Rules (Editar regras de reivindicação), escolha Add Rule (Adicionar regra). Na página Select Rule Template (Selecionar modelo de regra), em Claim rule template (Modelo de regra de reivindicação), escolha Send Claims Using a Custom Rule (Enviar reivindicações usando uma regra personalizada).
14. Na página Edit Rule – Get AD Groups (Editar regra – Obter grupos do AD), em Claim rule name (Nome da regra de reivindicação), insira Get AD Groups (Obter grupos do AD).
15. Em Custom rule (Regra personalizada), insira o seguinte.

```
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. Na página Edit Claim Rules (Editar regras de reivindicação), escolha Add Rule (Adicionar regra). Na página Select Rule Template (Selecionar modelo de regra), em Claim rule template (Modelo de regra de reivindicação), escolha Send Claims Using a Custom Rule (Enviar reivindicações usando uma regra personalizada).
17. Na página Edit Rule – Roles (Editar regra – Funções), em Claim rule name (Nome da regra de reivindicação), digite Roles (Funções).

18 Em Custom rule (Regra personalizada), insira o seguinte.

```
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-"));
```

Observe os ARNs do provedor SAML e a função a ser assumida. Neste exemplo, `arn:aws:iam:123456789012:saml-provider/ADFS` é o ARN do provedor SAML e `arn:aws:iam:123456789012:role/ADFS-` é o ARN da função.

3. Certifique-se de que você fez download do arquivo `federationmetadata.xml`. Verifique se o conteúdo do documento não tem caracteres inválidos. Este é o arquivo de metadados que você usa ao configurar a relação de confiança com a AWS.
4. Crie um provedor de identidade SAML do IAM no console do IAM. O documento de metadados fornecido é o arquivo XML de metadados da federação que você salvou quando configurou o Azure Enterprise Application. Para obter etapas detalhadas, consulte Criar e gerenciar um provedor de identidade do IAM (console) no Manual do usuário do IAM.
5. Crie uma função do IAM para a federação do SAML 2.0 no console do IAM. Para obter etapas detalhadas, consulte Criar uma função para o SAML no Manual do usuário do IAM.
6. Crie uma política do IAM que você possa anexar à função do IAM criada para a federação do SAML 2.0 no console do IAM. Para obter etapas detalhadas, consulte Criar políticas do IAM (console) no Manual do usuário do IAM. Para obter um exemplo do Azure AD, consulte Configurar a autenticação única de JDBC ou ODBC com o Microsoft Azure AD.

Como configurar o JDBC para autenticação no AD FS

- Configure seu cliente de banco de dados para se conectar ao cluster por meio do JDBC usando a autenticação única do Azure FS.

  Você pode utilizar qualquer cliente que use um driver JDBC para se conectar usando a autenticação única do AD FS ou usar uma linguagem, como Java, para se conectar por meio de um script. Para obter informações sobre instalação e configuração, consulte Configurar uma conexão para o driver JDBC versão 2.1 para o Amazon Redshift.

  Por exemplo, você pode usar SQLWorkbench/J como o cliente. Ao configurar o SQLWorkbench/j, a URL do seu banco de dados usa o seguinte formato.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Se você usar o SQLWorkbench/j como o cliente, execute as seguintes etapas:

a. Inicie o SQL Workbench/J. Na página Selecionar perfil de conexão, adicione um Grupo de perfis, por exemplo, **ADFS**.

b. Em Connection Profile (Perfil de conexão), insira o nome do perfil de conexão, por exemplo, **ADFS**.

c. Escolha Manage Drivers (Gerenciar drivers) e escolha Amazon Redshift. Escolha o ícone Open Folder (Abrir pasta) ao lado de Library (Biblioteca), e escolha o arquivo.jar JDBC apropriado.

d. Na página Select Connection Profile (Selecionar perfil de conexão), adicione informações ao perfil de conexão da seguinte maneira:

   - Em User (Usuário), insira o nome de usuário do AD FS. Este é o nome de usuário da conta do usado para o logon único que tem permissão para o cluster que você está tentando autenticar.
   - Em Password (Senha), insira a senha do AD FS.
   - Em Drivers, escolha Amazon Redshift (com.amazon.redshift.jdbc.Driver).
   - Para URL, insira **jdbc:redshift:iam://*your-cluster-identifier*:*your-cluster-region*/*your-database-name***.

e. Escolha Propriedades estendidas. Para plugin_name, insira **com.amazon.redshift.plugin.AdfsCredentialsProvider**. Esse valor especifica para o driver usar o método de autenticação única do AD FS.

Como configurar o ODBC para autenticação no AD FS

- Configure seu cliente de banco de dados para se conectar ao cluster por meio de ODBC usando a autenticação única do AD FS.

  O Amazon Redshift fornece drivers ODBC para sistemas operacionais Linux, Windows e macOS. Antes de instalar um driver de ODBC, será necessário determinar se a ferramenta do cliente SQL é de 32 ou 64 bits. Instale o driver de ODBC que corresponde aos requisitos da ferramenta de cliente SQL.

Além disso, instale e configure o driver ODBC Amazon Redshift mais recente para o seu sistema operacional da seguinte maneira:

- No Windows, consulte Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows.
- Para macOS, consulte Instalar o driver ODBC do Amazon Redshift no macOS X.
- Para Linux, consulte Instalar o driver ODBC do Amazon Redshift no Linux.

No Windows, na página Amazon Redshift ODBC Driver DSN Setup (Configuração do DSN do driver ODBC do Amazon Redshift), em Connection Settings (Configurações de conexão), insira as seguintes informações:

- Para Data Source Name (Nome da fonte de dados), insira ***your-DSN***. Isto especifica o nome da fonte de dados usado como o nome do perfil de ODBC.
- Para o Tipo de autenticação, escolha Provedor de identidade: SAML. Esse é o método que o driver de ODBC usa para autenticar por meio da autenticação única do AD FS.
- Para Cluster ID (ID do cluster), insira ***your-cluster-identifier***.
- Para Region (Região), insira ***your-cluster-region***.
- Para Database (Banco de dados), insira ***your-database-name***.
- Em User (Usuário), insira ***your-adfs-username***. Esse é o nome de usuário da conta do AD FS que está sendo usado para autenticação única que tem permissão para o cluster que você está tentando autenticar. Use isso somente quando Auth type (Tipo de autenticação) for Identity Provider: SAML (Provedor de identidade: SAML).
- Em Password (Senha), insira ***your-adfs-password***. Use isso somente quando Auth type (Tipo de autenticação) for Identity Provider: SAML (Provedor de identidade: SAML).

No macOS e no Linux, edite o arquivo `odbc.ini` da seguinte forma:

> **Note**
>
> Nenhuma entrada diferencia letras maiúsculas de minúsculas.

- Para clusterid, insira ***your-cluster-identifier***. Esse é o nome do cluster criado pelo Amazon Redshift.
- Para region (região), insira ***your-cluster-region***. Esta é a Região da AWS do cluster do Amazon Redshift criado.
- Para database (banco de dados), insira ***your-database-name***. Este é o nome do banco de dados que você está tentando acessar no cluster do Amazon Redshift.
- Para locale (localidade), insira **en-us**. Este é o idioma em que as mensagens de erro são exibidas.
- Para IAM, insira **1**. Esse valor especifica ao driver para autenticar usando credenciais do IAM.
- Em plugin_name, siga um destes procedimentos:
  - Na configuração de autenticação única do AD FS com MFA, digite **BrowserSAML**. Este é o método de autenticação que o driver ODBC usa para autenticar no AD FS.
  - Na configuração de autenticação única do AD FS, digite **ADFS**. Esse é o método que o driver de ODBC usa para autenticar por meio da autenticação única do Azure AD.
- Em uid, insira ***your-adfs-username***. Esse é o nome de usuário da conta do Microsoft Azure que está sendo usado para autenticação única que tem permissão para o cluster que você está tentando autenticar. Use isso somente quando plugin_name for ADFS.
- Em pwd, insira ***your-adfs-password***. Use isso somente quando plugin_name for ADFS.

No macOS e no Linux, edite também as configurações de perfil para adicionar as exportações a seguir.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Configurar a autenticação única de JDBC ou ODBC com o Ping Identity

É possível usar o Ping Identity como um provedor de identidade (IdP) para acessar seu cluster do Amazon Redshift. A seguir, você encontrará um procedimento que descreve como configurar uma relação de confiança para essa finalidade usando o portal PingOne. Para obter mais informações sobre como configurar a AWS como um provedor de serviços para Ping Identity, consulte

Configurando seu IdP SAML 2.0 com confiança da parte confiável e adicionar declarações no Manual do usuário do IAM.

Para configurar o Ping Identity e sua conta da AWS para que confiem uma na outra

1. Crie ou use um cluster existente do Amazon Redshift para que seus usuários de Ping Identity se conectem. Para configurar a conexão, certas propriedades deste cluster são necessárias, como o identificador de cluster. Para obter mais informações, consulte Criar um cluster.
2. Adicione o Amazon Redshift como uma nova aplicação SAML no portal PingOne. Para obter etapas detalhadas, consulte a documentação do Ping Identity.
    1. Acesse My Applications (Meus aplicativos).
    2. Em Add Application (Adicionar aplicativo), escolha New SAML Application (Novo aplicativo SAML).
    3. Em Application Name (Nome do aplicativo), insira **`Amazon Redshift`**.
    4. Em Protocol Version (Versão do protocolo), escolha SAML v2.0.
    5. Em Category (Categoria), escolha ***`your-application-category`***.
    6. Em Assertion Consumer Service (ACS), digite ***`your-redshift-local-host-url`***. Este é o host local e a porta para a qual a declaração de SAML redireciona.
    7. Em Entity ID (ID da entidade), insira `urn:amazon:webservices`.
    8. Em Signing (Assinar), escolha Sign Assertion (Assinar declaração).
    9. Na seção SSO Attribute Mapping (Mapeamento de atributo de SSO), crie as reivindicações conforme mostrado na tabela a seguir.

| Atributo do aplicativo | Atributo de ligação de identidade de valor literal |
| --- | --- |
| https://aws.amazon.com/SAML/Attributes/Role | arn:aws:iam::*123456789012* :role/*Ping*,arn:aws:iam::*123456789012* :saml-provider/*PingProvider* |
| https://aws.amazon.com/SAML/Attributes/RoleSessionName | email |
| https://redshift.amazon.com/SAML/Attributes/AutoCreate | "true" |

| Atributo do aplicativo | Atributo de ligação de identidade de valor literal |
| --- | --- |
| https://redshift.amazon.com/SAML/Attributes/DbUser | email |
| https://redshift.amazon.com/SAML/Attributes/DbGroups | Os grupos nos atributos “DbGroups” contêm o prefixo @directory. Para remover isso, em Ponte de identidade, insira memberOf. Em Função, escolha ExtractByRegularExpression. Em Expressão, insira (.*)[\@](?:.*). |

3. Em Group Access (Acesso de grupo), configure o seguinte acesso de grupo, se necessário:
   - 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. Revise sua configuração e faça alterações, se necessário.
5. Use o Initiate Single Sign-On (SSO) URL (URL de logon único inicial [SSO]) como o URL de login para o plug-in de Browser SAML.
6. Crie um provedor de identidade SAML do IAM no console do IAM. O documento de metadados fornecido é o arquivo XML de metadados da federação que você salvou quando configurou o Ping Identity. Para obter etapas detalhadas, consulte Criar e gerenciar um provedor de identidade do IAM (console) no Manual do usuário do IAM.
7. Crie uma função do IAM para a federação do SAML 2.0 no console do IAM. Para obter etapas detalhadas, consulte Criar uma função para o SAML no Manual do usuário do IAM.
8. Crie uma política do IAM que você possa anexar à função do IAM criada para a federação do SAML 2.0 no console do IAM. Para obter etapas detalhadas, consulte Criar políticas do IAM (console) no Manual do usuário do IAM. Para obter um exemplo do Azure AD, consulte Configurar a autenticação única de JDBC ou ODBC com o Microsoft Azure AD.

Como configurar o JDBC para autenticação para o Ping Identity

- Configure seu cliente de banco de dados para se conectar ao cluster por meio do JDBC usando a autenticação única do Ping Identity.

  Você pode usar qualquer cliente que utilize um driver JDBC para se conectar por meio da autenticação única do Ping Identity ou usar uma linguagem, como Java, para se conectar por meio de um script. Para obter informações sobre instalação e configuração, consulte Configurar uma conexão para o driver JDBC versão 2.1 para o Amazon Redshift.

  Por exemplo, você pode usar SQLWorkbench/J como o cliente. Ao configurar o SQLWorkbench/j, a URL do seu banco de dados usa o seguinte formato.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Se você usar o SQLWorkbench/j como o cliente, execute as seguintes etapas:

  a. Inicie o SQL Workbench/J. Na página Selecionar perfil de conexão, adicione um Grupo de perfis, por exemplo, **`Ping`**.

  b. Em Connection Profile (Perfil de conexão), insira ***`your-connection-profile-name`***, por exemplo, **`Ping`**.

  c. Escolha Manage Drivers (Gerenciar drivers) e escolha Amazon Redshift. Escolha o ícone Open Folder (Abrir pasta) ao lado de Library (Biblioteca), e escolha o arquivo.jar JDBC apropriado.

  d. Na página Select Connection Profile (Selecionar perfil de conexão), adicione informações ao perfil de conexão da seguinte maneira:

     - Em User (Usuário), insira seu nome do usuário do PingOne. Esse é o nome de usuário da conta do PingOne usado para o logon único que tem permissão para o cluster que você está tentando autenticar.
     - Em Password (Senha), insira sua senha do PingOne.
     - Em Drivers, escolha Amazon Redshift (com.amazon.redshift.jdbc.Driver).
     - Para URL, insira **`jdbc:redshift:iam://`*`your-cluster-identifier`*`:`*`your-cluster-region`*`/`*`your-database-name`***.

  e. Escolha Extended Properties (Propriedades estendidas) e siga um destes procedimentos:

- Em login_url, insira ***your-ping-sso-login-url***. Esse valor especifica ao URL para usar autenticação única para login.
- Para o Ping Identity, em plugin_name, insira **com.amazon.redshift.plugin.PingCredentialsProvider**. Esse valor especifica ao driver para usar a autenticação única do Ping Identity como método.
- Para o Ping Identity com autenticação única, em plugin_name, insira **com.amazon.redshift.plugin.BrowserSamlCredentialsProvider**. Esse valor especifica ao driver para usar a autenticação única do PingOne do Ping Identity como método.

Como configurar o ODBC para autenticação para o Ping Identity

- Configure o cliente de banco de dados para se conectar ao cluster por meio do ODBC usando a autenticação única do PingOne do Ping Identity.

  O Amazon Redshift fornece drivers ODBC para sistemas operacionais Linux, Windows e macOS. Antes de instalar um driver de ODBC, será necessário determinar se a ferramenta do cliente SQL é de 32 ou 64 bits. Instale o driver de ODBC que corresponde aos requisitos da ferramenta de cliente SQL.

  Além disso, instale e configure o driver ODBC Amazon Redshift mais recente para o seu sistema operacional da seguinte maneira:

  - No Windows, consulte Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows.
  - Para macOS, consulte Instalar o driver ODBC do Amazon Redshift no macOS X.
  - Para Linux, consulte Instalar o driver ODBC do Amazon Redshift no Linux.

  No Windows, na página Amazon Redshift ODBC Driver DSN Setup (Configuração do DSN do driver ODBC do Amazon Redshift), em Connection Settings (Configurações de conexão), insira as seguintes informações:

  - Para Data Source Name (Nome da fonte de dados), insira ***your-DSN***. Isto especifica o nome da fonte de dados usado como o nome do perfil de ODBC.
  - Em Auth type (Tipo de autenticação), siga um destes procedimentos:

  - Para a configuração do Ping Identity, escolha Provedor de identidade: Ping Federate. Esse é o método que o driver de ODBC usa para autenticar por meio da autenticação única do Ping Identity.
  - Para a configuração do Ping Identity com autenticação única, escolha Identity Provider: Browser SAML (Provedor de identidades: navegador SAML). Esse é o método que o driver de ODBC usa para autenticar por meio do Ping Identity com autenticação única.
- Para Cluster ID (ID do cluster), insira ***your-cluster-identifier***.
- Para Region (Região), insira ***your-cluster-region***.
- Para Database (Banco de dados), insira ***your-database-name***.
- Em User (Usuário), insira ***your-ping-username***. Esse é o nome de usuário da conta do PingOne usado para autenticação única que tem permissão para o cluster que você está tentando autenticar. Use isso somente quando Auth type (Tipo de autenticação) for Identity Provider: PingFederate (Provedor de identidade: PingFederate).
- Em Password (Senha), insira ***your-ping-password***. Use isso somente quando Auth type (Tipo de autenticação) for Identity Provider: PingFederate (Provedor de identidade: PingFederate).
- Em Porta de escuta, insira ***your-listen-port***. Esta é a porta que o servidor local está escutando. O padrão é 7890. Isso se aplica somente ao plug-in de Browser SAML.
- Em Response Timeout (Tempo limite de resposta), insira ***the-number-of-seconds***. Este é o número de segundos a aguardar antes do tempo limite quando o servidor IdP envia de volta uma resposta. O número mínimo de segundos deve ser 10. Se o tempo para estabelecer a conexão for maior do que esse limite, a conexão é cancelada. Isso se aplica somente ao plug-in de Browser SAML.
- Em Login URL (URL de login), insira ***your-login-url***. Isso se aplica somente ao plug-in de Browser SAML.

No macOS e no Linux, edite o arquivo `odbc.ini` da seguinte forma:

> **Note**
>
> Nenhuma entrada diferencia letras maiúsculas de minúsculas.

- Para clusterid, insira ***your-cluster-identifier***. Esse é o nome do cluster criado pelo Amazon Redshift.
- Para region (região), insira ***your-cluster-region***. Esta é a Região da AWS do cluster do Amazon Redshift criado.
- Para database (banco de dados), insira ***your-database-name***. Este é o nome do banco de dados que você está tentando acessar no cluster do Amazon Redshift.
- Para locale (localidade), insira **en-us**. Este é o idioma em que as mensagens de erro são exibidas.
- Para IAM, insira **1**. Esse valor especifica ao driver para autenticar usando credenciais do IAM.
- Em plugin_name, siga um destes procedimentos:
  - Para a configuração do Ping Identity, insira **BrowserSAML**. Este é o método de autenticação que o driver de ODBC usa para se autenticar no Ping Identity.
  - Na configuração do Ping Identity com autenticação única, digite **Ping**. Esse é o método que o driver de ODBC usa para autenticar por meio do Ping Identity com autenticação única.
- Em uid, insira ***your-ping-username***. Este é o nome de usuário da conta do Microsoft Azure que você está usando para logon único, que tem permissão para o cluster que você está tentando autenticar. Use isso somente quando plugin_name for Ping.
- Em pwd, insira ***your-ping-password***. Use isso somente quando plugin_name for Ping.
- Em login_url, insira ***your-login-url***. Esse é o URL de autenticação única inicial que retorna a resposta de SAML. Isso se aplica somente ao plug-in de Browser SAML.
- Em idp_response_timeout, insira ***the-number-of-seconds***. Esse é o período especificado em segundos para aguardar a resposta do PingOne Identity. Isso se aplica somente ao plug-in de Browser SAML.
- Em listen_port, insira ***your-listen-port***. Esta é a porta que o servidor local está escutando. O padrão é 7890. Isso se aplica somente ao plug-in de Browser SAML.

No macOS e no Linux, edite também as configurações de perfil para adicionar as exportações a seguir.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

### Configurar a autenticação única de JDBC ou ODBC com o Okta

É possível usar o Okta como um provedor de identidade (IdP) para acessar seu cluster do Amazon Redshift. A seguir, encontra-se um procedimento que descreve como configurar uma relação de confiança para essa finalidade. Para obter mais informações sobre como configurar a AWS como um provedor de serviços para Okta, consulte Configurar seu IdP SAML 2.0 com confiança de parte confiante e adicionar declarações no Manual do usuário do IAM.

Para configurar o Okta e sua conta da AWS para que confiem um no outro

1. Crie ou use um cluster existente do Amazon Redshift para os usuários do Okta se conectarem. Para configurar a conexão, certas propriedades deste cluster são necessárias, como o identificador de cluster. Para obter mais informações, consulte Criar um cluster.
2. Adicione o Amazon Redshift como uma nova aplicação no portal Okta. Para obter etapas detalhadas, consulte a Documentação do Okta.
   - Escolha Add Application (Adicionar aplicativo).
   - Em Add Application (Adicionar aplicativo), escolha Create New App (Criar novo aplicativo).
   - Na página Create a New Add Application Integration (Criar uma nova integração de aplicativos de adição), em Platform (Plataforma), escolha Web.
   - Em Sign on method (Método de logon), escolha SAML v2.0.
   - Na página General Settings (Configurações gerais), em App name (Nome do aplicativo), insira ***your-redshift-saml-sso-name***. Esse é o nome do seu aplicativo.
   - Na página Configurações de SAML, em URL de logon único, insira ***your-redshift-local-host-url***. Este é o host local e a porta para os quais a declaração de SAML redireciona, por exemplo `http://localhost:7890/redshift/`.
3. Use o valor URL de logon único como o URL do destinatário e o URL de destino.
4. Em Signing (Assinar), escolha Sign Assertion (Assinar declaração).
5. Para URI de público (ID da entidade SP), insira **`urn:amazon:webservices`** para as declarações, conforme mostrado na tabela a seguir.
6. Na seção Advanced Settings (Configurações avançadas), em SAML Issuer ID (ID do emissor SAML), insira ***your-Identity-Provider-Issuer-ID***, que você encontra na seção View Setup Instructions (Visualizar instruções de configuração).
7. Na seção Attribute Statements (Declarações de atributo), crie as reivindicações conforme mostrado na tabela a seguir.

| Nome da reivindicação | Valor |
| --- | --- |
| https://aws.amazon.com/SAML/Attributes/Role | arn:aws:iam::*123456789012* :role/*Okta*,arn:aws:iam::*123456789012* :saml-provider/*Okta* |
| https://aws.amazon.com/SAML/Attributes/RoleSessionName | user.email |
| https://redshift.amazon.com/SAML/Attributes/AutoCreate | "true" |
| https://redshift.amazon.com/SAML/Attributes/DbUser | user.email |

8. Na seção App Embed Link (Link de incorporação de aplicativo) localize o URL que você pode usar como o URL de login do plug-in SAML do navegador.
9. Crie um provedor de identidade SAML do IAM no console do IAM. O documento de metadados fornecido é o arquivo XML de metadados da federação que você salvou quando configurou o Okta. Para obter etapas detalhadas, consulte Criar e gerenciar um provedor de identidade do IAM (console) no Manual do usuário do IAM.
10. Crie uma função do IAM para a federação do SAML 2.0 no console do IAM. Para obter etapas detalhadas, consulte Criar uma função para o SAML no Manual do usuário do IAM.
11. Crie uma política do IAM que você possa anexar à função do IAM criada para a federação do SAML 2.0 no console do IAM. Para obter etapas detalhadas, consulte Criar políticas do IAM (console) no Manual do usuário do IAM. Para obter um exemplo do Azure AD, consulte Configurar a autenticação única de JDBC ou ODBC com o Microsoft Azure AD.

Como configurar o JDBC para autenticação no Okta

- Configure seu cliente de banco de dados para se conectar ao cluster por meio do JDBC usando a autenticação única do Okta.

  Você pode usar qualquer cliente que utilize um driver JDBC para se conectar por meio da autenticação única do Okta ou usar uma linguagem, como Java, para se conectar por meio de

um script. Para obter informações sobre instalação e configuração, consulte Configurar uma conexão para o driver JDBC versão 2.1 para o Amazon Redshift.

Por exemplo, você pode usar SQLWorkbench/J como o cliente. Ao configurar o SQLWorkbench/j, a URL do seu banco de dados usa o seguinte formato.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Se você usar o SQLWorkbench/j como o cliente, execute as seguintes etapas:

a. Inicie o SQL Workbench/J. Na página Selecionar perfil de conexão, adicione um Grupo de perfis, por exemplo, **`Okta`**.

b. Em Connection Profile (Perfil de conexão), insira ***`your-connection-profile-name`***, por exemplo, **`Okta`**.

c. Escolha Manage Drivers (Gerenciar drivers) e escolha Amazon Redshift. Escolha o ícone Open Folder (Abrir pasta) ao lado de Library (Biblioteca), e escolha o arquivo.jar JDBC apropriado.

d. Na página Select Connection Profile (Selecionar perfil de conexão), adicione informações ao perfil de conexão da seguinte maneira:

   - Em User (Usuário), insira o nome de usuário do Okta. Este é o nome de usuário da conta do Okta que está sendo usado para o logon único que tem permissão para o cluster que você está tentando autenticar.
   - Em Password (Senha), insira sua senha do Okta.
   - Em Drivers, escolha Amazon Redshift (com.amazon.redshift.jdbc.Driver).
   - Para URL, insira **`jdbc:redshift:iam://`*`your-cluster-identifier`*`:`*`your-cluster-region`*`/`*`your-database-name`***.

e. Escolha Extended Properties (Propriedades estendidas) e siga um destes procedimentos:

   - Em login_url, insira ***`your-okta-sso-login-url`***. Esse valor especifica ao URL para usar autenticação única para login no Okta.
   - Para autenticação única do Okta, em plugin_name, insira **`com.amazon.redshift.plugin.OktaCredentialsProvider`**. Esse valor especifica ao driver para usar a autenticação única do Okta como método.

- Para autenticação única do Okta com MFA, em plugin_name, insira **`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`**. Isso especifica para o driver usar o método de autenticação única do Okta com MFA.

Como configurar o ODBC para autenticação no Okta

- Configure seu cliente de banco de dados para se conectar ao cluster por meio do ODBC usando a autenticação única do Okta.

  O Amazon Redshift fornece drivers ODBC para sistemas operacionais Linux, Windows e macOS. Antes de instalar um driver de ODBC, será necessário determinar se a ferramenta do cliente SQL é de 32 ou 64 bits. Instale o driver de ODBC que corresponde aos requisitos da ferramenta de cliente SQL.

  Além disso, instale e configure o driver ODBC Amazon Redshift mais recente para o seu sistema operacional da seguinte maneira:

  - No Windows, consulte Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows.
  - Para macOS, consulte Instalar o driver ODBC do Amazon Redshift no macOS X.
  - Para Linux, consulte Instalar o driver ODBC do Amazon Redshift no Linux.

  No Windows, na página Amazon Redshift ODBC Driver DSN Setup (Configuração do DSN do driver ODBC do Amazon Redshift), em Connection Settings (Configurações de conexão), insira as seguintes informações:

  - Para Data Source Name (Nome da fonte de dados), insira ***`your-DSN`***. Isto especifica o nome da fonte de dados usado como o nome do perfil de ODBC.
  - Em Auth type (Tipo de autenticação), siga um destes procedimentos:
    - Para a configuração de autenticação única do Okta, escolha **`Identity Provider: Okta`**. Esse é o método que o driver de ODBC usa para autenticar por meio da autenticação única do Okta.
    - Para a configuração de autenticação única do Okta com MFA, escolha **`Identity Provider: Browser SAML`**. Esse é o método que o driver de ODBC usa para autenticar por meio da autenticação única do Okta com MFA.
  - Para Cluster ID (ID do cluster), insira ***`your-cluster-identifier`***.

- Para Region (Região), insira ***your-cluster-region***.
- Para Database (Banco de dados), insira ***your-database-name***.
- Em User (Usuário), insira ***your-okta-username***. Esse é o nome de usuário da conta do Okta usado para autenticação única que tem permissão para o cluster que você está tentando autenticar. Use isso somente quando Auth type (Tipo de autenticação) for Identity Provider: Okta (Provedor de identidade: Okta).
- Em Password (Senha), insira ***your-okta-password***. Use isso somente quando Auth type (Tipo de autenticação) for Identity Provider: Okta (Provedor de identidade: Okta).

No macOS e no Linux, edite o arquivo `odbc.ini` da seguinte forma:

> **Note**
>
> Nenhuma entrada diferencia letras maiúsculas de minúsculas.

- Para clusterid, insira ***your-cluster-identifier***. Esse é o nome do cluster criado pelo Amazon Redshift.
- Para region (região), insira ***your-cluster-region***. Esta é a Região da AWS do cluster do Amazon Redshift criado.
- Para database (banco de dados), insira ***your-database-name***. Este é o nome do banco de dados que você está tentando acessar no cluster do Amazon Redshift.
- Para locale (localidade), insira **`en-us`**. Este é o idioma em que as mensagens de erro são exibidas.
- Para IAM, insira **`1`**. Esse valor especifica ao driver para autenticar usando credenciais do IAM.
- Em plugin_name, siga um destes procedimentos:
  - Na configuração de autenticação única do Okta com MFA, digite **`BrowserSAML`**. Esse é o método que o driver de ODBC usa para autenticar por meio da autenticação única do Okta com MFA.
  - Na configuração de autenticação única do Okta, digite **`Okta`**. Esse é o método que o driver de ODBC usa para autenticar por meio da autenticação única do Okta.
- Em uid, insira ***your-okta-username***. Esse é o nome de usuário da conta do Okta usado para autenticação única que tem permissão para o cluster no qual você está tentando autenticar. Use isso somente quando plugin_name for Okta.

- Em pwd, insira ***your-okta-password***. Use isso somente quando plugin_name for Okta.
- Em login_url, insira ***your-login-url***. Esse é o URL de autenticação única inicial que retorna a resposta de SAML. Isso se aplica somente ao plug-in de Browser SAML.
- Em idp_response_timeout, insira ***the-number-of-seconds***. Esse é o período especificado em segundos para aguardar a resposta do PingOne. Isso se aplica somente ao plug-in de Browser SAML.
- Em listen_port, insira ***your-listen-port***. Esta é a porta que o servidor local está escutando. O padrão é 7890. Isso se aplica somente ao plug-in de Browser SAML.

No macOS e no Linux, edite também as configurações de perfil para adicionar as exportações a seguir.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Opções JDBC e ODBC para criar credenciais de usuário de banco de dados

Para usar o driver Amazon Redshift JDBC ou ODBC para criar credenciais de usuário do banco de dados, forneça o nome do usuário do banco de dados como uma opção JDBC ou ODBC. Opcional, o driver poderá criar um novo usuário de banco de dados, caso não exista um, e você poderá especificar uma lista de grupos de usuários de banco de dados aos quais o usuário se associará no login.

Se você usa um provedor de identidade (IdP), trabalhe com o administrador do IdP para determinar os valores corretos dessas opções. O administrador do IdP também pode configurar o IdP para fornecer essas opções; nesse caso, você não precisa fornecer as opções como JDBC ou ODBC. Para obter mais informações, consulte Configurar declarações de SAML para o IdP.

> **Note**
>
> Se você usar uma variável de política do IAM `${redshift:DbUser}`, conforme descrito em Políticas de recursos de GetClusterCredentials, o valor para `DbUser` será substituído pelo valor recuperado pelo contexto da solicitação da operação de API. Os drivers do Amazon Redshift usam o valor da variável `DbUser` fornecida pelo URL de conexão, em vez do valor fornecido como um atributo SAML.

Para ajudar a proteger essa configuração, recomendamos que você use uma condição em uma política do IAM para validar o valor `DbUser` com o `RoleSessionName`. Você pode encontrar exemplos de como definir uma condição usando uma política do IAM em Política de exemplo para usar GetClusterCredentials.

A tabela a seguir lista as opções de criação de credenciais de usuário de banco de dados.

| Opção | Descrição |
| --- | --- |
| DbUser | O nome de um usuário do banco de dados. Se houver um usuário chamado DbUser no banco de dados, as credenciais temporárias do usuário terão as mesmas permissões que o usuário existente. Se DbUser não existir no banco de dados e AutoCreate for definido como true, um novo usuário DbUser será criado. Se desejar, desabilite a senha de um usuário existente. Para obter mais informações, consulte ALTER_USER |
| AutoCreate | Especifique `true` para criar um usuário de banco de dados com o nome especificado como DbUser, caso ainda não exista um. O padrão é falso. |
| `DbGroups` | Uma lista delimitada por vírgulas dos nomes de um ou mais grupos de bancos de dados existentes que o usuário do banco de dados une para a sessão atual. Por padrão, o novo usuário é adicionado somente a PUBLIC. |

Gerar as credenciais de banco de dados para uma identidade do IAM usando a CLI ou a API do Amazon Redshift

Para gerar de modo programático as credenciais temporárias de usuário de banco de dados, o Amazon Redshift fornece o comando get-cluster-credentials para a operação de API AWS Command Line Interface (AWS CLI) e GetClusterCredentials. Ou você pode configurar seu cliente SQL com drivers JDBC ou ODBC do Amazon Redshift que gerenciam o processo de chamada da operação `GetClusterCredentials`, recuperando as credenciais do usuário do banco de dados e estabelecendo uma conexão entre seu cliente SQL e seu banco de dados Amazon Redshift. Para obter mais informações, consulte Opções JDBC e ODBC para criar credenciais de usuário de banco de dados.

> **Note**
>
> Recomendamos usar os drivers JDBC ou ODBC do Amazon Redshift para gerar credenciais de usuário de banco de dados.

Nesta seção, você encontrará etapas que permitirão chamar a operação `GetClusterCredentials` ou o comando get-cluster-credentials de modo programático, recuperar credenciais de usuário de banco de dados e conectar-se ao banco de dados.

Para gerar e usar credenciais de banco de dados temporárias

1. Crie ou modifique um usuário ou um perfil com as permissões necessárias. Para obter mais informações sobre as permissões do IAM, consulte Para criar um perfil do IAM com permissões para chamar GetClusterCredentials.
2. Como um usuário ou um perfil do IAM que você autorizou na etapa anterior, execute o comando da CLI get-cluster-credentials ou chame a operação de API `GetClusterCredentials` e forneça os seguintes valores:
   - Identificador de cluster – O nome do cluster que contém o banco de dados.
   - Nome do usuário do banco de dados – O nome de um usuário de banco de dados novo ou existente.
     - Se o usuário não existir no banco de dados e AutoCreate for definido como true, um novo usuário será criado com PASSWORD desabilitado.
     - Se o usuário não existir e AutoCreate for false, a solicitação apresentará falha.
     - Neste exemplo, o nome de usuário de banco de dados é `temp_creds_user`.
   - Autocriar – (Opcional) Crie um novo usuário se o nome de usuário do banco de dados não existir.
   - Nome do banco de dados – (opcional) O nome do banco de dados no qual o usuário está autorizado a fazer logon. Se o nome do banco de dados não for especificado, o usuário poderá fazer logon em qualquer banco de dados de cluster.
   - Grupos de banco de dados – (opcional) Uma lista de grupos de usuários de banco de dados existentes. Após login bem-sucedido, o usuário do banco de dados será adicionado aos grupos de usuários especificados. Se nenhum grupo for especificado, o usuário somente terá permissões de PUBLIC. Os nomes de grupos de usuários devem corresponder aos ARNs de recursos dbgroup especificados na política do IAM anexada ao usuário ou perfil.

- Tempo de expiração – (Opcional) O tempo, em segundos, até que as credenciais temporárias expirem. Você pode especificar um valor entre 900 segundos (15 minutos) e 3600 segundos (60 minutos). O padrão é 900 segundos.

3. O Amazon Redshift verifica se o usuário tem permissão para chamar a operação `GetClusterCredentials` com os recursos especificados.
4. O Amazon Redshift retorna uma senha temporária e o nome de usuário do banco de dados.

   O exemplo a seguir usa o Amazon Redshift CLI para gerar credenciais de banco de dados temporárias para um usuário existente denominado `temp_creds_user`.

```
aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
 temp_creds_user --db-name exampledb --duration-seconds 3600
```

   O resultado é conforme se segue.

```
{
  "DbUser": "IAM:temp_creds_user",
  "Expiration": "2016-12-08T21:12:53Z",
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpDHwXVPyJYBDm/
gqX2Eeaq6P3DgTzgPg=="
}
```

   O exemplo a seguir usa o Amazon Redshift CLI com autocreate para gerar credenciais de banco de dados temporárias para um novo usuário e adicionar o usuário ao grupo `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
```

   O resultado é conforme se segue.

```
{
  "DbUser": "IAMA:temp_creds_user:example_group",
  "Expiration": "2016-12-08T21:12:53Z",
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpDHwXVPyJYBDm/
gqX2Eeaq6P3DgTzgPg=="
}
```

5. Estabeleça uma conexão de autenticação Secure Socket Layer (SSL) com o cluster Amazon Redshift e envie uma solicitação de login com o nome de usuário e a senha da resposta `GetClusterCredentials`. Inclua o prefixo `IAM:` ou `IAMA:` com o nome de usuário; por exemplo, `IAM:temp_creds_user` ou `IAMA:temp_creds_user`.

   > **Important**
   >
   > Configure o cliente SQL para exigir o SSL. Caso contrário, se o cliente SQL tentar se conectar automaticamente com o SSL, ele poderá retornar a não SSL se houver qualquer tipo de falha. Nesse caso, a primeira tentativa de conexão poderá falhar porque as credenciais estão expiradas ou são inválidas e, depois, a segunda tentativa de conexão falhará porque a conexão não é SSL. Se isso ocorrer, pode ser que a primeira mensagem não apareça. Para obter mais informações sobre como se conectar ao cluster usando o SSL, consulte Configurar as opções de segurança para conexões.

6. Se a conexão não usar SSL, a tentativa de conexão apresentará falha.
7. O cluster envia uma solicitação `authentication` ao cliente SQL.
8. Em seguida, o cliente SQL envia uma senha temporária ao cluster.
9. Se a senha for válida e não tiver expirado, o cluster concluirá a conexão.

## Autorizar o Amazon Redshift a acessar outros serviços da AWS em seu nome

Alguns recursos do Amazon Redshift exigem que o Amazon Redshift acesse outros serviços da AWS em seu nome. Por exemplo, os comandos COPY e UNLOAD podem carregar ou descarregar dados em seu cluster Amazon Redshift usando um bucket do Amazon S3. O comando CREATE EXTERNAL FUNCTION pode invocar uma função do AWS Lambda usando uma função Lambda definida pelo usuário (UDF) escalar. O Amazon Redshift Spectrum pode usar um catálogo de dados no Amazon Athena ou no AWS Glue. Para que seus clusters Amazon Redshift atuem em seu nome, você fornece credenciais de segurança para seus clusters. O método preferido para fornecer credenciais de segurança é especificar uma função do AWS Identity and Access Management (IAM). Para COPY e UNLOAD, é possível fornecer as credenciais temporárias.

Os usuários precisam de acesso programático se quiserem interagir com a AWS de fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando a AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| Identificação da força de trabalho<br><br>(Usuários gerenciados no Centro de Identidade do IAM) | Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções da interface que deseja utilizar.<br><br>• Para a AWS CLI, consulte Configuração da AWS CLI para usar o AWS IAM Identity Center no AWS Command Line Interface Guia do usuário da .<br>• Para os SDKs da AWS, ferramentas e APIs da AWS, consulte Autenticação do Centro de Identidade do IAM no Guia de referência de ferramentas e SDKs da AWS. |
| IAM | Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções em Como usar credenciais temporárias com recursos da AWS no Guia do usuário do IAM. |
| IAM | (Não recomendado)<br>Use credenciais de longo prazo para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções da interface que deseja utilizar.<br><br>• Para a AWS CLI, consulte Autenticação usando as credenciais de usuário do IAM no Guia do usuário da AWS Command Line Interface. |

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| | | • Para as ferramentas e SDKs da AWS, consulte Autenticação usando as credenciais de longo prazo no Guia de referência de ferramentas e SDKs da AWS.<br>• Para as APIs da AWS, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM. |

Em seguida, descubra como criar uma função do IAM com as permissões apropriadas para acessar outros serviços da AWS. Você também precisa associar a função ao seu cluster e especificar o nome do recurso da Amazon (ARN) da função ao executar o comando Amazon Redshift. Para ter mais informações, consulte Autorizar operações COPY, UNLOAD, CREATE EXTERNAL FUNCTION e CREATE EXTERNAL SCHEMA usando funções do IAM.

Além disso, um superusuário pode conceder o privilégio ASSUMEROLE a usuários e grupos específicos para fornecer acesso a uma função para operações COPY e UNLOAD. Para obter informações, consulte GRANT no Guia do desenvolvedor de banco de dados do Amazon Redshift.

## Criar uma função do IAM para permitir que o cluster do Amazon Redshift acesse serviços da AWS

Para criar uma função IAM para permitir que seu cluster do Amazon Redshift se comunique com outros serviços da AWS em seu nome, execute as seguintes etapas. Os valores usados nesta seção são exemplos, você pode escolher valores com base em suas necessidades.

Para criar uma função do IAM para permitir que o Amazon Redshift acesse os serviços da AWS

1. Abra o console do IAM.
2. No painel de navegação, escolha Roles.

3. Escolha Criar Perfil.
4. Escolha serviço da AWS e clique em Redshift.
5. Em Select your use case, escolha Redshift - Customizable e clique em Next: Permissions. A página Attach permissions policy é exibida.
6. Para acesso ao Amazon S3 usando COPY, como exemplo, use **`AmazonS3ReadOnlyAccess`** anexe. Para acesso ao Amazon S3 usando COPY ou UNLOAD, sugerimos que você crie políticas gerenciadas que restrinjam o acesso ao bucket desejado e ao prefixo adequadamente. Para operações de leitura e gravação, recomendamos aplicar os privilégios mínimos e restringir apenas os buckets do Amazon S3 e prefixos chave necessários para o Amazon Redshift.

   Para acessar as funções do Lambda para o comando CREATE EXTERNAL FUNCTION, adicione **`AWSLambdaRole`**.

   Para o Redshift Spectrum, além do acesso ao Amazon S3, adicione **`AWSGlueConsoleFullAccess`** ou **`AmazonAthenaFullAccess`**.

   Escolha Próximo: etiquetas.
7. A página Adicionar tags é exibida. Opcionalmente, é possível adicionar tags. Selecione Next: Review (Próximo: revisar).
8. Para Role Name, digite um nome para sua função, por exemplo, **`RedshiftCopyUnload`**. Selecione Criar função.
9. A nova função está disponível para todos os usuários em clusters que usam a função. Para restringir acesso somente a usuários específicos em clusters específicos ou, a clusters em regiões específicas, edite a relação de confiança da função. Para ter mais informações, consulte Restringir acesso a funções do IAM.
10. Associe a função ao cluster. Você pode associar uma função do IAM a um cluster ao criar o cluster, ou adicionar a função a um cluster existente. Para ter mais informações, consulte Associar funções do IAM a clusters.

> **Note**
>
> Para restringir o acesso a dados específicos, use uma função do IAM que conceda o mínimo de privilégios necessários.

## Restringir acesso a funções do IAM

Por padrão, as funções de IAM que estão disponíveis para um cluster do Amazon Redshift estão disponíveis para todos os usuários desse cluster. Você pode optar por restringir as funções do IAM a usuários específicos do banco de dados do Amazon Redshift em clusters específicos ou a regiões específicas.

Para permitir que somente usuários de banco de dados específicos usem uma função do IAM, siga as etapas a seguir.

Para identificar usuários de banco de dados específicos com acesso a uma função do IAM

1. Identifique o nome do recurso da Amazon (ARN) para os usuários do banco de dados em seu cluster do Amazon Redshift. O ARN de um usuário de banco de dados está no formato: `arn:aws:redshift:`*`region`*`:`*`account-id`*`:dbuser:`*`cluster-name`*`/`*`user-name`*.

   Para o Amazon Redshift sem servidor, use o formato ARN a seguir. `arn:aws:redshift:`*`region`*`:`*`account-id`*`:dbuser:`*`workgroup-name`*`/`*`user-name`*
2. Abra o console do IAM.
3. No painel de navegação, escolha Perfis.
4. Escolha a função do IAM que você deseja restringir a usuários específicos do banco de dados do Amazon Redshift.
5. Escolha a guia Trust Relationships e Edit Trust Relationship. Uma nova função do IAM que permite ao Amazon Redshift acessar outros serviços da AWS em seu nome tem uma relação de confiança da seguinte maneira:

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

6. Adicione uma condição à seção da ação `sts:AssumeRole` da relação de confiança que limite o campo `sts:ExternalId` a valores especificados por você. Inclua um ARN para cada usuário do banco de dados para quem você deseja dar acesso à função. O ID externo pode ser qualquer string exclusiva.

   Por exemplo, a relação de confiança a seguir especifica que somente os usuários do banco de dados `user1` e `user2` no cluster `my-cluster` na região `us-west-2` têm permissão para usar essa função do IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "redshift.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": [
          "arn:aws:redshift:us-west-2:123456789012:dbuser:my-cluster/user1",
          "arn:aws:redshift:us-west-2:123456789012:dbuser:my-cluster/user2"
        ]
      }
    }
  }]
}
```

7. Escolha Update Trust Policy.

## Restringir uma função do IAM a uma região da AWS

Você pode restringir uma função do IAM para ser acessível somente em uma determinada região da AWS. Por padrão, as funções do IAM do Amazon Redshift não estão restritas a uma única região.

Para restringir o uso de uma função do IAM por região, siga estas etapas.

Para identificar regiões permitidas para uma função do IAM

1. Abra o Console do IAM em https://console.aws.amazon.com/.

2. No painel de navegação, escolha Perfis.
3. Escolha a função que você deseja modificar com regiões específicas.
4. Escolha a guia Trust Relationships e Edit Trust Relationship. Uma nova função do IAM que permite ao Amazon Redshift acessar outros serviços da AWS em seu nome tem uma relação de confiança da seguinte maneira:

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

5. Modifique a lista `Service` do `Principal` com a lista das regiões específicas para as quais você deseja permitir o uso da função. Cada região na lista `Service` deve estar no seguinte formato: `redshift.`*`region`*`.amazonaws.com`.

   Por exemplo, a relação de confiança editada permite o uso da função do IAM somente nas regiões `us-east-1` e `us-west-2`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.us-east-1.amazonaws.com",
          "redshift.us-west-2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. Escolher Update Trust Policy

## Encadeando funções do IAM no Amazon Redshift

Ao anexar uma função ao cluster, o cluster pode assumir essa função para acessar o Amazon S3, o Amazon Athena, o AWS Glue, e o AWS Lambda em seu nome. Se uma função anexada ao cluster não tiver acesso aos recursos necessários, você poderá encadear outra função, possivelmente pertencente a outra conta. O cluster assumirá a função encadeada temporariamente para acessar os dados. Você também pode conceder acesso entre contas com o encadeamento de funções. Cada função em cadeia assume a próxima função na cadeia, até que o cluster assuma a função no final da cadeia. O número máximo de funções do IAM que você pode associar está sujeito a uma cota. Para obter mais informações, consulte a cota "Funções do IAM de cluster para o Amazon Redshift acessar outros serviços da AWS" no Cotas para objetos do Amazon Redshift.

Por exemplo, suponha que a Empresa A deseja acessar dados em um bucket do Amazon S3 que pertence à Empresa B. A Empresa A cria uma função de serviço da AWS para o Amazon Redshift nomeada `RoleA` e o anexa ao seu cluster. A empresa B cria uma função chamada `RoleB` que é autorizada a acessar os dados no bucket da empresa B. Para acessar os dados no bucket da empresa B, a empresa A executa um comando COPY usando um parâmetro `iam_role` que encadeia `RoleA` e `RoleB`. Durante a operação COPY, `RoleA` assume temporariamente `RoleB` para acessar o bucket do Amazon S3.

Para encadear funções, você estabelece uma relação de confiança entre as funções. Uma função que assume uma outra função (por exemplo, `RoleA`) precisa ter uma política de permissões que conceda a ela a permissão para assumir a função da próxima função encadeada (por exemplo, `RoleB`). Por sua vez, a função que passa a permissão (`RoleB`) precisa ter uma política de confiança que permita que ela passe suas permissões para a função encadeada anterior (`RoleA`). Para obter mais informações, consulte Usar funções de IAM no Manual do usuário do IAM.

A primeira função na cadeia deve ser uma função anexada ao cluster. A primeira função, e cada função subsequente que assume a próxima função na cadeia, deve ter uma política que inclua uma declaração específica. Essa declaração tem o efeito de `Allow` na ação `sts:AssumeRole` e no nome de recurso da Amazon (ARN) da próxima função em um elemento `Resource`. Em nosso exemplo, `RoleA` tem a seguinte política de permissão que permite assumir `RoleB`, propriedade da conta da AWS `210987654321`.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "Stmt1487639602000",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::210987654321:role/RoleB"
       }
    ]
}
```

Uma função que passa para outra função deve estabelecer uma relação de confiança com a função que assume a função ou com a conta da AWS que possui a função. No exemplo, `RoleB` tem a seguinte política de confiança para estabelecer uma relação de confiança com a função `RoleA`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::role/RoleA"
      }
    }
  ]
}
```

A seguinte política de confiança estabelece uma relação de confiança com o proprietário da `RoleA`, conta da AWS `123456789012`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
```

```
  ]
}
```

> **Note**
>
> Para restringir a autorização de encadeamento de funções a usuários específicos, defina uma condição. Para ter mais informações, consulte Restringir acesso a funções do IAM.

Ao executar um comando UNLOAD, COPY, CREATE EXTERNAL FUNCTION ou CREATE EXTERNAL SCHEMA, você encadeia funções incluindo uma lista separada por vírgulas de ARNs de função no parâmetro`iam_role`. O exemplo a seguir mostra a sintaxe do encadeamento de funções no parâmetro `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**
>
> A cadeia de funções inteira é colocada entre aspas simples e não deve conter espaços.

Nos exemplos a seguir, `RoleA` é anexada ao cluster que pertence à conta da AWS `123456789012`. `RoleB`, que pertence à conta `210987654321`, tem permissão para acessar o bucket denominado `s3://companyb/redshift/`. O exemplo a seguir encadeia `RoleA` e `RoleB` para descarregar dados (comando UNLOAD) no 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';
```

O exemplo a seguir usa um comando COPY para carregar os dados que foram descarregados no exemplo anterior.

```
copy venue
from 's3://companyb/redshift/venue_pipe_'
```

```
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

No exemplo a seguir, o comando CREATE EXTERNAL SCHEMA usa funções encadeadas para assumir a função `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';
```

No exemplo a seguir, CREATE EXTERNAL FUNCTION usa funções encadeadas para assumir a função `RoleB`.

```
create external function lambda_example(varchar)
returns varchar
volatile
lambda 'exampleLambdaFunction'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

### Mais informações

Para obter mais informações, consulte também Autorizar operações COPY, UNLOAD, CREATE EXTERNAL FUNCTION e CREATE EXTERNAL SCHEMA usando funções do IAM.

## Autorizar operações COPY, UNLOAD, CREATE EXTERNAL FUNCTION e CREATE EXTERNAL SCHEMA usando funções do IAM

Você pode usar o comando COPY para carregar (ou importar) dados no Amazon Redshift e o comando UNLOAD para descarregar (ou exportar) dados do Amazon Redshift. Você pode usar o comando CREATE EXTERNAL FUNCTION para criar funções definidas pelo usuário que invocam funções do AWS Lambda.

Ao usar o Amazon Redshift Spectrum, você usa o comando CREATE EXTERNAL SCHEMA para especificar a localização de um bucket do Amazon S3 que contém seus dados. Ao executar os comandos COPY, UNLOAD ou CREATE EXTERNAL SCHEMA, você fornece credenciais de segurança. Essas credenciais autorizam seu cluster Amazon Redshift a ler ou gravar dados de e para seu destino, como um bucket do Amazon S3.

Ao executar o CREATE EXTERNAL FUNCTION, você fornece credenciais de segurança usando o parâmetro de função do IAM. Essas credenciais autorizam seu cluster do Amazon Redshift a invocar funções do Lambda do AWS Lambda. O método preferido para fornecer credenciais de segurança é

especificar uma função do AWS Identity and Access Management (IAM). Para COPY e UNLOAD, é possível fornecer as credenciais temporárias. Para obter informações sobre como criar uma função do IAM, consulte Autorizar o Amazon Redshift a acessar outros serviços da AWS em seu nome.

Os usuários precisam de acesso programático se quiserem interagir com a AWS de fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando a AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| Identificação da força de trabalho<br><br>(Usuários gerenciados no Centro de Identidade do IAM) | Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções da interface que deseja utilizar.<br><br>• Para a AWS CLI, consulte Configuração da AWS CLI para usar o AWS IAM Identity Center no AWS Command Line Interface Guia do usuário da .<br>• Para os SDKs da AWS, ferramentas e APIs da AWS, consulte Autenticação do Centro de Identidade do IAM no Guia de referência de ferramentas e SDKs da AWS. |
| IAM | Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | Siga as instruções em Como usar credenciais temporárias com recursos da AWS no Guia do usuário do IAM. |
| IAM | (Não recomendado) | Siga as instruções da interface que deseja utilizar. |

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| | Use credenciais de longo prazo para assinar solicitaç ões programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS. | • Para a AWS CLI, consulte Autenticação usando as credenciais de usuário do IAM no Guia do usuário da AWS Command Line Interface.<br>• Para as ferramentas e SDKs da AWS, consulte Autenticação usando as credenciais de longo prazo no Guia de referência de ferramentas e SDKs da AWS.<br>• Para as APIs da AWS, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM. |

As etapas para usar uma função do IAM são:

- Crie uma função do IAM para usar com seu cluster Amazon Redshift.
- Associe a função do IAM ao cluster.
- Inclua o ARN da função IAM ao chamar o comando COPY, UNLOAD, CREATE EXTERNAL SCHEMA ou CREATE EXTERNAL FUNCTION.

Neste tópico, você aprenderá a associar uma função do IAM a um cluster do Amazon Redshift.

Associar funções do IAM a clusters

Depois de criar uma função do IAM que autoriza o Amazon Redshift a acessar outros serviços da AWS para você, você deve associar essa função a um cluster do Amazon Redshift. Faça isso para poder usar a função para carregar ou descarregar dados.

Permissões necessárias para associar uma função do IAM a um cluster

Para associar um perfil do IAM a um cluster, um usuário deve ter a permissão `iam:PassRole` para esse perfil do IAM. Essa permissão permite que um administrador restrinja quais funções do IAM um usuário pode associar a clusters do Amazon Redshift. Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.

O exemplo a seguir mostra uma política do IAM que pode ser anexada a um usuário para permitir que ele realize estas ações:

- Obtenha os detalhes de todos os clusters do Amazon Redshift pertencentes à conta desse usuário.
- Associe qualquer uma das três funções do IAM a qualquer um dos dois clusters do 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"
            ]
        }
    ]
}
```

Depois que um usuário tem as permissões apropriadas, ele pode associar um perfil do IAM a um cluster do Amazon Redshift. A função do IAM está então pronta para uso com o comando COPY ou UNLOAD ou outros comandos do Amazon Redshift.

Para obter mais informações sobre políticas do IAM, consulte Visão geral das políticas do IAM no Guia do usuário do IAM.

Gerenciar a associação da função do IAM a um cluster

Você pode associar uma função do IAM a um cluster do Amazon Redshift ao criar o cluster. Ou você pode modificar um cluster existente e adicionar ou remover uma ou mais associações de funções do IAM.

Esteja ciente do seguinte:

- O número máximo de funções do IAM que você pode associar está sujeito a uma cota.
- Uma função do IAM pode ser associada a vários clusters do Amazon Redshift.
- Uma função do IAM pode ser associada a um cluster do Amazon Redshift apenas se a função do IAM e o cluster forem de propriedade da mesma conta da AWS.

Usar o console para gerenciar associações à função do IAM

Você pode gerenciar associações de função do IAM de um cluster ao console usando o procedimento a seguir.

Para gerenciar associações à função do IAM

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, depois selecione o cluster que deseja atualizar.
3. Em Actions (Ações), escolha Manage IAM roles (Gerenciar funções do IAM) para exibir a lista atual de funções do IAM associadas ao cluster.

4. Na página Manage IAM roles (Gerenciar funções do IAM), escolha as funções do IAM disponíveis para adição e escolha Add IAM role (Adicionar função do IAM).
5. Escolha Done (Concluído) para salvar as alterações.

### Usar a AWS CLI para gerenciar associações à função do IAM

É possível gerenciar associações à função do IAM de um cluster com a AWS CLI usando as abordagens a seguir.

#### Associar uma função do IAM a um cluster usando a AWS CLI

Para associar uma função do IAM a um cluster quando criado, especifique o nome de recurso da Amazon (ARN) da função do IAM do parâmetro `--iam-role-arns` do comando `create-cluster`. O número máximo de funções do IAM que você pode adicionar ao chamar o comando `create-cluster` está sujeito a uma cota.

Associar e desassociar funções do IAM com clusters do Amazon Redshift é um processo assíncrono. Você pode obter o status de todas as associações de cluster da função do IAM chamando o comando `describe-clusters`.

O exemplo a seguir associa duas funções do IAM ao cluster recém-criado chamado `my-redshift-cluster`.

```
aws redshift create-cluster \
    --cluster-identifier "my-redshift-cluster" \
    --node-type "dc1.large" \
    --number-of-nodes 16 \
    --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftCopyUnload" \
                    "arn:aws:iam::123456789012:role/SecondRedshiftRole"
```

Para associar uma função do IAM a um cluster existente do Amazon Redshift, especifique o nome do recurso da Amazon (ARN) da função IAM para o parâmetro `--add-iam-roles` do comando `modify-cluster-iam-roles` O número máximo de funções do IAM que você pode adicionar ao chamar o comando `modify-cluster-iam-roles` está sujeito a uma cota.

O exemplo a seguir associa uma função do IAM a um cluster existente chamado `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \
```

```
    --cluster-identifier "my-redshift-cluster" \
    --add-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Desassociar uma função do IAM de um cluster usando a AWS CLI

Para dissociar uma função do IAM de um cluster, especifique o ARN da função do IAM do parâmetro `--remove-iam-roles` do comando `modify-cluster-iam-roles`. `modify-cluster-iam-roles` O número máximo de funções do IAM que você pode remover ao chamar o comando `modify-cluster-iam-roles` está sujeito a uma cota.

O exemplo a seguir remove a associação de uma função do IAM para a conta da AWS `123456789012` de um cluster denominado `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier "my-redshift-cluster" \
    --remove-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Listar associações à função do IAM de um cluster usando a AWS CLI

Para listar todas as funções do IAM associadas a um cluster do Amazon Redshift e o status da associação de funções do IAM, chame o comando `describe-clusters`. O ARN de cada função do IAM associada ao cluster é retornado na lista `IamRoles` conforme mostrado na saída de exemplo a seguir.

As funções que foram associadas ao cluster mostram um status de `in-sync`. Funções no processo de associação ao cluster mostram um status `adding`. As funções que estão sendo desassociadas do cluster mostram um status de `removing`.

```
{
    "Clusters": [
        {
            "ClusterIdentifier": "my-redshift-cluster",
            "NodeType": "dc1.large",
            "NumberOfNodes": 16,
            "IamRoles": [
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                },
```

```
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                }
            ],
            ...
        },
        {
            "ClusterIdentifier": "my-second-redshift-cluster",
            "NodeType": "dc1.large",
            "NumberOfNodes": 10,
            "IamRoles": [
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                },
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                },
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/ThirdRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                }
            ],
            ...
        }
    ]
}
```

Para obter mais informações sobre como usar a AWS CLI, consulte o Manual do usuário do AWS CLI.

## Criar uma função do IAM como padrão para o Amazon Redshift

Quando você cria funções do IAM pelo console Redshift, o Amazon Redshift cria as funções em sua Conta da AWS de maneira programática e anexa automaticamente as políticas gerenciadas pela AWS para elas. Essa metodologia significa que você pode permanecer no console do Redshift e não precisa alternar para o console do IAM criar a função. Para um controle mais detalhado das permissões para uma função do IAM existente criada no console do Amazon Redshift, é possível anexar uma política gerenciada personalizada à função do IAM.

Visão geral das funções do IAM criadas no console

Quando você usa o console do Amazon Redshift para criar funções do IAM, o Amazon Redshift rastreia todas as funções do IAM criadas pelo console. O Amazon Redshift pré-seleciona a função padrão mais recente do IAM para criar todos os novos clusters e restaurar clusters de snapshots.

É possível criar uma função do IAM pelo console que tenha uma política com permissões para executar comandos SQL. Esses comandos incluem: COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL ou CREATE LIBRARY. Se preferir, você pode obter um controle mais detalhado do acesso do usuário a seus recursos da AWS criando e anexando políticas personalizadas à função do IAM.

Ao criar uma função do IAM e defini-la como padrão para o cluster usando o console, não é necessário fornecer o nome do recurso da Amazon (ARN) da função do IAM para executar autenticação e autorização.

Usar funções do IAM criadas no console do IAM

A função do IAM que você cria pelo console do cluster tem a política gerenciada `AmazonRedshiftAllCommandsFullAccess` anexada automaticamente. Essa função do IAM permite que o Amazon Redshift copie, carregue, consulte e analise dados de recursos da AWS em sua conta do IAM. A política gerenciada fornece acesso às operações COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL SCHEMA, CREATE MODEL e CREATE LIBRARY. A política também concede permissões para executar instruções SELECT para serviços relacionados da AWS, como Amazon S3, Amazon CloudWatch Logs, Amazon SageMaker e AWS Glue.

Os comandos CREATE EXTERNAL FUNCTION, CREATE EXTERNAL SCHEMA, CREATE MODEL e CREATE LIBRARY têm uma palavra-chave `default`. Para essa palavra-chave para esses comandos, o Amazon Redshift usa a função do IAM definida como padrão e associada ao cluster quando o comando COPY é executado. Você pode executar o comando DEFAULT_IAM_ROLE para verificar a função padrão do IAM atual que está anexada ao cluster.

Para controlar os privilégios de acesso da função do IAM criada e definida como padrão para o cluster do Redshift, use o privilégio ASSUMEROLE. Esse controle de acesso se aplica a usuários e grupos de banco de dados quando eles executam comandos como os listados anteriormente. Depois de conceder o privilégio ASSUMEROLE a um usuário ou grupo para uma função do IAM, o usuário ou grupo poderá assumir essa função ao executar esses comandos. Com o privilégio ASSUMEROLE, você pode conceder acesso aos comandos apropriados conforme necessário.

Com o console do Amazon Redshift, é possível fazer o seguinte:

- Criar uma função do IAM como padrão
- Remover funções do IAM do cluster
- Associar funções do IAM ao cluster
- Definir uma função do IAM como padrão
- Fazer com que uma função do IAM não seja padrão para o cluster

Permissões da política gerenciada AmazonRedshiftAllCommandsFullAccess

O exemplo a seguir exibe as permissões na política gerenciada `AmazonRedshiftAllCommandsFullAccess` que permite determinadas ações para a função do IAM definida como padrão para o cluster. A função do IAM com políticas de permissão anexadas autoriza o que um usuário ou grupo pode ou não fazer. Com essas permissões, é possível executar o comando COPY do Amazon S3, executar UNLOAD e usar o comando 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*/*"
            ]
}
```

O exemplo a seguir exibe as permissões na política gerenciada `AmazonRedshiftAllCommandsFullAccess` que permite determinadas ações para a função do IAM definida como padrão para o cluster. A função do IAM com políticas de permissão anexadas autoriza o que um usuário ou grupo pode ou não fazer. Com as permissões a seguir, é possível executar o comando CREATE EXTERNAL FUNCTION.

```
{
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": "arn:aws:lambda:*:*:function:*redshift*"
}
```

O exemplo a seguir exibe as permissões na política gerenciada `AmazonRedshiftAllCommandsFullAccess` que permite determinadas ações para a função do IAM definida como padrão para o cluster. A função do IAM com políticas de permissão anexadas autoriza o que um usuário ou grupo pode ou não fazer. Com as seguintes permissões, é possível executar os comandos CREATE EXTERNAL SCHEMA e CREATE EXTERNAL TABLE necessários para o 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*"
            ]
}
```

O exemplo a seguir exibe as permissões na política gerenciada `AmazonRedshiftAllCommandsFullAccess` que permite determinadas ações para a função do IAM definida como padrão para o cluster. A função do IAM com políticas de permissão anexadas autoriza o que um usuário ou grupo pode ou não fazer. Com as permissões a seguir, é possível executar o comando CREATE EXTERNAL SCHEMA usando consultas federadas.

```
{
            "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"
                }
            }
},
```

### Gerenciar funções do IAM criadas para um cluster usando o console

Para criar, modificar e remover funções do IAM criadas a partir do console do Amazon Redshift, use a seção Clusters no console.

### Criar uma função do IAM como padrão

No console, é possível criar uma função do IAM pelo console do cluster que tenha a política gerenciada `AmazonRedshiftAllCommandsFullAccess` anexada automaticamente. A nova função do IAM que você criar permitirá que o Amazon Redshift copie, carregue, consulte e analise dados de recursos da Amazon em sua conta do IAM.

Pode haver somente um conjunto de funções do IAM definido como padrão para o cluster. Se você criar outra função do IAM como padrão do cluster quando uma função do IAM existente estiver atualmente atribuída como padrão, a nova função do IAM substituirá a outra como padrão.

Para criar um novo cluster e um conjunto de funções do IAM como padrão para o novo cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters. Os clusters de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha Create cluster (Criar cluster) para criar um cluster.
4. Siga as instruções na página do console para inserir as propriedades de Cluster configuration (Configuração do cluster). Para obter mais informações sobre essa etapa, consulte Criar um cluster.
5. (Opcional) Escolha Load sample data (Carregar dados de exemplo) para carregar o conjunto de dados de exemplo no cluster do Amazon Redshift para começar a usar o editor de consultas para consultar dados.

   Se você estiver atrás do firewall, a porta do banco de dados deverá ser uma porta aberta que aceite conexões de entrada.
6. Siga as instruções na página do console para inserir as propriedades de Database configurations (Configurações de banco de dados).
7. Em Cluster permissions (Permissões do cluster), em Manage IAM roles (Gerenciar funções do IAM), escolha Create IAM role (Criar função do IAM).
8. Especifique um bucket do Amazon S3 para que a função do IAM seja acessada escolhendo um destes métodos:

- Selecione No additional Amazon S3 bucket (Nenhum bucket adicional do Amazon S3) para criar a função do IAM sem especificar buckets do Amazon S3.
- Escolha Any Amazon S3 bucket (Qualquer bucket do Amazon S3) para permitir que os usuários que tenham acesso ao cluster do Amazon Redshift também acessem qualquer bucket do Amazon S3 e o conteúdo dele em sua Conta da AWS.
- Escolha Specific Amazon S3 buckets (Buckets específicos do Amazon S3) para especificar um ou mais buckets do Amazon S3 que a função do IAM criada tenha função para acessar. Em seguida, escolha um ou mais buckets do Amazon S3 na tabela.

9. Escolha Create IAM role as default (Criar função do IAM como padrão). O Amazon Redshift cria e define automaticamente a função do IAM como padrão para o cluster.
10. Para criar o cluster, escolha Create cluster (Criar cluster). Podem ser necessários alguns minutos para preparar o cluster para ser usado.

### Remover funções do IAM do cluster

É possível remover uma ou mais funções do IAM de seu cluster.

Para remover funções do IAM do cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters. Os clusters de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha o cluster do qual você deseja remover a função do IAM.
4. Em Cluster permissions (Permissões do cluster), escolha uma ou mais funções do IAM que você deseja remover do cluster.
5. Em Manage IAM roles (Gerenciar funções do IAM), escolha Remove IAM roles (Remover funções do IAM).

### Associar funções do IAM ao cluster

É possível associar uma ou mais funções do IAM ao cluster.

Para associar funções do IAM ao cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters. Os clusters de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha o cluster ao qual você deseja associar funções do IAM.
4. Em Cluster permissions (Permissões do cluster), escolha uma ou mais funções do IAM que você deseja associar ao cluster.
5. Em Manage IAM roles (Gerenciar funções do IAM), escolha Associate IAM roles (Associar funções do IAM).
6. Escolha uma ou mais funções do IAM para associar ao cluster.
7. Em seguida, escolha Associate IAM roles (Associar funções do IAM).

Definir uma função do IAM como padrão

É possível definir uma função do IAM como padrão para o cluster.

Para tornar uma função do IAM padrão para o cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters. Os clusters de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha o cluster para o qual deseja definir uma função padrão do IAM.
4. Em Cluster permissions (Permissões do cluster, de Associated IAM roles (Funções do IAM associadas), escolha uma função do IAM que você deseja tornar padrão para o cluster.
5. Em Set default (Configurar padrão), escolha Make default (Tornar padrão).
6. Quando solicitado, escolha Set default (Configurar padrão) para confirmar como padrão a função do IAM especificada.

Fazer com que uma função do IAM não seja padrão para o cluster

É possível fazer com que uma função do IAM não seja padrão para o cluster.

Para desmarcar uma função do IAM como padrão para o cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters. Os clusters de sua conta na Região da AWS atual são listados. Um subconjunto de propriedades de cada cluster é exibido nas colunas na lista.
3. Escolha o cluster ao qual você deseja associar funções do IAM.
4. Em Cluster permissions (Permissões do cluster, de Associated IAM roles (Funções do IAM associadas), escolha a função do IAM padrão.
5. Em Set default (Configurar padrão), escolha Clear default (Desmarcar padrão).
6. Quando solicitado, escolha Clear default (Desmarcar padrão) para desmarcar a função do IAM especificada como padrão.

Gerenciar funções do IAM criadas em um cluster usando a AWS CLI

É possível gerenciar as funções do IAM criadas em um cluster usando a AWS CLI.

Para criar um cluster do Amazon Redshift com uma função do IAM definida como padrão

Para criar um cluster do Amazon Redshift com uma função do IAM definida como padrão para o cluster, use o comando `aws redshift create-cluster` da AWS CLI.

O seguinte comando da AWS CLI cria um cluster do Amazon Redshift e a função do IAM chamada myrole1. O comando AWS CLI também define myrole1 como o padrão para o 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'
```

O snippet a seguir é um exemplo da resposta.

```
{
    "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"
            }
        ]
        ...
    }
}
```

Para adicionar uma ou mais funções do IAM a um cluster do Amazon Redshift

Para adicionar uma ou mais funções do IAM associadas ao cluster, use o comando `aws redshift modify-cluster-iam-roles` da AWS CLI.

O seguinte comando AWS CLI adiciona `myrole3` e `myrole4` ao 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'
```

O snippet a seguir é um exemplo da resposta.

```
{
    "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"
            }
        ],
        ...
    }
}
```

Para remover uma ou mais funções do IAM de um cluster do Amazon Redshift

Para remover uma ou mais funções do IAM associadas ao cluster, use o comando `aws redshift modify-cluster-iam-roles` da AWS CLI.

O comando da AWS CLI a seguir remove `myrole3` e `myrole4` do 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'
```

O snippet a seguir é um exemplo da resposta.

```
{
    "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"
            }
        ],
        ...
    }
}
```

Para definir uma função do IAM associada como padrão para o cluster

Para definir uma função do IAM associada como padrão para o cluster, use o comando `aws redshift modify-cluster-iam-roles` da AWS CLI.

O comando da AWS CLI a seguir também define `myrole2` como o padrão para o cluster.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole2'
```

O snippet a seguir é um exemplo da resposta.

```
{
    "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"
```

```
            }
        ],
        ...
    }
}
```

Para definir uma função do IAM não associada como padrão para o cluster

Para definir uma função do IAM não associada como padrão para o cluster, use o comando `aws redshift modify-cluster-iam-roles` da AWS CLI.

O seguinte comando da AWS CLI adiciona `myrole2` ao cluster do Amazon Redshift e o define como padrão para o 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'
```

O snippet a seguir é um exemplo da resposta.

```
{
    "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"
            }
        ],
        ...
    }
```

```
}
```

Para restaurar um cluster de um snapshot e definir uma função do IAM como padrão para ele

Ao restaurar o cluster de um snapshot, é possível associar uma função do IAM existente ou criar uma nova e defini-la como padrão para o cluster.

Para restaurar um cluster do Amazon Redshift de um snapshot com uma função do IAM definida como padrão para o cluster, use o comando `aws redshift restore-from-cluster-snapshot` da AWS CLI.

O seguinte comando da AWS CLI restaura o cluster de um snapshot e define `myrole2` como padrão para o 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'
```

O snippet a seguir é um exemplo da resposta.

```
{
    "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"
            }
        ],
        ...
    }
}
```

## Usar uma identidade federada para gerenciar o acesso do Amazon Redshift aos recursos locais e às tabelas externas do Amazon Redshift Spectrum

Usar a federação de identidades na AWS com as credenciais fornecidas pelo `GetDatabaseCredentials` pode simplificar a autorização e o acesso a dados locais e externos. Atualmente, para dar aos usuários acesso aos dados externos que residem no Amazon S3, você cria um perfil do IAM com permissões definidas em uma política de permissões. Depois, os usuários com o perfil anexado podem acessar os dados externos. Isso funciona, mas se você quiser fornecer regras detalhadas, como tornar colunas específicas indisponíveis para determinado usuário, talvez seja necessário definir configurações adicionais no esquema externo. Neste tópico, mostramos como fornecer acesso a recursos com a federação de identidades da AWS, em vez de usar um perfil específico do IAM. A federação de identidades, com credenciais fornecidas pelo `GetDatabaseCredentials`, pode fornecer acesso a recursos do AWS Glue e do Redshift Spectrum por meio de regras detalhadas do IAM que são mais fáceis de especificar e alterar. Isso facilita a aplicação do acesso que está em conformidade com suas regras empresariais.

Os benefícios de usar credenciais federadas são os seguintes:

- Não é necessário gerenciar perfis do IAM anexados ao cluster para o Redshift Spectrum.
- Os administradores do cluster podem criar um esquema externo acessível por consumidores com diferentes contextos do IAM. Isso é útil, por exemplo, para realizar a filtragem de colunas em uma tabela, na qual consumidores diferentes consultam o mesmo esquema externo e obtêm campos variados nos registros retornados.
- É possível consultar o Amazon Redshift usando um usuário com permissões do IAM, em vez de apenas com um perfil.

### Preparar uma identidade para fazer login com a identidade federada

Antes de fazer login com identidade federada, você deve realizar várias etapas preliminares. Essas instruções pressupõem que você tenha um esquema externo existente do Redshift Spectrum que faz referência a um arquivo de dados armazenado em um bucket do Amazon S3 e que o bucket esteja na mesma conta do cluster Amazon Redshift ou do data warehouse do Amazon Redshift Serverless.

1. Crie uma identidade do IAM. Isso pode ser um usuário ou um perfil do IAM. Use qualquer nome permitido pelo IAM.
2. Anexe políticas de permissões à identidade. Especifique um destes fatores:

- `redshift:GetClusterCredentialsWithIAM` (para um cluster provisionado do Amazon Redshift)
- `redshift-serverless:GetCredentials` (para o Amazon Redshift Serverless)

É possível adicionar permissões com o editor de políticas por meio do console do IAM.

A identidade do IAM também precisa de permissões para acessar dados externos. Conceda acesso ao Amazon S3 adicionando diretamente as seguintes políticas gerenciadas da AWS:

- `AmazonS3ReadOnlyAccess`
- `AWSGlueConsoleFullAccess`

A última política gerenciada será necessária se você estiver usando o AWS Glue para preparar os dados externos. Para obter mais informações sobre as etapas para conceder acesso ao Amazon Redshift Spectrum, consulte "Criar uma função do IAM para o Amazon Redshift", que faz parte do guia de introdução do Amazon Redshift e do Redshift Spectrum. Ele mostra as etapas de adição de políticas do IAM para acessar o Redshift Spectrum.

3. Configure o cliente SQL para se conectar ao Amazon Redshift. Use o driver JDBC do Amazon Redshift e adicione as credenciais do usuário às propriedades de credencial da ferramenta. Um cliente como o SQL Workbench/J funciona bem para isso. Defina as seguintes propriedades estendidas de conexão do cliente:
   - AccessKeyID: o identificador da chave de acesso.
   - SecretAccessKey: a chave de acesso secreta. (Preste atenção ao risco de segurança de transmitir a chave secreta caso você não use criptografia.)
   - SessionToken: um conjunto de credenciais temporárias para um perfil do IAM.
   - groupFederation: defina como `true` se você estiver configurando a identidade federada para um cluster provisionado. Não defina esse parâmetro se você estiver usando o Amazon Redshift Serverless.
   - LogLevel: valor inteiro no nível de log. Isso é opcional.
4. Defina o URL como o endpoint JDBC encontrado no console do Amazon Redshift ou do Amazon Redshift Serverless. Substitua seu esquema de URL por jdbc:redshift:iam: e use esta formatação:

- Formato para um cluster provisionado do Amazon Redshift: `jdbc:redshift:iam://<cluster_id>.<unique_suffix>.<region>.redshift.amazonaws.com:<port>/<database_name>`

  Exemplo: `jdbc:redshift:iam://test1.12345abcdefg.us-east-1.redshift.amazonaws.com:5439/dev`
- Formato para o Amazon Redshift Serverless: `jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com:5439:<port>/<database_name>`

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

Depois de se conectar ao banco de dados pela primeira vez usando uma identidade do IAM, o Amazon Redshift cria automaticamente uma identidade do Amazon Redshift com o mesmo nome, com o prefixo `IAM:` para um usuário ou `IAMR:` para um perfil do IAM. As etapas restantes deste tópico mostram exemplos para um usuário.

Se um usuário do Redshift não for criado automaticamente, você poderá criar um executando uma instrução `CREATE USER`, usando uma conta de administrador e especificando o nome do usuário no formato `IAM:<user name>`.

5. Como administrador do cluster do Amazon Redshift, conceda ao usuário do Redshift as permissões necessárias para acessar o esquema externo.

```
GRANT ALL ON SCHEMA my_schema to "IAM:my_user";
```

Para permitir que o usuário do Redshift crie tabelas no esquema externo, ele deve ser proprietário do esquema. Por exemplo:

```
ALTER SCHEMA my_schema owner to "IAM:my_user";
```

6. Para verificar a configuração, execute uma consulta como usuário, usando o cliente SQL, depois que as permissões forem concedidas. Esse exemplo de consulta recupera dados de uma tabela externa.

```
SELECT * FROM my_schema.my_table;
```

Conceitos básicos da propagação de identidade e autorização para o Redshift Spectrum

A fim de transmitir uma identidade federada para consultar tabelas externas, defina `SESSION` como o valor para o parâmetro de consulta `IAM_ROLE` de `CREATE EXTERNAL SCHEMA`. As etapas a seguir mostram como configurar e utilizar `SESSION` para autorizar consultas no esquema externo.

1. Crie tabelas locais e externas. Tabelas externas catalogadas com o AWS Glue funcionam para isso.
2. Conecte-se ao Amazon Redshift com sua identidade do IAM. Conforme mencionado na seção anterior, quando a identidade se conecta ao Amazon Redshift, é criado um usuário de banco de dados do Redshift. O usuário é criado caso ainda não exista. Se o usuário for novo, o administrador deverá conceder a ele permissões para realizar tarefas no Amazon Redshift, como consultar e criar tabelas.
3. Conecte-se ao Redshift com sua conta de administrador. Execute o comando para criar um esquema externo usando o valor `SESSION`.

   ```
   create external schema spectrum_schema from data catalog
   database '<my_external_database>'
   region '<my_region>'
   iam_role 'SESSION'
   catalog_id '<my_catalog_id>';
   ```

   Observe que `catalog_id` está definido nesse caso. Essa é uma nova configuração adicionada com o recurso, pois `SESSION` substitui uma função específica.

   Nesse exemplo, os valores na consulta imitam como os valores reais aparecem.

   ```
   create external schema spectrum_schema from data catalog
   database 'spectrum_db'
   region 'us-east-1'
   iam_role 'SESSION'
   catalog_id '123456789012'
   ```

   O valor `catalog_id` nesse caso é o ID da sua conta da AWS.
4. Execute consultas para acessar seus dados externos usando a identidade do IAM com a qual você se conectou na etapa 2. Por exemplo:

   ```
   select * from spectrum_schema.table1;
   ```

Nesse caso, `table1` pode ser, por exemplo, dados formatados em JSON em um arquivo, em um bucket do Amazon S3.

5. Se você já tem um esquema externo que usa um perfil do IAM anexado ao cluster, apontando para seu banco de dados ou esquema externo, é possível substituir o esquema existente e usar uma identidade federada, conforme detalhado nestas etapas, ou criar uma.

`SESSION` indica que as credenciais da identidade federada são usadas para consultar o esquema externo. Ao usar o parâmetro de consulta `SESSION`, defina o `catalog_id`. Isso é necessário porque aponta para o catálogo de dados usado para o esquema. Anteriormente, o `catalog_id` era recuperado do valor atribuído a `iam_role`. Quando você configura a propagação de identidade e autorização dessa forma (por exemplo, para o Redshift Spectrum), usando credenciais federadas para consultar um esquema externo, a autorização por meio de um perfil do IAM não é necessária.

Observações de uso

Um erro de conexão comum é o seguinte: Erro do IAM ao recuperar credenciais temporárias: não é possível realizar unmarshaling da resposta de exceção com os operadores de unmarshaling fornecidos. Esse erro ocorre quando se tem um driver JDBC herdado. A versão mínima do driver necessária para identidade federada é 2.1.0.9. Você pode obter o driver JDBC em Baixe o driver JDBC do Amazon Redshift, versão 2.1.

Recursos adicionais do

Esses links fornecem informações adicionais para gerenciar o acesso a dados externos.

- Você ainda pode acessar os dados do Redshift Spectrum usando um perfil do IAM. Para ter mais informações, consulte Autorizar o Amazon Redshift a acessar outros serviços da AWS em seu nome.
- Ao gerenciar o acesso a tabelas externas com o AWS Lake Formation, você pode consultá-las usando o Redshift Spectrum com identidades federadas do IAM. Não é mais necessário gerenciar perfis do IAM anexados a clusters para que o Redshift Spectrum consulte dados registrados com o AWS Lake Formation. Para obter mais informações, consulte Usar o Amazon Redshift Spectrum com o AWS Lake Formation.

# Gerenciamento das senhas de administrador do Amazon Redshift usando AWS Secrets Manager

O Amazon Redshift pode se integrar ao AWS Secrets Manager para gerar e gerenciar as credenciais de administrador dentro de um segredo criptografado. Com AWS Secrets Manager, é possível substituir as senhas de administrador por uma chamada de API para recuperar programaticamente o segredo quando necessário. O uso de segredos, em vez de credenciais com codificação rígida, reduz o risco dessas credenciais serem expostas ou comprometidas. Para mais informações sobre o AWS Secrets Manager, consulte o Guia do usuário do AWS Secrets Manager.

Você pode especificar que o Amazon Redshift gerencia a senha de administrador usando o AWS Secrets Manager ao realizar uma das seguintes operações:

- Criação de um cluster provisionado ou de um namespace de tecnologia sem servidor
- Restauração de um cluster ou de um namespace de tecnologia sem servidor usando um snapshot

Quando você especifica que o Amazon Redshift gerencia a senha de administrador no AWS Secrets Manager, o Amazon Redshift gera a senha e a armazena no Secrets Manager. É possível acessar diretamente o segredo no AWS Secrets Manager para recuperar as credenciais do usuário de administrador. Também será possível especificar uma chave gerenciada pelo cliente para criptografar o segredo, se você precisar acessá-lo por outra conta da AWS. Também é possível usar a chave KMS fornecida pelo AWS Secrets Manager.

O Amazon Redshift gerencia as configurações do segredo e o alterna a cada 30 dias por padrão. É possível girar manualmente o segredo a qualquer momento. Se você excluir um cluster provisionado ou um namespace de tecnologia sem servidor que gerencia um segredo no AWS Secrets Manager, o segredo e os metadados associados também serão excluídos.

Para se conectar a um cluster ou a um namespace de tecnologia sem servidor com credenciais gerenciadas por segredo, você pode recuperar o segredo do AWS Secrets Manager usando o console do Secrets Manager ou a chamada de API do Secrets Manager. Para ter mais informações, consulte Recuperar segredos do AWS Secrets Manager e Conecte-se a um banco de dados SQL com credenciais em um segredo do AWS Secrets Manager no Guia do usuário do AWS Secrets Manager.

## Permissões necessárias para integração do AWS Secrets Manager

Os usuários devem ter as permissões necessárias para realizar operações relacionadas à integração do AWS Secrets Manager. Crie políticas do IAM que concedam permissões para realizar operações de API específicas nos recursos especificados dos quais eles precisam. Em seguida, anexe essas políticas aos conjuntos de permissões do IAM ou às funções que exigem essas permissões. Para ter mais informações, consulte Gerenciamento de Identidade e Acesso no Amazon Redshift.

O usuário que especifica que o Amazon Redshift gerencie a senha de administrador no AWS Secrets Manager deve ter permissões para realizar as seguintes operações:

- `secretsmanager:CreateSecret`
- `secretsmanager:RotateSecret`
- `secretsmanager:DescribeSecret`
- `secretsmanager:UpdateSecret`
- `secretsmanager:DeleteSecret`
- `secretsmanager:GetRandomPassword`
- `secretsmanager:TagResource`

Se quiser passar uma chave KMS no parâmetro `MasterPasswordSecretKmsKeyId` para clusters provisionados ou no parâmetro `AdminPasswordSecretKmsKeyId` para namespaces de tecnologia sem servidor, o usuário precisará das permissões a seguir, além das permissões listadas acima.

- `kms:Decrypt`
- `kms:GenerateDataKey`
- `kms:CreateGrant`
- `kms:RetireGrant`

## Troca do segredo da senha de administrador

Por padrão, o Amazon Redshift troca automaticamente o segredo a cada 30 dias para garantir que as credenciais não continuem as mesmas por períodos prolongados. Quando o Amazon Redshift troca um segredo de senha de administrador, o AWS Secrets Manager atualiza o segredo existente para conter uma nova senha de administrador. O Amazon Redshift altera a senha de administrador do cluster para corresponder à senha no segredo atualizado.

Você pode trocar imediatamente um segredo, em vez de aguardar uma troca programada usando AWS Secrets Manager. Para obter mais informações, consulte Rotate AWS Secrets Manager secrets no Guia de usuário do AWS Secrets Manager.

## Recuperação do nome do recurso da Amazon (ARN) do segredo no Amazon Redshift

Você pode exibir o nome do recurso da Amazon (ARN) em busca de qualquer segredo gerenciado pelo AWS Secrets Manager usando o console do Amazon Redshift. Depois de recuperar o ARN do segredo, você poderá exibir detalhes sobre o segredo e os dados criptografados no segredo usando o AWS Secrets Manager. Para obter mais informações sobre como recuperar segredos usando o ARN, consulte Retrieve secrets no Guia de usuário do AWS Secrets Manager.

Exibição dos detalhes sobre um segredo de um cluster provisionado pelo Amazon Redshift

Exiba o nome do recurso da Amazon (ARN) do segredo do cluster usando o console do Amazon Redshift com o seguinte procedimento:

1. Faça logon no AWS Management Console e abra o console do Amazon Redshift.
2. No painel Visão geral do cluster, escolha o cluster cujo segredo você deseja exibir.
3. Escolha a guia Properties (Propriedades).
4. Exiba o ARN do segredo em ARN em ARN de credenciais de administrador. Esse ARN é o identificador do segredo, que é possível usar no AWS Secrets Manager para exibir os detalhes do segredo.

Exibição dos detalhes sobre um segredo para um namespace do Amazon Redshift sem servidor

Exiba o nome do recurso da Amazon (ARN) do segredo do namespace de tecnologia sem servidor usando o console do Amazon Redshift com o seguinte procedimento:

1. Faça logon no AWS Management Console e abra o console do Amazon Redshift.
2. No painel Clusters provisionados, escolha Acessar a tecnologia sem servidor no canto superior direito da página.
3. No painel de tecnologia sem servidor, role até o painel Namespaces/Grupos de trabalho e escolha o namespace cujo segredo você deseja visualizar.
4. No painel Informações gerais, exiba o ARN do segredo em ARN de credenciais de administrador. Esse ARN é o identificador do segredo, que é possível usar no AWS Secrets Manager para exibir os detalhes do segredo.

# Criar um segredo para credenciais de conexão de banco de dados

Você pode criar um segredo do Secrets Manager para armazenar as credenciais usadas para conexão com um cluster provisionado do Amazon Redshift ou um namespace e grupo de trabalho do Redshift sem servidor.

Como criar um segredo usado para conexão com um banco de dados em um cluster provisionado

1. Abra o console do Secrets Manager em (https://console.aws.amazon.com/secretsmanager/).
2. Selecione Armazenar um novo segredo.
3. Escolha Credenciais para um cluster do Amazon Redshift.

   Insira as informações para:

   - Nome do usuário
   - Senha
   - Chave de criptografia

   Escolha um cluster para o qual criar credenciais secretas.
4. Escolha Próximo para ir para a próxima tela.
5. Adicione uma chave de tag iniciada com a string “Redshift”.
6. Continue inserindo informações sobre seu segredo seguindo as várias telas até armazenar suas alterações.

Confirme se aparece uma mensagem informando que o segredo foi armazenado com sucesso. Também é possível visualizar o segredo no console do Secrets Manager. Você pode usá-lo para se conectar a um banco de dados em um cluster no console do Amazon Redshift e no Editor de Consultas do Amazon Redshift v2, utilizando o método de conexão do AWS Secrets Manager. Você também deve adicionar uma chave de tag iniciada com a string “Redshift” para que o segredo seja listado na aplicação web do editor de consultas v2.

Como criar um segredo usado para conexão com um banco de dados em um grupo de trabalho do Redshift sem servidor

1. Abra o console do Redshift sem servidor.
2. Acesse Configuração do namespace.

3. Escolha um namespace para o qual criar credenciais secretas.
4. Abra Ações, Edite credenciais de administrador.
5. Em Senha do administrador, escolha Gerenciar credenciais do administrador no AWS Secrets Manager.
6. Escolha Salvar alterações para salvar suas alterações.

Confirme se aparece uma mensagem informando que a senha foi alterada com sucesso. Também é possível visualizar o segredo no console do Secrets Manager. Você pode usá-lo para se conectar a um banco de dados em um grupo de trabalho no console do Amazon Redshift sem servidor e no Editor de Consultas do Amazon Redshift v2, utilizando o método de conexão do AWS Secrets Manager. Você também deve adicionar uma chave de tag iniciada com a string “Redshift” para que o segredo seja listado na aplicação web do editor de consultas v2.

## Considerações sobre como usar o AWS Secrets Manager com o Amazon Redshift

Ao usar AWS Secrets Manager para gerenciar o cluster provisionado ou as credenciais de administrador do namespace de tecnologia sem servidor, considere o seguinte:

- Quando pausar um cluster cujas credenciais de administrador são gerenciadas pelo AWS Secrets Manager, o segredo do cluster não será excluído e você continuará recebendo a cobrança pelo segredo. Os segredos só são excluídos quando você exclui o cluster.
- Se o cluster for pausado quando o Amazon Redshift tentar trocar o segredo anexado, a troca vai falhar. Nesse caso, o Amazon Redshift interrompe a troca automática e não vai tentar trocá-la novamente, mesmo depois que você retomar o cluster. Você deve reiniciar a programação de rotação automática usando a chamada de API `secretsmanager:RotateSecret` para fazer o AWS Secrets Manager continuar trocando o segredo automaticamente.
- Se o namespace de tecnologia sem servidor não tiver um grupo de trabalho associado quando o Amazon Redshift tentar trocar o segredo anexado, a troca vai falhar e não tentar trocá-lo novamente, mesmo depois de você anexar um grupo de trabalho. Você deve reiniciar a programação de rotação automática usando a chamada de API `secretsmanager:RotateSecret` para fazer o AWS Secrets Manager continuar trocando o segredo automaticamente.

# Registrar em log e monitorar no Amazon Redshift

O monitoramento é uma parte importante para manter a confiabilidade, disponibilidade e performance do Amazon Redshift e de suas soluções da AWS. Você pode coletar dados de monitoramento de todas as partes da sua solução da AWS para que possa depurar mais facilmente uma falha multiponto, caso ocorra. A AWS fornece várias ferramentas para monitorar seus recursos do Amazon Redshift e responder a possíveis incidentes:

Alarmes do Amazon CloudWatch

Com o uso de alarmes do Amazon CloudWatch, você observa uma única métrica durante um período especificado. Se a métrica exceder determinado limite, uma notificação será enviada para um tópico do Amazon SNS ou para uma política do AWS Auto Scaling. Os alarmes do CloudWatch não invocam ações só porque estão em um determinado estado. O estado deve ter sido alterado e mantido por uma quantidade especificada de períodos. Para obter mais informações, consulte Gerenciar alarmes. Para obter uma lista das métricas, consulte Monitorar o Amazon Redshift usando métricas do CloudWatch.

Logs do AWS CloudTrail

O CloudTrail fornece um registro das operações de API executadas por um usuário do IAM, um perfil do IAM ou um serviço da AWS no Amazon Redshift. Usando as informações coletadas pelo CloudTrail, você pode determinar a solicitação feita ao Amazon Redshift, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando foi feita e detalhes adicionais. Para obter mais informações, consulte Registrar em log com o CloudTrail.

## Registro em log da auditoria de banco de dados

O Amazon Redshift registra informações sobre conexões e atividades do usuário em seu banco de dados. Esses logs ajudam a monitorar o banco de dados para fins de segurança e solução de problemas, um processo conhecido como auditoria de banco de dados. Os logs podem ser armazenados em:

- Buckets do Amazon S3: eles fornecem acesso com recursos de segurança de dados a usuários responsáveis por monitorar atividades no banco de dados.
- Amazon CloudWatch: é possível visualizar dados de log de auditoria usando os recursos incorporados ao CloudWatch, como de visualização e ações de configuração.

> **Note**
>
> SYS_CONNECTION_LOG coleta dados de log de conexão para o Amazon Redshift sem servidor. Quando você coleta dados de logs de auditoria para o Amazon Redshift sem servidor, não é possível enviá-los a arquivos de log, somente ao CloudWatch.

Tópicos


- Logs do Amazon Redshift
- Habilitar o log
- Enviar logs de auditoria ao Amazon CloudWatch
- Gerenciar arquivos de log no Amazon S3
- Solução de problemas de registro em log de auditoria do Amazon Redshift no Amazon S3
- Registro em log de chamadas de API do Amazon Redshift com o AWS CloudTrail
- Configurar a auditoria usando o console
- Configurar registro em log usando a AWS CLI e a API do Amazon Redshift


## Logs do Amazon Redshift

O Amazon Redshift registra informações nos seguintes arquivos de log:

- Log de conexão: registra tentativas de autenticação, conexões e desconexões.
- Log do usuário: registra informações sobre as alterações nas definições do usuário do banco de dados.
- Log de atividades do usuário: registra cada consulta antes de ser executada no banco de dados.

Os logs de conexão e de usuário são úteis principalmente para fins de segurança. É possível usar o log de conexão para monitorar informações sobre os usuários que estão se conectando ao banco de dados e informações relacionadas às conexões. Essas informações podem ser seus endereços IP, quando fizeram a solicitação, o tipo de autenticação que usaram e assim por diante. Você pode usar o log do usuário para monitorar alterar feitas nas definições dos usuários do banco de dados.

O log de atividade do usuário é útil principalmente para fins de solução de problemas. Ele acompanha informações sobre os tipos de consultas que os usuários e o sistema realizam no banco de dados.

O log de conexão e o log do usuário correspondem a informações armazenadas nas tabelas de sistema no banco de dados. Você pode usar as tabelas de sistema para obter as mesmas informações, mas os arquivos de log oferecem um mecanismo mais simples de recuperação e análise. Os arquivos de log contam com permissões do Amazon S3 em vez de permissões de banco de dados para realizar consultas nas tabelas. Além disso, exibindo as informações em arquivos de log, em vez de consultar as tabelas do sistema, você reduz todo o impacto da interação com o banco de dados.

> **Note**
>
> Os arquivos de log não são tão atuais quanto as tabelas de log do sistema, que são STL_USERLOG e STL_CONNECTION_LOG. Os registros mais antigos, exceto o último registro, são copiados para os arquivos de log.

> **Note**
>
> Para o Amazon Redshift sem servidor, SYS_CONNECTION_LOG coleta dados de log de conexão. Quando você coleta dados de logs de auditoria para o Amazon Redshift sem servidor, não é possível enviá-los a arquivos de log, somente ao CloudWatch.

### Log de conexão

Registra em log as tentativas de autenticação, além de conexões e desconexões. A tabela a seguir descreve as informações no log de conexão. Para obter mais informações sobre esses campos, consulte STL_CONNECTION_LOG no Guia do desenvolvedor de banco de dados do Amazon Redshift. Para obter mais informações sobre os dados de log de conexão coletados para o Amazon Redshift sem servidor, consulte SYS_CONNECTION_LOG.

| Nome da coluna | Descrição |
| --- | --- |
| evento | O evento de conexão ou de autenticação. |
| recordtime | O horário em que o evento ocorreu. |
| remotehost | O nome ou endereço IP do host remoto. |

| Nome da coluna | Descrição |
| --- | --- |
| remoteport | O número da porta do host remoto. |
| pid | O ID do processo associado à instrução. |
| dbname | Database name. |
| username | User name. |
| authmethod | O método de autenticação. |
| duration | A duração da conexão em microssegundos. |
| sslversion | A versão do Secure Sockets Layer (SSL). |
| sslcipher | A codificação do SSL. |
| mtu | A unidade de transmissão máxima (MTU). |
| sslcompression | O tipo de compactação do SSL. |
| sslexpansion | O tipo de expansão do SSL. |
| iamauthguid | O ID de autenticação do AWS Identity and Access Management (IAM) para a solicitação do AWS CloudTrail. Esse é o identificador da chamada da API GetClusterCredentials para criar as credenciais que estão sendo usadas para determinada conexão. |
| application_name | A iniciais ou o nome atualizado da aplicação de uma sessão. |
| os_version | A versão do sistema operacional que está na máquina cliente que se conecta ao cluster do Amazon Redshift. |
| driver_version | A versão do driver ODBC ou JDBC que se conecta ao cluster do Amazon Redshift a partir das ferramentas de cliente SQL de terceiros. |
| plugin_name | O nome do plugin usado para se conectar ao seu cluster do Amazon Redshift. |

| Nome da coluna | Descrição |
| --- | --- |
| protocol_ version | A versão do protocolo interno que o driver do Amazon Redshift usa ao estabelecer sua conexão com o servidor. |
| sessionid | O identificador exclusivo global da sessão atual. |
| compression | O algoritmo de compactação em uso para a conexão. |

Log do usuário

Registra os detalhes das seguintes alterações de um usuário de banco de dados:

- Criar usuário
- Descartar usuário
- Alterar usuário (renomear)
- Alterar usuário (alterar as propriedades)

| Nome da coluna | Descrição |
| --- | --- |
| userid | O ID do usuário afetado pela alteração. |
| username | O nome de usuário do usuário afetado pelas alterações. |
| oldusername | Para uma ação de renomeação, o nome de usuário original. Para qualquer outra ação, este campo é vazio. |
| ação | A ação ocorrida. Valores válidos:<br>• Alter<br>• Criar<br>• Drop<br>• Renomear |

| Nome da coluna | Descrição |
| --- | --- |
| usecreatedb | Se for verdadeiro (1), indica que o usuário tem permissões para criar um banco de dados. |
| usesuper | Se for verdadeiro (1), indica que o usuário é um superusuário. |
| usecatupd | Se for verdadeiro (1), indica que o usuário pode atualizar catálogos do sistema. |
| valuntil | A data de expiração da senha. |
| pid | ID do processo. |
| xid | ID da transação. |
| recordtime | O horário (em UTC) de início da consulta. |

Consulte a visualização de sistema SYS_USERLOG para encontrar mais informações sobre alterações nos usuários. Essa visualização inclui dados de log do Amazon Redshift sem servidor.

Log de atividades do usuário

Registra em log todas as consultas antes de serem executadas no banco de dados.

| Nome da coluna | Descrição |
| --- | --- |
| recordtime | O horário em que o evento ocorreu. |
| db | Database name. |
| usuário | User name. |
| pid | O ID do processo associado à instrução. |
| userid | ID de usuário. |
| xid | ID da transação. |

| Nome da coluna | Descrição |
| --- | --- |
| consulta | Um prefixo de LOG: depois do texto da consulta, inclusive novas linhas. |

## Habilitar o log

O registro de auditoria não é ativado por padrão no Amazon Redshift. Quando você ativa o registro em log no cluster, o Amazon Redshift exporta os logs para o Amazon CloudWatch ou cria e carrega os logs para o Amazon S3, que capturam dados desde o momento em que o registro em log de auditoria é habilitado até o momento atual. Toda atualização do registro em log é uma continuação dos logs anteriores.

O registro em log de auditoria no CloudWatch ou no Amazon S3 é um processo manual opcional. O registro em log em tabelas do sistema não é opcional e ocorre automaticamente no cluster. Para obter mais informações sobre registro em log de tabelas do sistema, consulte Referência de tabelas do sistema no Guia do desenvolvedor de banco de dados do Amazon Redshift.

O log de conexão, o log do usuário e o log de atividades do usuário são ativados juntos usando o AWS Management Console, a referência de API do Amazon Redshift ou a AWS Command Line Interface (AWS CLI). Para o log de atividade do usuário, você também deve ativar o parâmetro `enable_user_activity_logging` do banco de dados. Se você ativar somente o recurso de registro em log da auditoria, mas não o parâmetro associado, os logs de auditoria do banco de dados registrarão em log as informações somente dos logs de conexão e de usuários, mas não o log de atividades do usuário. Por padrão, o parâmetro `enable_user_activity_logging` não é habilitado (`false`). É possível defini-lo como `true` para habilitar o log de atividades do usuário. Para ter mais informações, consulte Grupos de parâmetros do Amazon Redshift.

## Enviar logs de auditoria ao Amazon CloudWatch

Quando você habilita o registro em log no CloudWatch, o Amazon Redshift exporta dados de log de conexão de cluster, usuário e atividade do usuário para um grupo de logs do Amazon CloudWatch Logs. Os dados do log não mudam com relação ao esquema. O CloudWatch foi criado para monitorar aplicações, e você pode usá-lo para realizar análise em tempo real ou configurá-lo para executar ações. Também é possível usar o Amazon CloudWatch Logs para armazenar seus registros de log em armazenamento durável.

O uso do CloudWatch para visualizar logs é uma alternativa recomendada ao armazenamento de arquivos de log no Amazon S3. Ele não requer muita configuração e pode atender aos seus requisitos de monitoramento, especialmente se você já o utiliza para monitorar outros serviços e aplicações.

Grupos de logs e eventos de log no Amazon CloudWatch

Depois de selecionar quais logs do Amazon Redshift deseja exportar, você pode monitorar eventos de log no Amazon CloudWatch Logs. Um novo grupo de logs é criado automaticamente para o Amazon Redshift sem servidor com o seguinte prefixo, em que `log_type` representa o tipo de log.

```
/aws/redshift/cluster/<cluster_name>/<log_type>
```

Por exemplo, se você optar por exportar o log de conexão, os dados de log serão armazenados no grupo de logs a seguir.

```
/aws/redshift/cluster/cluster1/connectionlog
```

Os eventos de log são exportados para um grupo de logs usando o fluxo de log. Para pesquisar informações nos eventos de log para um endpoint sem servidor, use o console do Amazon CloudWatch Logs, a AWS CLI ou a API do Amazon CloudWatch Logs. Para obter informações sobre como procurar e filtrar dados de log, consulte Criar métricas de eventos de log usando filtros.

No CloudWatch, você pode pesquisar seus dados de log com uma sintaxe de consulta que fornece granularidade e flexibilidade. Para obter mais informações, consulte Sintaxe de consulta do CloudWatch Logs Insights.

Migrar para o registro em log de auditoria do Amazon CloudWatch

Em qualquer situação em que você estiver enviando logs ao Amazon S3 e alterar a configuração, por exemplo, para enviar logs ao CloudWatch, os logs que permanecerem no Amazon S3 não serão afetados. Você ainda pode consultar os dados de log nos buckets do Amazon S3 em que eles residem.

## Gerenciar arquivos de log no Amazon S3

O número e o tamanho dos arquivos de log do Amazon Redshift no Amazon S3 dependem muito da atividade em seu cluster. Se você tiver um cluster ativo que está gerando um grande número de logs,

o Amazon Redshift pode gerar os arquivos de log com mais frequência. Você pode ter uma série de arquivos de log para o mesmo tipo de atividade, como ter vários logs de conexão na mesma hora.

Quando o Amazon Redshift usa o Amazon S3 para armazenar logs, você incorre em cobranças pelo armazenamento usado no Amazon S3. Antes de configurar o registro em log no Amazon S3, planeje por quanto tempo precisará armazenar os arquivos de log. Para isso, determine quando os arquivos de log podem ser excluídos ou arquivados com base em suas necessidades de auditoria. O plano criado depende muito do tipo de dados que você armazena, como dados sujeitos à conformidade ou requisitos regulatórios. Para obter mais informações sobre preço do Amazon S3, consulte Preço do Amazon Simple Storage Service (S3).

Limitações ao habilitar o registro no Amazon S3

O registro de auditoria tem as seguintes restrições:

- Só é possível usar criptografia (AES-256) de chaves gerenciadas pelo Amazon S3 (SSE-S3).
- Os buckets do Amazon S3 devem ter o recurso de bloqueio de objetos do S3 desativado.

Permissões de bucket para registro em log de auditoria do Amazon Redshift

Quando você ativa o registro em log no Amazon S3, o Amazon Redshift coleta informações de registro e as carrega para os arquivos de log armazenados no Amazon S3. Você pode usar um bucket existente ou um novo bucket. O Amazon Redshift requer as seguintes permissões do IAM para o bucket:

- `s3:GetBucketAcl` O serviço requer permissões de leitura para o bucket do Amazon S3 para que possa identificar o proprietário do bucket.
- `s3:PutObject` O serviço requer permissões put object para carregar os logs. Além disso, o usuário ou perfil do IAM que ativa o registro deve ter a permissão `s3:PutObject` para o bucket do Amazon S3. Sempre que o upload dos logs é feito, o serviço determina se o proprietário do bucket atual corresponde ao proprietário do bucket no momento em que o registro em log foi ativado. Se esses proprietários não corresponderem, você receberá um erro.

Se, ao habilitar o registro de auditoria, você selecionar a opção para criar um novo bucket, as permissões corretas serão aplicadas a ele. No entanto, se você criar seu próprio bucket no Amazon S3 ou usar um bucket existente, será necessário adicionar uma política de bucket que inclui o nome do bucket. Os logs são entregues usando credenciais da entidade principal do serviço. Para a

maioria das Regiões da AWS, você adiciona o nome da entidade principal do serviço do Redshift, *redshift.amazonaws.com*.

A política de bucket usa o formato a seguir. *ServiceName* e *BucketName* são espaços reservados para seus próprios valores. Especifique também as ações e os recursos associados na política de 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/*"
            ]
        }
    ]
}
```

O exemplo a seguir é uma política de bucket para a Região Leste dos EUA (Norte da Virgínia) e bucket chamado `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/*"
            ]
        }
    ]
}
```

As regiões que não estão habilitadas por padrão, também conhecidas como regiões “opt-in”, exigem um nome da entidade principal do serviço específico da região. Para isso, o nome da entidade principal do serviço inclui a região, no formato `redshift.region.amazonaws.com`. Por exemplo, *`redshift.ap-east-1.amazonaws.com`* para a região Ásia-Pacífico (Hong Kong). Para obter uma lista das regiões que não estão habilitadas por padrão, consulte Gerenciar Regiões da AWS na Referência geral da AWS.

> **Note**
>
> O nome da entidade principal do serviço específico da região corresponde à região em que o cluster está localizado.

Práticas recomendadas para arquivos de log

Quando o Redshift carrega arquivos de log para o Amazon S3, os arquivos grandes podem ser carregados em partes. Se o carregamento fracionado não for bem-sucedido, é possível que partes de um arquivo permaneçam no bucket do Amazon S3. Isso pode resultar em custos adicionais de armazenamento, por isso é importante entender o que ocorre quando um carregamento fracionado falha. Para obter uma explicação detalhada sobre carregamento fracionado para registros de auditoria, consulte Carregar e copiar objetos usando carregamento fracionado e Anular um carregamento fracionado.

Para obter mais informações sobre como criar buckets do S3 e adicionar políticas de bucket, consulte Criar um bucket e Editar permissões de bucket no Guia do usuário do Amazon Simple Storage Service.

Estrutura de bucket para registro em log de auditoria do Amazon Redshift

Por padrão, o Amazon Redshift organiza os arquivos de log no bucket do Amazon S3 usando o seguinte bucket e a seguinte estrutura de objeto:

`AWSLogs/AccountID/ServiceName/Region/Year/Month/Day/AccountID_ServiceName_Region`

Um exemplo é `AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`.

Se você fornecer um prefixo das chaves do Amazon S3, coloque o prefixo no início da chave.

Por exemplo, se você especificar um prefixo de myprefix: `myprefix/AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

O prefixo das chaves do Amazon S3 não poderá exceder 512 caracteres. Não pode conter espaços ( ), aspas duplas (“), aspas simples (‘) e barra invertida (\). Também há vários caracteres especiais e de controle que não são permitidos. Os códigos hexadecimais desses caracteres são os seguintes:

- x00 até x20
- x22
- x27
- x5c
- x7f ou maior

## Solução de problemas de registro em log de auditoria do Amazon Redshift no Amazon S3

O registro em log de auditoria do Amazon Redshift pode ser interrompido pelos seguintes motivos:

- O Amazon Redshift não tem permissão para carregar os logs no bucket do Amazon S3. Verifique se o bucket está configurado com a política do IAM correta. Para ter mais informações, consulte Permissões de bucket para registro em log de auditoria do Amazon Redshift.
- O proprietário do bucket mudou. Quando o Amazon Redshift carrega os logs, ele verifica se o proprietário do bucket é o mesmo de quando o registro em log foi habilitado. Se o proprietário do

bucket foi alterado, o Amazon Redshift não pode carregar logs até que você configure outro bucket para usar para registro em log de auditoria.

- Não foi possível encontrar o bucket. Se o bucket for excluído no Amazon S3, o Amazon Redshift não poderá carregar logs. Você precisa recriar o bucket ou configurar o Amazon Redshift para carregar logs para um bucket diferente.

## Registro em log de chamadas de API do Amazon Redshift com o AWS CloudTrail

O Amazon Redshift é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou serviço da AWS no Amazon Redshift. O CloudTrail captura todas as chamadas de API para Amazon Redshift como eventos. Para obter mais informações sobre a integração do Amazon Redshift com o AWS CloudTrail, consulte “Logging with CloudTrail” (Registro em log com o CloudTrail).

Você pode usar o CloudTrail independentemente ou além do registro em log de auditoria do banco de dados do Amazon Redshift.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

## Configurar a auditoria usando o console

Configure o Amazon Redshift para exportar dados de log de auditoria. Os logs podem ser exportados para o CloudWatch ou como arquivos para buckets do Amazon S3.

Habilitar o registro em log de auditoria usando o console

Etapas do console

Para habilitar o log de auditoria para um cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters, depois selecione o cluster que deseja atualizar.
3. Escolha a guia Properties (Propriedades). No painel Database configurations (Configurações de banco de dados), escolha Edit (Editar) e, em seguida, Edit audit logging (Editar registro em log de auditoria).
4. Na página Edit audit logging (Editar registro em log de auditoria), selecione Turn on (Ativar) e S3 bucket (Bucket do S3) ou CloudWatch. Recomendamos usar o CloudWatch porque a administração é fácil e tem recursos úteis para visualização de dados.

5. Escolha quais logs deseja exportar.
6. Escolha Save changes (Salvar alterações).

### Configurar registro em log usando a AWS CLI e a API do Amazon Redshift

Você pode usar as seguintes operações da CLI do Amazon Redshift para configurar o registro em log de auditoria:

- describe-logging-status
- disable-logging
- enable-logging

Você pode usar as seguintes operações da API do Amazon Redshift para configurar o registro em log de auditoria:

- DescribeLoggingStatus
- DisableLogging
- EnableLogging

## Registrar em log com o CloudTrail

### Registro em log de chamadas com o AWS CloudTrail

O Amazon Redshift, o compartilhamento de dados, o Amazon Redshift Serverless, a API de dados do Amazon Redshift e o editor de consultas v2 estão todos integrados ao AWS CloudTrail. O CloudTrail é um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS no Amazon Redshift. O CloudTrail captura todas as chamadas de API para Amazon Redshift como eventos. As chamadas capturadas incluem chamadas do console do Redshift e chamadas de código para as operações do Redshift.

Se você criar uma trilha do CloudTrail, poderá ter a entrega contínua de eventos do CloudTrail em um bucket do Amazon S3, inclusive eventos do Redshift. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Histórico de eventos. Usando as informações coletadas pela CloudTrail, você pode determinar certas coisas. Eles incluem a solicitação feita ao Redshift, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando foi feita e detalhes adicionais.

Você pode usar o CloudTrail independentemente ou além do registro em log de auditoria do banco de dados do Amazon Redshift.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

## Trabalhar com informações no CloudTrail

O CloudTrail é ativado na conta da AWS quando ela é criada. Quando ocorre uma atividade, ela é registrada em um evento do CloudTrail com outros eventos de serviços da AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte Trabalhar com o histórico de eventos do CloudTrail no Guia do Usuário do AWS CloudTrail.

Para um registro contínuo de eventos em sua conta da AWS, inclusive eventos para Redshift, crie uma trilha. O CloudTrail usa trilhas para entregar arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as Regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte o seguinte no Guia do usuário do AWS CloudTrail:

- Visão geral da criação de uma trilha
- Serviços e Integrações Compatíveis com CloudTrail
- Configurando Notificações Amazon SNS para CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas

Todas as ações do Amazon Redshift, do Amazon Redshift Serverless, da API de dados, de compartilhamento de dados e do editor de consultas v2 são registradas pelo CloudTrail. Por exemplo, as chamadas para as ações `AuthorizeDatashare`, `CreateNamespace`, `ExecuteStatement` e `CreateConnection` gerarão entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário da raiz ou do .
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.

- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o Elemento userIdentity do CloudTrail no Guia do usuário do AWS CloudTrail.

## Noções básicas sobre entradas de arquivos de log

Uma trilha é uma configuração que permite a entrega de eventos como registros de log a um bucket do Amazon S3 especificado. Os arquivos de log CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública, portanto não são exibidos em uma ordem específica.

## Exemplo de unidade de compartilhamento de dados do Amazon Redshift

O exemplo a seguir ilustra uma entrada de log do CloudTrail que demonstra a operação `AuthorizeDataShare`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
                "arn": "arn:aws:sts::111122223333:user/janedoe",
                "accountId": "111122223333",
                "userName": "janedoe"
            },
            "attributes": {
                "creationDate": "2021-08-02T23:40:45Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-08-02T23:40:58Z",
```

```
    "eventSource": "redshift.amazonaws.com",
    "eventName": "AuthorizeDataShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.227.36.75",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "consumerIdentifier": "555555555555"
    },
    "responseElements": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "producerNamespaceArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "producerArn": "arn:aws:redshift:us-
east-1:111122223333:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "allowPubliclyAccessibleConsumers": true,
        "dataShareAssociations": [
            {
                "consumerIdentifier": "555555555555",
                "status": "AUTHORIZED",
                "createdDate": "Aug 2, 2021 11:40:56 PM",
                "statusChangeDate": "Aug 2, 2021 11:40:57 PM"
            }
        ]
    },
    "requestID": "87ee1c99-9e41-42be-a5c4-00495f928422",
    "eventID": "03a3d818-37c8-46a6-aad5-0151803bdb09",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


## Exemplo do Amazon Redshift Serverless

O Amazon Redshift Serverless é integrado ao AWS CloudTrail para fornecer um registro das ações realizadas no Amazon Redshift Serverless. O CloudTrail captura todas as chamadas de API para Amazon Redshift Serverless como eventos. Para obter mais informações sobre os recursos do Amazon Redshift Serverless, consulte "Visão geral de recursos do Amazon Redshift Serverless".

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `CreateNamespace`.


```
{
    "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",
}
```

## Exemplos de API de dados do Amazon Redshift

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `ExecuteStatement`.

```
{
    "eventVersion":"1.05",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn":"arn:aws:sts::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
        "userName": "janedoe"
    },
    "eventTime":"2020-08-19T17:55:59Z",
    "eventSource":"redshift-data.amazonaws.com",
    "eventName":"ExecuteStatement",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"192.0.2.0",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters":{
        "clusterIdentifier":"example-cluster-identifier",
```

```
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "sql":"***OMITTED***"
    },
    "responseElements":{
        "clusterIdentifier":"example-cluster-identifier",
        "createdAt":"Aug 19, 2020 5:55:58 PM",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "id":"5c52b37b-9e07-40c1-98de-12ccd1419be7"
    },
    "requestID":"00c924d3-652e-4939-8a7a-cd0612eeb8ac",
    "eventID":"c1fb7076-102f-43e5-9ec9-40820bcc1175",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "recipientAccountId":"123456789012"
}
```

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `ExecuteStatement` mostrando o `clientToken` usado para idempotência.

```
{
    "eventVersion":"1.05",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn":"arn:aws:sts::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
        "userName": "janedoe"
    },
    "eventTime":"2020-08-19T17:55:59Z",
    "eventSource":"redshift-data.amazonaws.com",
    "eventName":"ExecuteStatement",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"192.0.2.0",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters":{
        "clusterIdentifier":"example-cluster-identifier",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "sql":"***OMITTED***",
```

```
        "clientToken":"32db2e10-69ac-4534-b3fc-a191052616ce"
    },
    "responseElements":{
        "clusterIdentifier":"example-cluster-identifier",
        "createdAt":"Aug 19, 2020 5:55:58 PM",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "id":"5c52b37b-9e07-40c1-98de-12ccd1419be7"
    },
    "requestID":"00c924d3-652e-4939-8a7a-cd0612eeb8ac",
    "eventID":"c1fb7076-102f-43e5-9ec9-40820bcc1175",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "recipientAccountId":"123456789012"
}
```

## Exemplo do Editor de Consultas v2 do Amazon Redshift

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `CreateConnection`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAKEOFPINEXAMPLE:session",
        "arn": "arn:aws:sts::123456789012:assumed-role/MyRole/session",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAKEOFPINEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/MyRole",
                "accountId": "123456789012",
                "userName": "MyRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-09-21T17:19:02Z",
                "mfaAuthenticated": "false"
            }
        }
```

```
    },
    "eventTime": "2022-09-21T22:22:05Z",
    "eventSource": "sqlworkbench.amazonaws.com",
    "eventName": "CreateConnection",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "192.2.0.2",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0)
 Gecko/20100101 Firefox/102.0",
    "requestParameters": {
        "password": "***",
        "databaseName": "***",
        "isServerless": false,
        "name": "***",
        "host": "redshift-cluster-2.c8robpbxvbf9.ca-central-1.redshift.amazonaws.com",
        "authenticationType": "***",
        "clusterId": "redshift-cluster-2",
        "username": "***",
        "tags": {
            "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
        }
    },
    "responseElements": {
        "result": true,
        "code": "",
        "data": {
            "id": "arn:aws:sqlworkbench:ca-central-1:123456789012:connection/ce56b1be-
dd65-4bfb-8b17-12345123456",
            "name": "***",
            "authenticationType": "***",
            "databaseName": "***",
            "secretArn": "arn:aws:secretsmanager:ca-
central-1:123456789012:secret:sqlworkbench!7da333b4-9a07-4917-b1dc-12345123456-qTCoFm",
            "clusterId": "redshift-cluster-2",
            "dbUser": "***",
            "userSettings": "***",
            "recordDate": "2022-09-21 22:22:05",
            "updatedDate": "2022-09-21 22:22:05",
            "accountId": "123456789012",
            "tags": {
                "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
            },
            "isServerless": false
        }
    },
```

```
    "requestID": "9b82f483-9c03-4cdd-bb49-a7009e7da714",
    "eventID": "a7cdd442-e92f-46a2-bc82-2325588d41c3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

## IDs de conta do Amazon Redshift nos logs do AWS CloudTrail

Quando o Amazon Redshift chama outro serviço da AWS para você, a chamada é registrada com uma ID de conta que pertence ao Amazon Redshift. Ela não é registrada em log com o ID de sua conta. Por exemplo, suponha que o Amazon Redshift chame operações do AWS Key Management Service (AWS KMS) como `CreateGrant`, `Decrypt`, `Encrypt` e `RetireGrant` para gerenciar a criptografia em seu cluster. Nesse caso, as chamadas são registradas em log pelo AWS CloudTrail usando uma ID de conta do Amazon Redshift.

O Amazon Redshift usa os IDs de conta na tabela a seguir ao chamar outros serviços da AWS.

| Região | Região | ID da conta |
|---|---|---|
| Região Leste dos EUA (N. da Virgínia) | us-east-1 | 368064434614 |
| Região Leste dos EUA (Ohio) | us-east-2 | 790247189693 |
| Região Oeste dos EUA (Norte da Califórnia). | us-west-1 | 703715109447 |
| Região Oeste dos EUA (Oregon) | us-west-2 | 473191095985 |
| Região África (Cidade do Cabo) | af-south-1 | 420376844563 |
| Região Ásia-Pacífico (Hong Kong) | ap-east-1 | 651179539253 |
| Ásia-Pacífico (Haiderabade) | ap-south-2 | 297058826802 |
| Região Ásia-Pacífico (Jacarta) | ap-southeast-3 | 623197973179 |

| Região | Região | ID da conta |
|---|---|---|
| Região Ásia-Pacífico (Melbourne) | ap-southeast-4 | 945512339897 |
| Região Ásia-Pacífico (Mumbai) | ap-south-1 | 408097707231 |
| Região Ásia-Pacífico (Osaka) | ap-northeast-3 | 398671365691 |
| Região Ásia-Pacífico (Seul) | ap-northeast-2 | 713597048934 |
| Região Ásia-Pacífico (Singapura) | ap-southeast-1 | 960118270566 |
| Região Ásia-Pacífico (Sydney) | ap-southeast-2 | 485979073181 |
| Região Ásia-Pacífico (Tóquio) | ap-northeast-1 | 615915377779 |
| Região Canadá (Central) | ca-central-1 | 764870610256 |
| Região Oeste do Canadá (Calgary) | ca-west-1 | 83090344646 |
| Região Europa (Frankfurt) | eu-central-1 | 434091160558 |
| Região Europa (Irlanda) | eu-west-1 | 246478207311 |
| Região Europa (Londres) | eu-west-2 | 885798887673 |
| Região Europa (Milão) | eu-south-1 | 041313461515 |
| Região Europa (Paris) | eu-west-3 | 694668203235 |
| Região Europa (Espanha) | eu-south-2 | 028811157404 |
| Região Europa (Estocolmo) | eu-north-1 | 553461782468 |
| Região Europa (Zurique) | eu-central-2 | 668912161003 |
| Região de Israel (Tel Aviv) | il-central-1 | 901883065212 |
| Região Oriente Médio (Bahrein) | me-south-1 | 051362938876 |

| Região | Região | ID da conta |
| --- | --- | --- |
| Região do Oriente Médio (Emirados Árabes Unidos) | me-central-1 | 595013617770 |
| Região América do Sul (São Paulo) | sa-east-1 | 392442076723 |

O exemplo a seguir mostra uma entrada de log do CloudTrail para a operação de Decrypt do AWS KMS que foi chamada pelo Amazon Redshift.

```
{

    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAI5QPCMKLTL4VHFCYY:i-0f53e22dbe5df8a89",
        "arn": "arn:aws:sts::790247189693:assumed-role/prod-23264-role-wp/
i-0f53e22dbe5df8a89",
        "accountId": "790247189693",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2017-03-03T16:24:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAI5QPCMKLTL4VHFCYY",
                "arn": "arn:aws:iam::790247189693:role/prod-23264-role-wp",
                "accountId": "790247189693",
                "userName": "prod-23264-role-wp"
            }
        }
    },
    "eventTime": "2017-03-03T17:16:51Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "52.14.143.61",
    "userAgent": "aws-internal/3",
```

```
    "requestParameters": {
        "encryptionContext": {
            "aws:redshift:createtime": "20170303T1710Z",
            "aws:redshift:arn": "arn:aws:redshift:us-east-2:123456789012:cluster:my-dw-
instance-2"
        }
    },
    "responseElements": null,
    "requestID": "30d2fe51-0035-11e7-ab67-17595a8411c8",
    "eventID": "619bad54-1764-4de4-a786-8898b0a7f40c",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/f8f4f94f-e588-4254-
b7e8-078b99270be7",
            "accountId": "123456789012",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012",
    "sharedEventID": "c1daefea-a5c2-4fab-b6f4-d8eaa1e522dc"

}
```

# Validação de compatibilidade do Amazon Redshift

Auditores terceirizados avaliam a segurança e a compatibilidade do Amazon Redshift como parte de vários programas de compatibilidade da AWS. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista dos serviços da AWS no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode baixar relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Download de relatórios no AWS Artifact.

Sua responsabilidade de compatibilidade ao usar o Amazon Redshift é determinada pela confidencialidade de seus dados, pelas metas de compatibilidade da sua empresa e pelas regulamentações e leis aplicáveis. Caso o uso do Amazon Redshift esteja sujeito à compatibilidade com padrões como HIPAA, PCI ou FedRAMP, a AWS fornecerá os seguintes recursos para ajudar:

- Guias de início rápido de segurança e compatibilidade que discutem as considerações de arquitetura e fornecem etapas para a implantação de ambientes de linha de base focados em compatibilidade e segurança na AWS.
- Whitepaper sobre arquitetura para compatibilidade e segurança da HIPAA, que descreve como as empresas podem usar a AWS para criar aplicações compatíveis com a HIPAA.
- Recursos de compatibilidade da AWS, uma coleção de manuais e guias que pode ser aplicada ao seu setor e à sua localização.
- AWS Config, um serviço da AWS que avalia até que ponto suas configurações de recursos atendem adequadamente a práticas internas e a diretrizes e regulamentações da indústria.
- O AWS Security Hub, um serviço da AWS, fornece uma visão completa do estado da segurança na AWS e ajuda a verificar a compatibilidade com os padrões de segurança da indústria e as práticas recomendadas. O Security Hub usa controles de segurança para avaliar configurações de recursos e padrões de segurança que ajudam você a cumprir vários frameworks de conformidade. Para obter mais informações sobre como usar o Security Hub para avaliar os recursos do Amazon Redshift, consulte Controles do Amazon Redshift no Guia do usuário do AWS Security Hub.

Os documentos de compatibilidade e segurança a seguir cobrem o Amazon Redshift e estão disponíveis sob demanda por meio do AWS Artifact. Para obter mais informações, consulte AWS Artifact.

- Cloud Computing Compliance Controls Catalogue (C5)
- ISO 27001:2013 Statement of Applicability (SoA)
- Certificado ISO 27001:2013
- ISO 27017:2015 Statement of Applicability (SoA)
- Certificado ISO 27017:2015
- ISO 27018:2015 Statement of Applicability (SoA)
- Certificado ISO 27018:2014
- Certificado ISO 9001:2015
- Certificado de Conformidade do PCI DSS (AOC) e Resumo de Responsabilidade
- Relatório Service Organization Controls (SOC) 1
- Relatório Service Organization Controls (SOC) 2
- Relatório de Confidencialidade Service Organization Controls (SOC) 2

# Resiliência no Amazon Redshift

A infraestrutura global da AWS é criada com base em regiões da AWS e zonas de disponibilidade da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta taxa de transferência e redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, com mais tolerância a falhas e mais escaláveis do que as infraestruturas com único datacenter ou infraestruturas com vários datacenters tradicionais.

Quase todas as regiões da AWS têm várias zonas de disponibilidade e datacenters. Você pode implantar suas aplicações em diversas zonas de disponibilidade na mesma região para tolerância de falha e baixa latência.

Para mover um cluster para outra zona de disponibilidade sem perda de dados ou alterações em suas aplicações, é possível configurar a realocação para o cluster. Com a realocação, você pode continuar as operações quando houver uma interrupção do serviço em seu cluster com impacto mínimo. Quando a realocação de cluster está ativada, o Amazon Redshift pode optar por realocar clusters em algumas situações. Para obter mais informações sobre a realocação no Amazon Redshift, consulte Realocar um cluster.

Em cenários de falha quando ocorre um evento inesperado em uma zona de disponibilidade, é possível configurar uma implantação (multi-AZ) de várias zonas de disponibilidade para garantir que o data warehouse do Amazon Redshift possa continuar operando. O Amazon Redshift implanta recursos computacionais iguais em duas zonas de disponibilidade que podem ser acessadas por meio de um único endpoint. Em caso de falha em uma zona de disponibilidade inteira, os recursos computacionais restantes na segunda zona de disponibilidade estarão disponíveis para continuar processando as workloads. Para obter mais informações sobre implantações Multi-AZ, consulte Configuração da implantação multi-AZ.

Para obter mais informações sobre as regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

# Segurança da infraestrutura no Amazon Redshift

Como serviço gerenciado, o Amazon Redshift é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a

infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar segurança: AWS Well-Architected Framework.

Você usa as chamadas de API publicadas da AWS para acessar o Amazon Redshift por meio da rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

## Isolamento de rede

Uma nuvem privada virtual (VPC) baseada no serviço Amazon VPC é sua rede privada e logicamente isolada na Nuvem AWS. Você pode implantar um cluster do Amazon Redshift dentro de uma VPC seguindo estas etapas:

- Crie um VPC em uma região da AWS. Para obter mais informações, consulte O que é o Amazon VPC? no Manual do usuário do Amazon VPC.
- Crie duas ou mais sub-redes de VPC privadas. Para obter mais informações, consulte VPCs e sub-redes no Manual do usuário do Amazon VPC.
- Implante um cluster do Amazon Redshift. Para obter mais informações, consulte Grupos de sub-rede de cluster do Amazon Redshift.

Um cluster do Amazon Redshift é bloqueado por padrão no provisionamento. Para permitir o tráfego de rede de entrada de clientes do Amazon Redshift, associe um grupo de segurança da VPC a um cluster do Amazon Redshift. Para obter mais informações, consulte Grupos de sub-rede de cluster do Amazon Redshift.

Para permitir tráfego somente de e para intervalos específicos de endereços IP, atualize os grupos de segurança com sua VPC. Um exemplo é permitir tráfego somente de e para sua rede corporativa.

Ao configurar listas de controle de acesso associadas às sub-redes com que o cluster do Amazon Redshift está marcado, verifique se os respectivos intervalos CIDR do S3 da Região da AWS estão adicionados à lista de permissões para regras de entrada e saída. Isso permite que você execute operações baseadas em S3, como Redshift Spectrum, COPY e UNLOAD, sem interrupções.

O exemplo de comando a seguir analisa a resposta JSON de todos os endereços IPv4 usados no Amazon S3, na região 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
```

Para obter instruções sobre como obter intervalos de IP do S3 para uma região específica, consulte Intervalos de endereços IP da AWS.

O Amazon Redshift oferece suporte à implantação de clusters em VPCs de locação dedicadas. Para obter mais informações, consulte Instâncias dedicadas no Guia do usuário do Amazon EC2.

## Grupos de segurança de clusters do Amazon Redshift

Quando você provisiona um cluster do Amazon Redshift, ele é bloqueado por padrão para que ninguém tenha acesso a ele. Para conceder a outros usuários acesso de entrada a um cluster do Amazon Redshift, você associa o cluster a um grupo de segurança. Se você estiver na plataforma EC2-VPC, poderá usar um grupo de segurança Amazon VPC existente ou definir um novo e associá-lo a um cluster. Para obter mais informações sobre o gerenciamento de um cluster na plataforma EC2-VPC, consulte Gerenciamento de clusters em uma VPC.

Se estiver na plataforma EC2-Classic, você vai definir um security group de cluster e associá-lo a um cluster. A plataforma EC2-Classic será retirada. Recomendamos que você execute o cluster em uma plataforma EC2-VPC, em vez de uma plataforma EC2-Classic. No entanto, você pode restaurar um snapshot EC2-Classic para um cluster EC2-VPC usando o console do Amazon Redshift. Para mais informações, consulte Restauração de um cluster usando um snapshot.

# Conectar ao Amazon Redshift usando um endpoint da interface da VPC

Você pode se conectar diretamente ao serviço de API do Amazon Redshift usando um endpoint da interface da VPC (AWS PrivateLink) em sua nuvem privada virtual (VPC) em vez de se conectar pela Internet. Para obter mais informações sobre as ações de API do Amazon Redshift, consulte Ações na Referência de API do Amazon Redshift. Para obter mais informações sobre AWS PrivateLink, consulte Endpoints da interface da VPC (AWS PrivateLink) no Manual do usuário do Amazon VPC. Observe que a conexão JDBC/ODBC com o cluster não faz parte do serviço de API do Amazon Redshift.

Quando você usa um endpoint da interface da VPC, a comunicação entre seu VPC e o Amazon Redshift é conduzida inteiramente dentro da rede da AWS, o que pode fornecer maior segurança. Cada VPC endpoint é representado por uma ou mais interfaces de rede elástica com endereços IP privados em suas sub-redes da VPC. Para obter mais informações sobre interfaces de rede elástica, consulte Interfaces de rede elástica no Manual do usuário do Amazon EC2 para instâncias do Linux.

Um endpoint da interface da VPC conecta sua VPC diretamente ao Amazon Redshift. Ele não usa um gateway da Internet, um dispositivo de conversão de endereço de rede (NAT), uma conexão de rede privada virtual (VPN) ou conexão AWS Direct Connect. As instâncias em sua VPC não precisam de endereços IP públicos para se comunicarem com a API do Amazon Redshift.

Para usar o Amazon Redshift por meio da VPC, você tem duas opções. Um deles é conectar a partir de uma instância que esteja dentro da VPC. O outro é conectar sua rede privada à sua VPC usando uma opção de AWS VPN ou do AWS Direct Connect. Para obter mais informações sobre opções de AWS VPN, consulte Conexões VPN no Manual do usuário do Amazon VPC. Para obter informações sobre o AWS Direct Connect, consulte Criação de uma conexão, no Manual do usuário do AWS Direct Connect.

É possível criar um endpoint da interface da VPC para se conectar ao Amazon Redshift usando o AWS Management Console ou os comandos da AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Criação de um endpoint de interface.

Depois de criar um endpoint da interface da VPC, você poderá habilitar nomes de host DNS privados para o endpoint. Quando você fizer isso, o endpoint padrão do Amazon Redshift (`https://redshift.Region.amazonaws.com`) resolve para o endpoint da VPC.

Se você não habilitar nomes de host DNS privados, o Amazon VPC fornece um nome de endpoint do DNS que você pode usar no formato a seguir.

```
VPC_endpoint_ID.redshift.Region.vpce.amazonaws.com
```

Para obter mais informações, consulte Endpoints da interface da VPC(AWS PrivateLink) no Manual do usuário do Amazon VPC.

O Amazon Redshift oferece suporte a chamadas para todas as suas Operações de API dentro de sua VPC.

É possível anexar políticas de endpoint da VPC a um endpoint da VPC para controlar o acesso aos principais do AWS Identity and Access Management (IAM). Também é possível associar grupos de segurança a um endpoint da VPC para controlar o acesso de entrada e saída com base na origem e no destino do tráfego de rede. Um exemplo é um intervalo de endereços IP. Para obter mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Manual do usuário da Amazon VPC.

## Criar uma política de endpoint da VPC para o Amazon Redshift

Você pode criar uma política de endpoints da VPC para Amazon Redshift para especificar o seguinte:

- O principal que pode ou não executar ações
- As ações que podem ser executadas
- Os recursos nos quais as ações podem ser executadas

Para obter mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Veja a seguir exemplos de políticas de endpoint da VPC.

Tópicos

- Exemplo: política de endpoint da VPC que nega todo o acesso de uma conta da AWS especificada
- Exemplo: política de endpoint da VPC para permitir o acesso à VPC apenas a um perfil do IAM especificado
- Exemplo: política de endpoint da VPC para permitir o acesso ao VPC apenas a um principal IAM especificado (usuário)
- Exemplo: política de endpoint da VPC para permitir operações somente leitura do Amazon Redshift

- Exemplo: política de endpoint da VPC negando acesso a um cluster especificado

Exemplo: política de endpoint da VPC que nega todo o acesso de uma conta da AWS especificada

A política de endpoint da VPC a seguir nega o *123456789012* da conta da AWS todo o acesso aos recursos que usam este endpoint.

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Exemplo: política de endpoint da VPC para permitir o acesso à VPC apenas a um perfil do IAM especificado

A política de endpoint da VPC a seguir permite acesso total somente ao perfil do IAM *redshiftrole* na conta da AWS *123456789012*. Todos os outros principais IAM têm acesso negado usando o endpoint.

```
   {
    "Statement": [
        {
```

```
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:role/redshiftrole"
                ]
            }
        }]
}
```

Isso é apenas um exemplo. Na maioria dos casos de uso, recomendamos anexar permissões para ações específicas a fim de restringir o escopo das permissões.

Exemplo: política de endpoint da VPC para permitir o acesso ao VPC apenas a um principal IAM especificado (usuário)

A política de endpoint da VPC a seguir permite acesso total somente ao usuário do IAM *redshiftadmin* na conta da AWS *123456789012*. Todos os outros principais IAM têm acesso negado usando o endpoint.

```
   {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:user/redshiftadmin"
                ]
            }
        }]
}
```

Isso é apenas um exemplo. Na maioria dos casos de uso, recomendamos anexar permissões a um perfil antes de atribuí-lo a um usuário. Além disso, recomendamos o uso de ações específicas para restringir o escopo das permissões.

Exemplo: política de endpoint da VPC para permitir operações somente leitura do Amazon Redshift

A política de endpoint da VPC a seguir permite que apenas a conta da AWS *123456789012* execute as ações especificadas do Amazon Redshift.

As ações especificadas fornecem o equivalente ao acesso somente leitura para o Amazon Redshift. Todas as outras ações na VPC serão negadas para a conta especificada. Além disso, todas as outras contas têm acesso negado. Para obter uma lista de ações do Amazon Redshift, consulte Ações, recursos e chaves de condição do Amazon Redshift no Manual do usuário do 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"
                ]
            }
        }
    ]
}
```

Exemplo: política de endpoint da VPC negando acesso a um cluster especificado

A política de endpoint da VPC a seguir permite acesso total a todas as contas e principais. Ao mesmo tempo, nega qualquer acesso para a conta da AWS *123456789012* em ações executadas no cluster do Amazon Redshift com ID de cluster *my-redshift-cluster*. Outras ações do Amazon Redshift que não oferecem suporte a permissões de nível de recurso para clusters ainda são permitidas. Para obter uma lista de ações do Amazon Redshift e seu tipo de recurso correspondente, consulte Ações, recursos e chaves de condição do Amazon Redshift no Manual do usuário do 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"
                ]
            }
```

```
        }
    ]
}
```

# Análise de configuração e vulnerabilidade no Amazon Redshift

A AWS se encarrega das tarefas básicas de segurança, como aplicação de patches a bancos de dados e sistemas operacionais (SOs) convidados, configuração de firewalls e recuperação de desastres (DR). Esses procedimentos foram revisados por terceiros certificados. Para obter mais informações, consulte Validação de compatibilidade do Amazon Redshift, o Modelo de responsabilidade compartilhada e Práticas recomendadas de segurança, identidade e compatibilidade.

O Amazon Redshift aplica atualizações e patches automaticamente ao seu data warehouse para que você possa se concentrar na aplicação, e não na administração dele. Os patches e as atualizações são aplicados durante uma janela de manutenção configurável. Para obter mais informações, consulte . Janelas de manutenção.

O editor de consultas v2 do Amazon Redshift é uma aplicação gerenciada pela AWS. Todos os patches e atualizações são aplicados pela AWS conforme necessário.

# Tarefas de rede

Você pode realizar tarefas de rede, como personalizar sua conexão com um banco de dados do Redshift. Também é possível executar tarefas relacionadas ao DNS, como configurar um nome de domínio personalizado. Essas tarefas de configuração são disponibilizadas quando você tem um cluster provisionado pelo Amazon Redshift ou com um grupo de trabalho do Amazon Redshift sem servidor.

Tópicos


- Usar um nome de domínio personalizado para conexões de clientes
- Trabalhando com endpoints da VPC gerenciados por Redshift
- Roteamento aprimorado da VPC no Amazon Redshift


## Usar um nome de domínio personalizado para conexões de clientes

Você pode criar um nome de domínio personalizado, também conhecido como URL personalizado, tanto para o cluster do Amazon Redshift quanto para o grupo de trabalho do Amazon Redshift sem servidor. Trata-se de um registro DNS fácil de ler que roteia conexões do cliente SQL para o endpoint. Você pode configurá-lo para um cluster ou grupo de trabalho existente a qualquer momento. Ele oferece vários benefícios:

- O nome de domínio personalizado é uma string mais simples do que o URL padrão, que normalmente inclui o nome do cluster ou o nome do grupo de trabalho e a região. É mais fácil de lembrar e usar.
- Você pode rotear rapidamente o tráfego para um novo cluster ou grupo de trabalho em um caso de failover, por exemplo. Dessa forma, os clientes não precisam fazer alterações na configuração ao se reconectarem. As conexões podem ser redirecionadas centralmente, com o mínimo de interrupção.
- Você pode evitar o compartilhamento de informações privadas, como o nome de um servidor em um URL de conexão. Você pode ocultá-las em um URL personalizado.

Quando se configura um nome de domínio personalizado usando um CNAME, não há nenhuma cobrança adicional do Amazon Redshift. Você poderá receber uma cobrança do provedor de

DNS por um nome de domínio, se criar um, mas esse custo geralmente é baixo. Para obter mais informações, consulte Configurar um nome de domínio personalizado.

## Segurança para um nome de domínio personalizado

O Amazon Redshift ou o Amazon Redshift sem servidor exige um certificado Secure Sockets Layer (SSL) validado para um endpoint personalizado a fim de manter a segurança da comunicação e verificar a propriedade do nome do domínio. É possível usar sua conta do AWS Certificate Manager com uma AWS KMS key para gerenciamento seguro de certificados. A validação de segurança inclui a verificação completa do nome do host (sslmode=verify-full).

### Renovação de um certificado

As renovações de certificado são gerenciadas pelo Amazon Redshift somente quando você escolhe a validação de DNS, em vez da validação por e-mail. Se você usar a validação por e-mail, poderá usar o certificado, mas deverá realizar a renovação por conta própria, antes da expiração. Recomendamos que você escolha a validação de DNS para o certificado. É possível monitorar as datas de expiração dos certificados importados no AWS Certificate Manager.

## Configurar um nome de domínio personalizado

A configuração do nome de domínio personalizado consiste em diversas tarefas: entre elas está o registro do nome de domínio com o provedor DNS e a criação de um certificado. Depois de realizar essas partes do trabalho, você vai configurar o nome de domínio personalizado no console do Amazon Redshift ou no console do Amazon Redshift sem servidor ou configurá-lo com comandos AWS CLI. As seções a seguir detalham as etapas.

### Registrar um nome de domínio e escolher um certificado

É necessário ter um nome de domínio da internet registrado para configurar um nome de domínio personalizado no Amazon Redshift. Você pode registrar um domínio da internet usando o Route 53 ou um provedor de registro de domínios de terceiros. Você conclui essas tarefas fora do console do Amazon Redshift. Domínio registrado é um pré-requisito para concluir os procedimentos restantes a fim de criar um domínio personalizado.

> **Note**
>
> Se você estiver usando um cluster provisionado, antes de realizar as etapas para configurar o nome de domínio personalizado, ele deverá ter a realocação habilitada. Para obter mais

informações, consulte Realocar um cluster. Esta etapa não é necessária para o Amazon Redshift sem servidor.

O nome de domínio personalizado geralmente inclui o domínio raiz e um subdomínio, como `mycluster.example.com`. Para configurá-lo, execute as seguintes etapas:

Crie uma entrada DNS CNAME para o nome de domínio personalizado

1. Registre um domínio raiz, por exemplo `example.com`. Se preferir, use um domínio em vigor. O nome personalizado pode ser limitado por restrições de caracteres específicos ou por outras validações de nomenclatura. Para obter mais informações sobre como registrar um domínio com o Route 53, consulte Registrar um novo domínio.
2. Adicione um registro DNS CNAME apontando o nome de domínio personalizado para o endpoint do Redshift para o cluster ou o grupo de trabalho. Você pode encontrar o endpoint nas propriedades do cluster ou do grupo de trabalho, no console do Redshift ou no console do Amazon Redshift sem servidor. Copie o URL do JDBC disponível nas propriedades do cluster ou do grupo de trabalho, em Informações gerais. Os URLs têm a seguinte aparência:

   - Para um cluster do Amazon Redshift: `redshift-cluster-sample.abc123456.us-east-1.redshift.amazonaws.com`
   - Para um grupo de trabalho do Amazon Redshift sem servidor: `endpoint-name.012345678901.us-east-1-dev.redshift-serverless-dev.amazonaws.com`

   Se o URL tiver um prefixo JDBC, remova-o.

   > **Note**
   >
   > Os registros DNS estão sujeitos à disponibilidade, pois cada nome deve ser exclusivo e estar disponível para uso na organização.

Limitações

Existem algumas restrições em relação à criação de registros CNAME para um domínio personalizado:

- A criação de vários nomes de domínio personalizados para o mesmo cluster provisionado ou o grupo de trabalho do Amazon Redshift sem servidor não é compatível. Você só pode associar um registro CNAME.
- A associação de um registro CNAME com mais de um cluster ou grupo de trabalho não é compatível. O CNAME de cada recurso do Redshift deve ser exclusivo.

Depois de registrar o domínio e criar o registro CNAME, você seleciona um certificado novo ou em vigor. Você executa essa etapa usando o AWS Certificate Manager:

Solicitar um certificado do ACM para um nome de domínio

1. Faça login no AWS Management Console e abra o console do ACM em https://console.aws.amazon.com/acm/.
2. Selecione Request a certificate.
3. Insira o nome de domínio personalizado no campo Nome de domínio.

   > **Note**
   >
   > É possível especificar vários prefixos, além do domínio do certificado, a fim de usar um único certificado para vários registros de domínio personalizado. Para ilustrar, você pode usar registros adicionais, como `one.example.com`, `two.example.com`, ou um registro DNS curinga como `*.example.com`, com o mesmo certificado.

4. Escolha Review and request.
5. Escolha Confirm and request.
6. Para uma solicitação válida, um proprietário registrado do domínio da Internet deve concordar com a solicitação antes que o ACM emita o certificado. O status deve aparecer como Emitido no console do ACM quando você concluir as etapas.

É recomendável criar um certificado validado por DNS que atenda à elegibilidade para renovação gerenciada, disponível com AWS Certificate Manager. Renovação gerenciada indica que o ACM vai renovar automaticamente os certificados ou enviar avisos por e-mail quando a expiração da validade estiver se aproximando. Para obter mais informações, consulte Managed renewal for ACM certificates.

## Criar o domínio personalizado

Você pode usar o console do Amazon Redshift ou do Amazon Redshift sem servidor para criar o URL de domínio personalizado. Se você não o configurou, a propriedade de Nome de domínio personalizado aparece como um traço (–) em Informações gerais. Depois de criar o registro CNAME e o certificado, você vai atribuir o nome de domínio personalizado para o cluster ou o grupo de trabalho.

Para criar uma associação de domínio personalizada, as seguintes permissões do IAM são obrigatórias:

- `redshift:CreateCustomDomainAssociation`: é possível restringir a permissão a um cluster específico adicionando seu ARN.
- `redshiftServerless:CreateCustomDomainAssociation`: você pode restringir a permissão a um grupo de trabalho específico adicionando o ARN.
- `acm:DescribeCertificate`

Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.

Você atribui o nome de domínio personalizado executando as etapas a seguir.

1. Escolha o cluster no console do Redshift ou o grupo de trabalho no console do Amazon Redshift sem servidor e escolha Criar nome de domínio personalizado no menu Ação. Uma caixa de diálogo é exibida.
2. Digite o nome de domínio personalizado.
3. Selecione o ARN do AWS Certificate Manager para o certificado do ACM. Confirme as alterações. De acordo com as orientações nas etapas que você seguiu para criar o certificado, é recomendável escolher um certificado validado por DNS que seja elegível para renovação gerenciada por meio do AWS Certificate Manager.
4. Verifique nas propriedades do cluster se o Nome de domínio personalizado e o ARN do certificado de domínio personalizado estão preenchidos com seus dados. A Data de validade do certificado de domínio personalizado também está listada.

Depois que o domínio personalizado for configurado, o uso de `sslmode=verify-full` só vai funcionar para o novo domínio personalizado. Não funciona para o endpoint padrão.

No entanto, você ainda pode se conectar ao endpoint padrão usando outros modos ssl, como `sslmode=verify-ca`.

Renomear um cluster que tem um domínio personalizado atribuído usando o console

> **Note**
>
> Essa série de etapas não se aplica a um grupo de trabalho do Amazon Redshift sem servidor. Você não pode alterar o nome do grupo de trabalho.

Para renomear um cluster que tenha um nome de domínio personalizado, é necessária a permissão `acm:DescribeCertificate` do IAM.

1. Acesse o console do Amazon Redshift e escolha o cluster cujo nome você deseja alterar. Escolha Editar para editar as propriedades do cluster.
2. Edite o Identificador do cluster. Também é possível alterar outras propriedades do cluster. Em seguida, escolha Salvar alterações.
3. Depois de renomear o cluster, você precisará atualizar o registro DNS para alterar a entrada CNAME do domínio personalizado e apontar para o endpoint atualizado do Amazon Redshift.

Atualização do registro CNAME em um caso de uso de recuperação de desastres

O uso de um registro CNAME para criar um domínio personalizado pode ser útil em um caso de recuperação de desastres. Se você não conseguir acessar o data warehouse, o procedimento a seguir detalha as ações que você poderá tomar quando não conseguir acessar o cluster do banco de dados ou o grupo de trabalho primário.

Presumimos que você siga práticas de alta disponibilidade e tenha recursos secundários disponíveis. Nesse caso, por exemplo, você pode ter um cluster ou um grupo de trabalho em espera quente disponível que receba regularmente dados restaurados do cluster primário. Esse data warehouse de backup pode estar em outra zona de disponibilidade AWS ou em uma região à parte. Você pode redirecionar clientes para ele concluindo as seguintes etapas:

1. Esta etapa pressupõe que o cluster ou o grupo de trabalho esteja disponível no console. Se não estiver, você poderá ignorá-lo: escolha o cluster primário no console do Amazon Redshift ou o grupo de trabalho primário no console do Amazon Redshift sem servidor. O nome de domínio

personalizado é exibido nas propriedades. Escolha Excluir nome de domínio personalizado no menu Ações. Na janela exibida, digite delete para confirmar e escolha Excluir.

2. Escolha o novo cluster ou grupo de trabalho. Siga as etapas deste tópico para criar um nome de domínio personalizado. Use o mesmo nome de domínio e selecione o mesmo registro CNAME usado no cluster ou no grupo de trabalho primário. Se o recurso secundário estiver em uma nova região, você deverá criar e usar um novo certificado.
3. Vá até o provedor de registro de domínio. Pode ser Route 53 ou um provedor de terceiros. Selecione o registro CNAME criado originalmente por você. Quando criou o registro, você o configurou a fim de rotear tráfego para o URL do endpoint do cluster ou do grupo de trabalho primário. Altere o valor para o URL do endpoint do cluster ou do grupo de trabalho em espera. Depois de você salvar a alteração, ela vai rotear o tráfego para o novo recurso. Talvez seja necessário aguardar a propagação do DNS.
4. Esta é uma etapa opcional: altere as regras do tráfego de rede do grupo de segurança de entrada e saída a fim de rotear o tráfego para o cluster ou o grupo de trabalho em espera. Além disso, quando ativa o recurso em espera, pressupõe-se que você já tenha executado ou planeja executar operações de restauração para alinhar os dados em espera com os dados de produção.

Uma vantagem de alterar o valor do URL do endpoint para redirecionar o tráfego é que não existem alterações na configuração necessárias para clientes que usem o nome de domínio personalizado. As propriedades de conexão não precisam mudar.

Todas as etapas da recuperação de desastres seguidas por você devem se adequar ao plano de disponibilidade existente. Outras estratégias de resiliência, como a implantação de recursos em várias regiões ou técnicas de backup sofisticadas, estão além do escopo deste documento.

> **Note**
>
> Como lembrete, a realocação do cluster não é um pré-requisito para configurar recursos de rede do Redshift adicionais, como os usados na recuperação de desastres ou para outros fins. Você não precisa ativá-la para permitir o seguinte:
>
> - Conexão de uma VPC entre contas ou regiões ao Redshift: você pode se conectar a partir de uma nuvem privada virtual (VPC) da AWS a outra que contenha um banco de dados do Redshift. Isso facilita o gerenciamento, por exemplo, do acesso do cliente a partir de contas ou VPCs diferentes, sem precisar dar acesso local à VPC para identidades

conectadas ao banco de dados. Para obter mais informações, consulte Connecting to Amazon Redshift Serverless from a Redshift VPC endpoint in another account or region.

- Configuração de um nome de domínio personalizado: você pode criar um nome de domínio personalizado, conforme descrito neste tópico, para deixar o nome do endpoint mais relevante e simples.

Descrever associações de domínio personalizadas usando comandos de CLI

Use os comandos nesta seção para obter uma lista de nomes de domínio personalizados associados a um cluster provisionado específico ou a um grupo de trabalho do Amazon Redshift sem servidor.

Você precisa das seguintes permissões:

- Para um cluster provisionado: `redshift:DescribeCustomDomainAssociations`
- Para um grupo de trabalho do Amazon Redshift sem servidor: `redshiftServerless:ListCnameAssociations`

Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.

Este é um comando de exemplo para listar os nomes de domínio personalizados para um determinado cluster do Amazon Redshift:

```
aws redshift describe-custom-domain-association --cluster-id redshiftclustersample --
custom-domain-name customdomainname
```

Você poderá executar esse comando quando tiver um nome de domínio personalizado habilitado para determinar os nomes de domínio personalizados associados ao cluster. Para obter mais informações sobre o comando CLI para descrever associações de domínio personalizadas, consulte describe-custom-domain-association.

Da mesma forma, este é um comando de exemplo para listar os nomes de domínio personalizados para um determinado grupo de trabalho do Amazon Redshift sem servidor: Existem algumas maneiras diferentes de fazer isso. Você só pode fornecer o nome de domínio personalizado:

```
aws redshift-serverless list-cname-associations --custom-domain-
name customdomainnamesample
```

Você também pode obter as associações fornecendo apenas o nome do grupo de trabalho:

```
aws redshift-serverless list-cname-associations --workgroup-name workgroupnamesample
```

Você também pode obter as associações fornecendo apenas o ARN do certificado:

```
aws redshift-serverless list-cname-associations --custom-certificate-
arn certificatearnsample
```

Você poderá executar esses comandos quando tiver um nome de domínio personalizado habilitado para determinar os nomes de domínio personalizados associados ao grupo de trabalho. Você também pode executar um comando para obter as propriedades de uma associação de domínio personalizada. Para isso, você deve fornecer o nome de domínio personalizado e o nome do grupo de trabalho como parâmetros. Ele retorna o ARN do certificado, o nome do grupo de trabalho e o tempo de expiração do certificado do domínio personalizado:

```
aws redshift-serverless get-custom-domain-association --workgroup-
name workgroupnamesample --custom-domain-name customdomainnamesample
```

Para obter mais informações sobre comandos de referência da CLI disponíveis para o Amazon Redshift sem servidor, consulte redshift-serverless.

Associação do domínio personalizado a um certificado diferente

Para criar a associação de certificado para um nome de domínio personalizado, as seguintes permissões do IAM são obrigatórias:

- `redshift:ModifyCustomDomainAssociation`
- `acm:DescribeCertificate`

Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.

Use o comando a seguir para associar o domínio personalizado a um certificado diferente. Os argumentos `custom-domain-certificate-arn` e `--custom-domain-name` são obrigatórios. O ARN do novo certificado deve ser diferente do ARN existente.

```
aws redshift modify-custom-domain-association --cluster-id redshiftclustersample --
custom-domain-name customdomainnamesample --custom-domain-certificate-arn ARNsample
```

O exemplo a seguir mostra como associar o domínio personalizado a um certificado diferente para um grupo de trabalho do Amazon Redshift sem servidor.

```
aws redshift-serverless modify-custom-domain-association --workgroup-
name redshiftworkgroupsample --custom-domain-name customdomainnamesample --custom-
domain-certificate-arn ARNsample
```

Há um atraso máximo de 30 segundos até você conseguir se conectar ao cluster. Parte desse atraso ocorre quando o cluster do Amazon Redshift atualiza suas propriedades, e há um atraso adicional à medida que o DNS é atualizado. Para obter mais informações sobre a API e cada configuração de propriedade, consulte ModifyCustomDomainAssociation.

Exclusão do domínio personalizado

Para excluir o nome de domínio personalizado, o usuário deve ter permissões para as seguintes ações:

- Para um cluster provisionado: `redshift:DeleteCustomDomainAssociation`
- Para um grupo de trabalho do Amazon Redshift sem servidor: `redshiftServerless:DeleteCustomDomainAssociation`

No console

Você pode excluir o nome de domínio personalizado selecionando o botão Ações e escolhendo Excluir nome de domínio personalizado. Depois de fazer isso, você ainda conseguirá se conectar ao servidor atualizando as ferramentas para usar os endpoints listados no console.

Uso de um comando da CLI

O exemplo a seguir mostra como excluir o nome de domínio personalizado. A operação de exclusão exige que você forneça o nome de domínio personalizado existente para o cluster.

```
aws redshift delete-custom-domain-association --cluster-id redshiftclustersample --
custom-domain-name customdomainnamesample
```

O exemplo a seguir mostra como excluir o nome de domínio personalizado para um grupo de trabalho do Amazon Redshift sem servidor. O nome de domínio personalizado é um parâmetro obrigatório.

```
aws redshift-serverless delete-custom-domain-association --workgroup-name workgroupname
 --custom-domain-name customdomainname
```

Para obter mais informações, consulte DeleteCustomDomainAssociation.

## Conectar-se ao cluster ou ao grupo de trabalho com um nome de domínio personalizado usando um cliente SQL

Para se conectar a um nome de domínio personalizado, as seguintes permissões do IAM são obrigatórias para um cluster provisionado: `redshift:DescribeCustomDomainAssociations` Para o Amazon Redshift sem servidor, você não precisa adicionar permissões.

Como prática recomendada, anexe políticas de permissões a um perfil do IAM e, depois, atribua-as a usuários e grupos, conforme necessário. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Redshift.

Depois de concluir as etapas para criar o CNAME e atribuí-lo ao cluster ou ao grupo de trabalho no console, você poderá fornecer o URL personalizado nas propriedades de conexão do cliente SQL. Pode haver um atraso na propagação do DNS imediatamente após a criação de um registro CNAME.

1. Abra um cliente SQL. Por exemplo, você pode usar SQL/Workbench J. Abra as propriedades de uma conexão e adicione o nome de domínio personalizado para a string de conexão. Por exemplo, `jdbc:redshift://mycluster.example.com:5439/dev?sslmode=verify-full`. Neste exemplo, `dev` especifica o banco de dados padrão.
2. Adicione o Nome de usuário e a Senha do usuário do banco de dados.
3. Teste a conexão. A possibilidade de consultar recursos do banco de dados, como tabelas específicas, pode variar com base nas permissões concedidas ao usuário do banco de dados ou às funções de banco de dados do Amazon Redshift atribuídas.

   Talvez você precise definir o cluster ou o grupo de trabalho como acessível publicamente para se conectar a ele, caso ele esteja em uma VPC. É possível alterar essa configuração nas propriedades da rede.

> **Note**
>
> As conexões com um nome de domínio personalizado são compatíveis com drivers JDBC e Python. As conexões ODBC não são compatíveis.

# Trabalhando com endpoints da VPC gerenciados por Redshift

Por padrão, um cluster do Amazon Redshift ou um grupo de trabalho do Amazon Redshift sem servidor é provisionado em uma nuvem privada virtual (VPC). A VPC pode ser acessada por meio de outra VPC ou sub-rede quando você permite acesso público ou configura um gateway da internet, um dispositivo NAT ou uma conexão do AWS Direct Connect para rotear o tráfego para ela. Ou você pode acessar um cluster ou grupo de trabalho configurando um endpoint da VPC gerenciado pelo Redshift (habilitado pelo AWS PrivateLink).

É possível configurar um endpoint da VPC gerenciado pelo Redshift como uma conexão privada entre uma VPC que contém um cluster ou grupo de trabalho e uma VPC em que uma ferramenta cliente está sendo executada. Se o cluster ou grupo de trabalho estiver em outra conta, o proprietário da conta (concessor) precisará conceder acesso à conta que está estabelecendo conexão (favorecida). Com essa abordagem, você pode acessar o data warehouse sem usar um endereço IP público ou rotear tráfego pela internet.

Estes são os motivos comuns para permitir o acesso usando um endpoint da VPC gerenciado pelo Redshift:

- Uma conta A da AWS deseja permitir que uma VPC em uma conta B da AWS tenha acesso a um cluster ou grupo de trabalho.
- Uma conta A da AWS deseja permitir que uma VPC que também está na conta A da AWS tenha acesso a um cluster ou grupo de trabalho.
- A conta A da AWS deseja permitir que uma sub-rede diferente na VPC dentro da conta A da AWS tenha acesso a um cluster ou grupo de trabalho.

O fluxo de trabalho para configurar um endpoint da VPC gerenciado pelo Redshift para acessar um cluster ou grupo de trabalho em outra conta é o seguinte:

1. A conta de proprietário concede autorização de acesso a outra conta e especifica o ID da conta da AWS e o identificador da VPC (ou de todas as VPCs) do favorecido.

2. A conta do favorecido é notificada de que eles têm permissão para criar um endpoint da VPC gerenciado por Redshift.
3. A conta do favorecido cria um endpoint da VPC gerenciado por Redshift.
4. A conta do favorecido acessa o cluster ou grupo de trabalho da conta do proprietário usando o endpoint da VPC gerenciado pelo Redshift.

Você pode fazer isso usando o console do Amazon Redshift, a AWS CLI ou a API do Amazon Redshift.

## Considerações ao usar endpoints da VPC gerenciados por Redshift

> **Note**
>
> Para criar ou modificar endpoints da gerenciados pelo Redshift, você precisa da permissão `ec2:CreateVpcEndpoint` ou `ec2:ModifyVpcEndpoint` na política do IAM, além de outras permissões especificadas na política `AmazonRedshiftFullAccess` gerenciada pela AWS.

Ao usar endpoints da VPC gerenciados pelo Redshift, lembre-se do seguinte:

- Certifique-se de que o cluster a ser acessado é um tipo de nó RA3. Um grupo de trabalho do Amazon Redshift sem servidor também trabalha para isso.
- Para clusters provisionados, o cluster a ser acessado dever ter a realocação de cluster ativada. Para obter informações sobre os requisitos para ativar a realocação de cluster, consulte Realocar um cluster.
- Verifique se o cluster ou grupo de trabalho a ser acessado por meio do respectivo grupo de segurança está disponível nos intervalos de portas válidos 5431-5455 e 8191-8215. O padrão é 5439.
- Você pode modificar os grupos de segurança da VPC associados a um endpoint da VPC gerenciado por Redshift existente. Para modificar outras configurações, exclua o endpoint da VPC gerenciado pelo Redshift atual e crie um novo.
- O número de endpoints da VPC gerenciados por Redshift que você pode criar está limitado à cota de endpoint da VPC.
- Os endpoints da VPC gerenciados por Redshift não são acessíveis pela Internet. Um endpoint da VPC gerenciado pelo Redshift é acessível somente dentro da VPC em que o endpoint é

provisionado ou de qualquer VPC emparelhada com a VPC em que o endpoint é provisionado conforme permitido pelas tabelas de rotas e pelos grupos de segurança.

- Você não pode usar o console da Amazon VPC para gerenciar endpoints da VPC gerenciados pelo Redshift.
- Quando você cria um endpoint da VPC gerenciado pelo Redshift para um cluster provisionado, a VPC escolhida deve ter um grupo de sub-redes. Para criar um grupo de sub-redes, consulte Gerenciamento de grupos de sub-redes de cluster usando o console.

Para obter informações sobre cotas e restrições de nomeação, consulte Cotas e limites no Amazon Redshift.

Para obter mais informações sobre preços, consulte Preços do AWS PrivateLink.

## Gerenciar endpoints da VPC gerenciados pelo Redshift usando o console

Você pode configurar o uso de endpoints da VPC gerenciados por Redshift usando o console do Amazon Redshift.

### Como conceder acesso ao

Se a VPC pela qual você deseja acessar seu cluster ou grupo de trabalho estiver em outra conta da AWS, você deve autorizá-la por meio da conta do proprietário (concessor).

Como permitir que uma VPC em outra conta da AWS tenha acesso ao seu cluster ou grupo de trabalho

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters. Para o Amazon Redshift sem servidor, escolha Painel da tecnologia sem servidor.
3. Para um cluster ao qual você deseja permitir acesso, visualize os detalhes escolhendo o nome do cluster. Escolha a guia Propriedades do cluster.

   A seção Contas concedidas exibe as contas e as VPCs correspondentes que têm acesso ao cluster. Para um grupo de trabalho do Amazon Redshift sem servidor, escolha o grupo de trabalho. As contas concedidas estão disponíveis na guia Acesso a dados.
4. Selecione Conceder acesso para exibir um formulário para inserir Informações do favorecido para adicionar uma conta.

5. Para o ID da conta da AWS, insira o ID da conta que você está concedendo acesso. Você pode conceder acesso a VPCs específicas ou a todas as VPCs na conta especificada.
6. Selecione Conceder acesso para conceder acesso.

## Criar um endpoint da VPC gerenciado por Redshift

Se você possui um cluster ou grupo de trabalho ou recebeu acesso para gerenciá-lo, poderá criar um endpoint da VPC gerenciado pelo Redshift para ele.

Para criar um endpoint da VPC gerenciado por Redshift

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Configurations (Configurações).

   A página Configurações exibe os endpoints da VPC gerenciados por Redshift que foram criados. Para exibir detalhes de um endpoint, escolha seu nome. Para o Amazon Redshift sem servidor, os endpoints da VPC estão na guia Acesso a dados quando você escolhe o grupo de trabalho.
3. Selecione Criar endpoint para exibir um formulário para inserir informações sobre o endpoint a ser adicionado.
4. Insira valores para Nome do endpoint, AWSID da conta de 12 dígitos, Nuvem privada virtual (VPC) em que o endpoint está localizado, Sub-rede e Grupo de segurança da VPC.

   A sub-rede em Sub-rede define as sub-redes e os endereços IP em que o Amazon Redshift implanta o endpoint. O Amazon Redshift escolhe uma sub-rede que tenha endereços IP disponíveis para a interface de rede associada ao endpoint.

   As regras de grupo de segurança em Grupo de segurança da VPC definem portas, protocolos e fontes para o tráfego de entrada que você está autorizando para o endpoint. O acesso à porta selecionada é permitido por meio do grupo de segurança ou do intervalo CIDR em que as workloads são executadas.
5. Selecione Criar endpoint para criar o endpoint.

Depois que o endpoint for criado, você poderá acessar o cluster ou grupo de trabalho por meio do URL mostrado em URL do endpoint nas definições de configuração para o endpoint da VPC gerenciado pelo Redshift.

## Gerenciar endpoints da VPC gerenciados por Redshift usando a AWS CLI

Você pode usar as seguintes operações da CLI do Amazon Redshift para trabalhar com endpoints da VPC gerenciados por Redshift. Para obter mais informações, consulte Referência de comandos da AWS CLI.

- authorize-endpoint-access
- revoke-endpoint-access
- create-endpoint-access
- modify-endpoint-access
- delete-endpoint-access
- describe-endpoint-access
- describe-endpoint-authorization

## Gerenciar endpoints da VPC gerenciados por Redshift usando operações de API do Amazon Redshift

Você pode usar as seguintes operações de API do Amazon Redshift para trabalhar com endpoints da VPC gerenciados por Redshift. Para obter mais informações, consulte a Referência de API do Amazon Redshift.

- AuthorizeEndpointAccess
- RevokeEndpointAccess
- CreateEndpointAccess
- ModifyEndpointAccess
- DeleteEndpointAccess
- DescribeEndpointAccess
- DescribeEndpointAuthorization

## Gerenciamento de endpoints da VPC gerenciados por Redshift usando o AWS CloudFormation

Para obter informações sobre o tipo de recurso do AWS CloudFormation para criar um endpoint da VPC gerenciado pelo Redshift usando AWS CloudFormation, consulte AWS::Redshift::EndpointAccess no Guia do usuário do AWS CloudFormation.

# Roteamento aprimorado da VPC no Amazon Redshift

Quando você usa o roteamento VPC aprimorado do Amazon Redshift, o Amazon Redshift força todo o tráfego COPY e UNLOAD entre seu cluster e seus repositórios de dados por meio de sua Virtual Private Cloud (VPC) com base no serviço Amazon VPC. Ao usar o roteamento VPC aprimorado, você pode usar recursos VPC padrão, como grupos de segurança da VPC, listas de controle de acesso à rede (ACLs), endpoints da VPC, políticas de endpoint da VPC, gateways da Internet e servidores Sistema de Nomes de Domínio (DNS), conforme descrito no Manual do usuário do Amazon VPC. Você usa esses recursos para gerenciar rigidamente o fluxo de dados entre o cluster do Amazon Redshift e outros recursos. Ao usar o roteamento aprimorado de VPC para rotear tráfego pela VPC, também é possível usar logs de fluxo da VPC para monitorar o tráfego de COPY e UNLOAD.

Os clusters do Amazon Redshift e os grupos de trabalho do Amazon Redshift Serverless oferecem suporte ao roteamento aprimorado de VPC. Não é possível usar o roteamento aprimorado de VPC com o Redshift Spectrum. Para ter mais informações, consulte Redshift Spectrum e roteamento aprimorado de VPC.

Se o roteamento aprimorado de VPC não estiver ativado, o Amazon Redshift roteará o tráfego pela Internet, incluindo o tráfego para outros serviços na rede da AWS.

> **Important**
>
> Como o roteamento VPC aprimorado afeta a maneira como o Amazon Redshift acessa outros recursos, os comandos COPY e UNLOAD podem falhar, a menos que você configure seu VPC corretamente. Você deve criar especificamente um caminho de rede entre a VPC do cluster e os recursos de dados, conforme descrito a seguir.

Quando você executa um comando COPY ou UNLOAD em um cluster com o roteamento aprimorado de VPC ativado, a VPC roteia o tráfego para o recurso especificado usando o caminho de rede mais rígido, ou mais específico, disponível.

Por exemplo, você pode configurar os seguintes percursos na VPC:

- Endpoints da VPC - Para o tráfego para um bucket do Amazon S3 na mesma região da AWS do seu cluster, você pode criar um endpoint da VPC para direcionar o tráfego diretamente para o bucket. Ao usar endpoints da VPC, você pode anexar uma política de endpoint para gerenciar o acesso ao Amazon S3. Para obter mais informações sobre como usar endpoints com o Amazon Redshift, consulte Trabalhar com endpoints da VPC. Se você usa o Lake Formation, pode encontrar mais informações sobre como estabelecer uma conexão privada entre a VPC e o AWS Lake Formation em AWS Lake Formation e endpoints da VPC de interface (AWS PrivateLink).
- Gateway NAT – Você pode se conectar a um bucket do Amazon S3 em outra região da AWS, e você pode se conectar a outro serviço dentro da rede da AWS. Você também pode acessar uma instância de host fora da rede da AWS. Para fazer isso, configure um gateway de conversão de endereços de rede (NAT), conforme descrito no Manual do usuário do Amazon VPC.
- Gateway da Internet – Para se conectar a serviços da AWS fora da VPC, você pode anexar um gateway da Internet à sua sub-rede da VPC, conforme descrito no Manual do usuário do Amazon VPC. Para usar um gateway de Internet, o cluster deve ter um IP público a fim de permitir que outros serviços se comuniquem com o cluster.

Para obter mais informações, consulte endpoints da VPC no Manual do usuário do Amazon VPC.

Não há cobrança adicional pelo uso do roteamento aprimorado de VPC. Você pode incorrer em cobranças de transferência de dados adicionais para determinadas operações. Isso inclui operações como UNLOAD para o Amazon S3 em uma região da AWS diferente. COPY do Amazon EMR ou Secure Shell (SSH) com endereços IP públicos. Para obter mais informações sobre a definição de preço, consulte Definição de preço do Amazon EC2.

Tópicos

- Trabalhar com endpoints da VPC
- Enhanced VPC routing
- Redshift Spectrum e roteamento aprimorado de VPC

# Trabalhar com endpoints da VPC

Você pode usar um endpoint da VPC para criar uma conexão gerenciada entre o cluster do Amazon Redshift em uma VPC e o Amazon Simple Storage Service (Amazon S3). Ao fazer isso, o tráfego de COPY e UNLOAD entre seu banco de dados e seus dados no Amazon S3 permanece em seu Amazon VPC. Você pode anexar uma política de endpoint ao endpoint para gerenciar mais de perto o acesso aos dados. Por exemplo, você pode adicionar uma política ao seu endpoint da VPC que permite o descarregamento de dados apenas para um bucket do Amazon S3 específico em sua conta.

> **Important**
>
> Atualmente, o Amazon Redshift dá suporte a endpoints da VPC somente para conexão com o Amazon S3. Quando o Amazon VPC adiciona suporte para outros serviços da AWS para usar endpoints da VPC, o Amazon Redshift também oferece suporte a essas conexões de endpoint da VPC. Para se conectar a um bucket do Amazon S3 usando um endpoint da VPC, o cluster do Amazon Redshift e o bucket do Amazon S3 a que ele se conecta devem estar na mesma região da AWS.

Para usar endpoints da VPC, crie um endpoint da VPC para a VPC em que o data warehouse está e ative o roteamento aprimorado de VPC. Você pode ativar o roteamento aprimorado de VPC ao criar o cluster ou grupo de trabalho, ou pode modificar um cluster ou grupo de trabalho em uma VPC para usar o roteamento aprimorado de VPC.

Um endpoint da VPC usa tabelas de rotas para controlar o roteamento de tráfego entre um cluster ou grupo de trabalho na VPC e o Amazon S3. Todos os clusters e grupos de trabalho nas sub-rede associadas às tabelas de rotas especificadas usam automaticamente esse endpoint para acessar o serviço.

A VPC usa a rota mais específica ou a mais restritiva, de acordo com o tráfego para determinar como rotear o tráfego. Por exemplo, suponha que você tenha uma rota em sua tabela de rotas para todo o tráfego da Internet (0.0.0.0/0) que aponta para um gateway da Internet e um endpoint do Amazon S3. Nesse caso, a rota do endpoint tem precedência para todo o tráfego destinado ao Amazon S3. Isso ocorre porque o intervalo de endereços IP para o serviço Amazon S3 é mais específico do que 0.0.0.0/0. Neste exemplo, todo o outro tráfego de Internet vai para seu gateway da Internet, incluindo o tráfego que é destinado a buckets do Amazon S3 em outras Regiões da AWS.

Para obter mais informações sobre como criar endpoints, consulte Criar um endpoint da VPC no Guia do usuário da Amazon VPC.

Use políticas de endpoint para controlar o acesso de seu cluster ou grupo de trabalho aos buckets do Amazon S3 que contêm seus arquivos de dados. Para obter um controle mais específico, você também pode anexar uma política de endpoint personalizada. Para obter mais informações, consulte Controlar o Acesso a Serviços Usando Políticas de Endpoint no AWS PrivateLink Guia.

Não há cobrança adicional pelo uso de endpoints. Aplicam-se as cobranças padrão pela transferência de dados e pela utilização de recursos. Para obter mais informações sobre a definição de preço, consulte Definição de preço do Amazon EC2.

## Enhanced VPC routing

Você pode ativar o roteamento aprimorado de VPC ao criar ou modificar um cluster, e ao criar ou modificar um grupo de trabalho do Amazon Redshift Serverless.

Para trabalhar com o roteamento aprimorado de VPC, o cluster deve atender aos seguintes requisitos e limitações:

- O cluster deve estar em uma VPC.

  Se você anexar um endpoint da VPC do Amazon S3, seu cluster usará o endpoint da VPC apenas para acessar os buckets do Amazon S3 na mesma região da AWS. Para acessar buckets em outra região da AWS (sem usar o endpoint da VPC) ou para acessar outros serviços da AWS, torne seu cluster acessível publicamente ou use um gateway de conversão de endereço de rede (NAT). Para ter mais informações, consulte Criar um cluster em uma VPC.
- Você deve habilitar a resolução Serviço de Nome de Domínio (DNS) em sua VPC. Como alternativa, se você estiver usando seu próprio servidor DNS, certifique-se de que as solicitações DNS para o Amazon S3 sejam resolvidas corretamente para os endereços IP mantidos pela AWS. Para obter mais informações, consulte Usar DNS com a VPC, no Guia do usuário da Amazon VPC.
- Os nomes de host DNS devem ser ativados na VPC. Por padrão, os nomes de hosts DNS estão ativados.
- Suas políticas de endpoint da VPC devem permitir o acesso a qualquer bucket do Amazon S3 usado com chamadas COPY, UNLOAD ou CREATE LIBRARY no Amazon Redshift, incluindo acesso a quaisquer arquivos manifesto envolvidos. Para COPY em hosts remotos, as políticas de endpoint devem permitir acesso a cada máquina de host. Para obter mais informações, consulte

Permissões do IAM para COPY, UNLOAD e CREATE LIBRARY no Guia do desenvolvedor de banco de dados do Amazon Redshift.

Para criar um cluster com o Enhanced VPC routing

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Provisioned clusters dashboard (Painel de clusters provisionados), depois selecione Create cluster (Criar Cluster) e insira as propriedades de Cluster details (Detalhes do cluster).
3. Para exibir a seção Additional configurations (Configurações adicionais), desative Use defaults (Usar padrões).
4. Navegue até a seção Network and security (Rede e segurança).
5. Para ativar o Enhanced VPC routing (Roteamento aprimorado de VPC), escolha Turn on (Ativar) para forçar o tráfego do cluster pela VPC.
6. Para criar o cluster, escolha Create cluster (Criar cluster). Podem ser necessários alguns minutos para preparar o cluster para ser usado.

Como criar um grupo de trabalho do Amazon Redshift sem servidor com roteamento aprimorado de VPC

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Serverless dashboard (Painel do Serverless), selecione Create workgroup (Criar grupo de trabalho) e insira as propriedades para o grupo de trabalho.
3. Navegue até a seção Network and security (Rede e segurança).
4. Selecione Turn on enhanced VPC routing (Ativar roteamento aprimorado de VPC) para rotear o tráfego de rede pela VPC.
5. Escolha Next (Avançar) e termine de inserir as propriedades do grupo de trabalho, depois selecione Create (Criar) para criar o grupo de trabalho.

# Redshift Spectrum e roteamento aprimorado de VPC

O Amazon Redshift Spectrum não oferece suporte ao roteamento aprimorado de VPC com clusters provisionados. O roteamento aprimorado da VPC do Amazon Redshift roteia o tráfego específico por meio de sua VPC. Todo o tráfego entre seu cluster e seus buckets do Amazon S3 é forçado a passar por seu Amazon VPC. O Redshift Spectrum executa recursos gerenciados pela AWS que são de propriedade do Amazon Redshift. Como esses recursos estão fora da VPC, o Redshift Spectrum não usa o roteamento aprimorado de VPC.

O tráfego entre o Redshift Spectrum e o Amazon S3 é roteado com segurança pela rede privada da AWS, fora da VPC. O tráfego em trânsito é assinado usando o protocolo Amazon Signature versão 4 (SIGv4) e criptografado usando HTTPS. Este tráfego é autorizado com base na função do IAM anexada ao seu cluster do Amazon Redshift. Para gerenciar ainda mais o tráfego do Redshift Spectrum, você pode modificar a função do IAM do seu cluster e sua política anexada ao bucket do Amazon S3. Também pode ser necessário configurar seu VPC para permitir que seu cluster acesse o Athena ou o AWS Glue, conforme detalhado a seguir.

Observe que, como o roteamento VPC aprimorado afeta a maneira como o Amazon Redshift acessa outros recursos, as consultas podem falhar, a menos que você configure a VPC corretamente. Para obter mais informações, consulte Roteamento aprimorado da VPC no Amazon Redshift, que discute com mais detalhes a criação de um endpoint da VPC, um gateway de conversão de endereços de rede (gateway NAT) e outros recursos de rede para direcionar o tráfego aos buckets do Amazon S3.

> **Note**
>
> O Amazon Redshift Serverless oferece suporte ao roteamento aprimorado de VPC para consultas a tabelas externas no Amazon S3.

## Considerações ao usar o Amazon Redshift Spectrum

Veja a seguir as considerações sobre o uso do Redshift Spectrum:

- Políticas de acesso ao bucket
- Função do IAM do cluster
- Registrar em log e auditar o acesso ao Amazon S3
- Acesso ao AWS Glue ou Amazon Athena

### Políticas de acesso ao bucket

Você pode controlar o acesso aos dados em seus buckets do Amazon S3 usando uma política de bucket anexada ao bucket e usando uma função do IAM anexada ao cluster.

O Redshift Spectrum em clusters provisionados não pode acessar dados armazenados em buckets do Amazon S3 que usam uma política de bucket que restringe o acesso apenas a endpoints da VPC especificados. Em vez disso, use uma política de bucket que restrinja o acesso apenas a entidades principais específicas, como uma conta específica da AWS ou usuários específicos.

Para a função do IAM que tem acesso ao bucket, use uma relação de confiança que permita que a função seja assumida apenas pela entidade principal de serviço do Amazon Redshift. Quando anexada ao seu cluster, a função pode ser usada apenas no contexto do Amazon Redshift e não pode ser compartilhada fora do cluster. Para ter mais informações, consulte Restringir acesso a funções do IAM. Uma política de controle de serviços (SCP) também pode ser usada para restringir ainda mais o perfil. Consulte Impedir que usuários e perfis do IAM façam alterações especificadas, com uma exceção para um perfil de administrador especificado no Guia do usuário do AWS Organizations.

Para usar o Redshift Spectrum, nenhuma política do IAM bloqueando o uso de URLs pré-assinadas pode estar em vigor.

O seguinte exemplo de política de bucket permite acesso ao bucket especificado somente a partir do tráfego originado pelo Redshift Spectrum pertencente à conta da 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"
   }
  }
 }]
```

```
}
```

Função do IAM do cluster

A função associada ao seu cluster deve ter uma relação de confiança que permita que seja assumida apenas pelo serviço do Amazon Redshift, como mostrado a seguir.

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

Você pode adicionar uma política à função do cluster que impede o acesso de COPY e UNLOAD a um bucket específico. A política a seguir permite o tráfego para o bucket especificado somente a partir do 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"}}
    }]
}
```

Para obter mais informações, consulte Políticas do IAM para o Redshift Spectrum no Guia do desenvolvedor de bancos de dados do Amazon Redshift.

Registrar em log e auditar o acesso ao Amazon S3

Um dos benefícios ao usar o roteamento aprimorado da VPC do Amazon Redshift é que todo o tráfego de COPY e UNLOAD é registrado nos logs de fluxo da VPC. O tráfego originado do Redshift

Spectrum para o Amazon S3 não passa pelo seu VPC, portanto, não é registrado nos logs de fluxo do VPC. Quando o Redshift Spectrum acessa dados no Amazon S3, ele executa essas operações no contexto da conta da AWS e dos respectivos privilégios de função. Você pode registrar e auditar o acesso ao Amazon S3 usando o registro em log de acesso ao servidor no AWS CloudTrail e Amazon S3.

Certifique-se de que os intervalos de IP do S3 sejam adicionados à sua lista de permissões. Para saber mais sobre os intervalos de IP do S3 necessários, consulte Isolamento de rede.

Registros do AWS CloudTrail

Para rastrear todo o acesso a objetos no Amazon S3, incluindo o acesso ao Redshift Spectrum, habilite o registro em log do CloudTrail para objetos do Amazon S3.

Você pode usar o CloudTrail para visualizar, pesquisar, baixar, arquivar, analisar e responder à atividade da conta em sua infraestrutura da AWS. Para obter mais informações, consulte Conceitos básicos do CloudTrail.

Por padrão, o CloudTrail rastreia somente as ações do nível do bucket. Para rastrear as ações em nível de objeto (como `GetObject`), habilite eventos de dados e gerenciamento para cada bucket registrado em log.

Registro em log de acesso ao servidor do Amazon S3

O registro em log de acesso ao servidor fornece detalhes sobre as solicitações que são feitas a um bucket. As informações de log de acesso podem ser úteis em auditorias de segurança e acesso. Para obter mais informações, consulte Como habilitar o registro de acesso ao servidor no Guia do usuário do Amazon Simple Storage Service.

Para obter mais informações, consulte a postagem do blog sobre segurança da AWS Como usar políticas de bucket e aplicar defesa adequadamente para ajudar a proteger seus dados do Amazon S3.

Acesso ao AWS Glue ou Amazon Athena

O Redshift Spectrum acessa seu catálogo de dados no AWS Glue ou no Athena. Outra opção é usar um metastore do Hive dedicado para seu catálogo de dados.

Para habilitar o acesso ao AWS Glue ou ao Athena, configure seu VPC com um gateway da Internet ou gateway NAT. Configure seus grupos de segurança da VPC para permitir tráfego de saída para os endpoints públicos para o AWS Glue e o Athena. Como alternativa, você pode configurar um

endpoint de interface da VPC para AWS Glue para acessar AWS Glue Data Catalog. Quando você usa um endpoint de interface da VPC, a comunicação entre sua VPC e o AWS Glue é realizada na rede da AWS. Para obter mais informações, consulte Criação de um endpoint de interface.

Você pode configurar os seguintes percursos na VPC:

- Gateway da Internet – Para se conectar a serviços da AWS fora da VPC, você pode anexar um gateway da Internet à sua sub-rede da VPC, conforme descrito no Manual do usuário do Amazon VPC. Para usar um gateway de internet, o cluster deve ter um endereço IP público a fim de permitir que outros serviços se comuniquem com o cluster.
- Gateway NAT – Para se conectar a um bucket do Amazon S3 em outra região da AWS ou a outro serviço dentro da rede da AWS, configure um gateway de conversão de endereços de rede (NAT) conforme descrito no Manual do usuário do Amazon VPC. Use essa configuração também para acessar uma instância de host fora da rede da AWS.

Para ter mais informações, consulte Roteamento aprimorado da VPC no Amazon Redshift.

# Monitorar a performance do cluster do Amazon Redshift

O Amazon Redshift fornece dados e métricas de performance para que você possa rastrear a integridade e a performance de seus clusters e bancos de dados. Nesta seção, discutimos os tipos de dados com os quais você pode trabalhar no Amazon Redshift, especificamente no console do Amazon Redshift.

Tópicos


- Visão geral
- Monitorar o Amazon Redshift usando métricas do CloudWatch
- Trabalhar com dados de performance no console do Amazon Redshift


## Visão geral

Os dados de performance que você pode usar no console do Amazon Redshift se enquadram em duas categorias:

- Métricas do Amazon CloudWatch – As métricas do Amazon CloudWatch ajudam a monitorar os aspectos físicos do seu cluster, como a utilização da CPU, latência e rendimento. Os dados métricos são exibidos diretamente no console do Amazon Redshift. Você também pode visualizá-los no console do CloudWatch. Como alternativa, você pode consumi-lo de qualquer outra maneira de trabalhar com métricas, como com a AWS CLI ou um dos AWS SDKs.
- Consultar/carregar dados de performance – Os dados de performance ajudam a monitorar a atividade e a performance do banco de dados. Esses dados são agregados no console do Amazon Redshift para ajudá-lo a correlacionar facilmente o que você vê nas métricas do CloudWatch com consultas de banco de dados específicas e eventos de carga. Você também pode criar as próprias consultas de performance personalizadas e executá-las diretamente no banco de dados. Os dados de performance de consulta e carga são exibidos apenas no console do Amazon Redshift. Não é publicado como métricas do CloudWatch.

Os dados de performance são integrados ao console do Amazon Redshift, proporcionando uma experiência mais rica das seguintes maneiras:

- Os dados de performance associados a um cluster são exibidos de maneira contextual quando você exibe um cluster, em que possa precisar tomar decisões sobre o cluster, como redimensionamento.
- Algumas métricas de performance são exibidas em unidades com escala mais apropriada no console do Amazon Redshift em comparação com o CloudWatch. Por exemplo, `WriteThroughput` é exibido em GB/s (em comparação com bytes/s no CloudWatch), que é uma unidade mais relevante para o espaço de armazenamento típico de um nó.
- Você pode exibir facilmente os dados de performance dos nós de um cluster no mesmo gráfico. Dessa forma, você poderá monitorar facilmente a performance de todos os nós de um cluster. Você também pode ver dados de performance de cada nó.

O Amazon Redshift fornece dados de performance (tanto métricas do CloudWatch quanto dados de consulta e carga) sem custo adicional. Os dados de performance são registrados a cada minuto. Você pode acessar valores históricos de dados de performance no console do Amazon Redshift. Para obter informações detalhadas sobre como usar o CloudWatch para acessar os dados de performance do Amazon Redshift expostos como métricas do CloudWatch, consulte O que é o CloudWatch? no Manual do usuário do Amazon CloudWatch.

## Monitorar o Amazon Redshift usando métricas do CloudWatch

Usando as métricas do CloudWatch para Amazon Redshift, você pode obter informações sobre a integridade e a performance do seu cluster e ver as informações no nível do nó. Ao trabalhar com essas métricas, é importante lembrar que cada uma delas tem uma ou mais dimensões associadas. Essas dimensões informam a que a métrica se aplica, ou seja, o escopo da métrica. O Amazon Redshift tem as seguintes duas dimensões:

- As métricas que têm uma dimensão `NodeID` são métricas que fornecem dados de performance de nós de um cluster. Esse conjunto de métricas inclui nós de computação e líderes. Entre os exemplos dessas métricas estão `CPUUtilization`, `ReadIOPS`, `WriteIOPS`.
- As métricas que têm somente uma dimensão `ClusterIdentifier` são métricas que fornecem dados de performance para os clusters. Entre os exemplos dessas métricas estão `HealthStatus` e `MaintenanceMode`.

> **Note**
>
> Em alguns casos, uma métrica específica do cluster representa uma agregação de comportamento do nó. Nesses casos, cuidado ao interpretar o valor da métrica, pois o comportamento do nó líder é agregado ao nó de computação.

Para obter informações gerais sobre as métricas e dimensões do CloudWatch, consulte Conceitos do CloudWatch no Manual do usuário do Amazon CloudWatch.

Para obter uma descrição mais detalhada das métricas do CloudWatch para Amazon Redshift, consulte as seções a seguir.

Tópicos


- Métricas do Amazon Redshift
- Dimensões para métricas do Amazon Redshift
- Dados de performance de consulta e carga do Amazon Redshift


## Métricas do Amazon Redshift

O namespace `AWS/Redshift` inclui as métricas a seguir. Salvo indicação em contrário, as métricas são coletadas em intervalos de 1 minuto.

Cargo

| Métrica | Descrição |
| --- | --- |
| `CommitQueueLength` | O número de transações que aguardam confirmação em algum momento.<br><br>Unidades: contagem<br><br>Dimensões: `ClusterIdentifier` |
| `ConcurrencyScaling ActiveClusters` | O número de clusters de escalabilidade da simultaneidade que estão processando consultas ativamente em um determinado momento. |

| Métrica | Descrição |
| --- | --- |
| | Unidades: contagem<br><br>Dimensões: `ClusterIdentifier` |
| `ConcurrencyScaling Seconds` | O número de segundos usados pelos clusters de escalabilidade da simultaneidade que têm atividade de processamento ativo de consultas.<br><br>Unidades: contagem<br><br>Dimensões: `ClusterIdentifier` |
| `CPUUtilization` | O percentual de utilização da CPU. Para clusters, esta métrica representa uma agregação dos valores de utilização da CPU de todos os nós (principais e de computação).<br><br>Unidades: percentual<br><br>Dimensões: `ClusterIdentifier` , `NodeID`<br><br>Dimensões: `ClusterIdentifier` |
| `DatabaseConnections` | O número de conexões do banco de dados com um cluster.<br><br>Unidades: contagem<br><br>Dimensões: `ClusterIdentifier` |

| Métrica | Descrição |
| --- | --- |
| `HealthStatus` | Indica a saúde do cluster. A cada minuto, o cluster se conecta ao banco de dados e executa uma consulta simples. Se conseguir executar essa operação com êxito, o cluster é considerado saudável. Caso contrário, o cluster está com problemas. Um status não saudável pode ocorrer quando o banco de dados do cluster está sob carga extremamente pesada ou se houver um problema de configuração com um banco de dados no cluster.<br><br>**Note**<br>No Amazon CloudWatch, essa métrica é relatada como 1 ou 0, enquanto no console do Amazon Redshift, essa métrica é exibida com as palavras `HEALTHY` ou `UNHEALTHY` por conveniência. Quando essa métrica é exibida no console do Amazon Redshift, as médias de amostragem são ignoradas e apenas `HEALTHY` ou `UNHEALTHY` são exibidas. No Amazon CloudWatch, valores diferentes de 1 e 0 podem ocorrer devido a problemas de amostragem. Qualquer valor abaixo de 1 para `HealthStatus` é reportado como 0 (`UNHEALTHY`).<br><br>Unidades: contagem (1/0) (`HEALTHY`/`UNHEALTHY` no console do Amazon Redshift)<br><br>Dimensões: `ClusterIdentifier` |

| Métrica | Descrição |
| --- | --- |
| `MaintenanceMode` | Indica se o cluster está no modo de manutenção.<br><br>**Note**<br>No Amazon CloudWatch, essa métrica é relatada como 1 ou 0, enquanto no console do Amazon Redshift, essa métrica é exibida com as palavras `ON` ou `OFF` por conveniência. Quando essa métrica é exibida no console do Amazon Redshift, as médias de amostragem são ignoradas e apenas `ON` ou `OFF` são exibidas. No Amazon CloudWatch, valores diferentes de 1 e 0 podem ocorrer devido a problemas na amostragem. Qualquer valor acima de 0 para `MaintenanceMode` é reportado como 1 (`ON`).<br><br>Unidades: contagem (1/0) (`ON`/`OFF` no console do Amazon Redshift).<br><br>Dimensões: `ClusterIdentifier` |
| `MaxConfiguredConcurrencyScalingClusters` | Número máximo de clusters de escalabilidade da simultaneidade configurados a partir do grupo de parâmetros. Para obter mais informações, consulte Grupos de parâmetros do Amazon Redshift.<br><br>Unidades: contagem<br><br>Dimensões: `ClusterIdentifier` |
| `NetworkReceiveThroughput` | A taxa em que o nó ou cluster recebe dados.<br><br>Unidade: bytes/segundo (MB/s no console do Amazon Redshift)<br><br>Dimensões: `ClusterIdentifier` , `NodeID`<br><br>Dimensões: `ClusterIdentifier` |

| Métrica | Descrição |
| --- | --- |
| `NetworkTransmitThroughput` | A taxa em que o nó ou cluster grava dados.<br><br>Unidade: bytes/segundo (MB/s no console do Amazon Redshift)<br><br>Dimensões: `ClusterIdentifier` , `NodeID`<br><br>Dimensões: `ClusterIdentifier` |
| `PercentageDiskSpaceUsed` | O percentual do espaço em disco utilizado.<br><br>Unidades: percentual<br><br>Dimensões: `ClusterIdentifier`<br><br>Dimensões: `ClusterIdentifier` , `NodeID` |
| `QueriesCompletedPerSecond` | O número médio de consultas concluídas por segundo. Relatado em intervalos de 5 minutos. Essa métrica não é compatível com clusters de nó único.<br><br>Unidade: contagem/segundo<br><br>Dimensões: `ClusterIdentifier` , `latency`<br><br>Dimensões: `ClusterIdentifier` , `wlmid` |
| `QueryDuration` | O tempo médio para concluir uma consulta. Relatado em intervalos de 5 minutos. Essa métrica não é compatível com clusters de nó único.<br><br>Unidade: microssegundos<br><br>Dimensões: `ClusterIdentifier` , `NodeID`, `latency`<br><br>Dimensões: `ClusterIdentifier` , `latency`<br><br>Dimensões: `ClusterIdentifier` , `NodeID`, `wlmid` |

| Métrica | Descrição |
| --- | --- |
| QueryRuntimeBreakdown | O tempo total que as consultas gastam em execução por estágio de consulta. Relatado em intervalos de 5 minutos.<br><br>Unidade: milissegundos<br><br>Dimensões: ClusterIdentifier, NodeID, stage<br><br>Dimensões: ClusterIdentifier, stage |
| ReadIOPS | O número médio de operações de leitura de disco por segundo.<br><br>Unidade: contagem/segundo<br><br>Dimensões: ClusterIdentifier , NodeID<br><br>Dimensões: ClusterIdentifier |
| ReadLatency | O tempo médio necessário para operações de I/O de leitura de disco.<br><br>Unidades: segundos<br><br>Dimensões: ClusterIdentifier , NodeID<br><br>Dimensões: ClusterIdentifier |
| ReadThroughput | O número médio de bytes lidos do disco por segundo.<br><br>Unidade: bytes (GB/s no console do Amazon Redshift)<br><br>Dimensões: ClusterIdentifier , NodeID<br><br>Dimensões: ClusterIdentifier |
| RedshiftManagedStorageTotalCapacity | Capacidade total de armazenamento gerenciado.<br><br>Unidades: megabytes<br><br>Dimensões: ClusterIdentifier |

| Métrica | Descrição |
| --- | --- |
| `TotalTableCount` | O número de tabelas de usuário abertas em um momento específico. Esse total não inclui tabelas do Amazon Redshift Spectrum.<br><br>Unidades: contagem<br><br>Dimensões: `ClusterIdentifier` |
| `WLMQueueLength` | O número de consultas aguardando para entrar em uma fila de gerenciamento do workload (WLM).<br><br>Unidades: contagem<br><br>Dimensões: `ClusterIdentifier` , `service class`<br><br>Dimensões: `ClusterIdentifier` , `QueueName` |
| `WLMQueueWaitTime` | Tempo total que as consultas ficaram esperando na fila de gerenciamento do workload (WLM). Relatado em intervalos de 5 minutos.<br><br>Unidade: milissegundos.<br><br>Dimensões: `ClusterIdentifier` , `QueryPriority`<br><br>Dimensões: `ClusterIdentifier` , `wlmid`<br><br>Dimensões: `ClusterIdentifier` , `QueueName` |
| `WLMQueriesCompletedPerSecond` | O número médio de consultas concluídas por segundo de uma fila de gerenciamento do workload (WLM). Relatado em intervalos de 5 minutos. Essa métrica não é compatível com clusters de nó único.<br><br>Unidade: contagem/segundo<br><br>Dimensões: `ClusterIdentifier` , `wlmid`<br><br>Dimensões: `ClusterIdentifier` , `QueueName` |

| Métrica | Descrição |
| --- | --- |
| `WLMQueryDuration` | O tempo médio para concluir uma consulta de uma fila de gerenciamento do workload (WLM). Relatado em intervalos de 5 minutos. Essa métrica não é compatível com clusters de nó único.<br><br>Unidade: microssegundos<br><br>Dimensões: `ClusterIdentifier` , `wlmid`<br><br>Dimensões: `ClusterIdentifier` , `QueueName` |
| `WLMRunningQueries` | O número de consultas em execução no cluster principal e no cluster de escalabilidade da simultaneidade por fila do WLM.<br><br>Unidades: contagem<br><br>Dimensões: `ClusterIdentifier` , `wlmid`<br><br>Dimensões: `ClusterIdentifier` , `QueueName` |
| `WriteIOPS` | O número médio de operações de gravação por segundo.<br><br>Unidade: contagem/segundo<br><br>Dimensões: `ClusterIdentifier` , `NodeID`<br><br>Dimensões: `ClusterIdentifier` |
| `WriteLatency` | O tempo médio necessário para operações de I/O de gravação em disco.<br><br>Unidades: segundos<br><br>Dimensões: `ClusterIdentifier` , `NodeID`<br><br>Dimensões: `ClusterIdentifier` |

| Métrica | Descrição |
| --- | --- |
| `WriteThroughput` | O número médio de bytes gravados no disco por segundo.<br><br>Unidade: bytes (GB/s no console do Amazon Redshift)<br><br>Dimensões: `ClusterIdentifier` , `NodeID`<br><br>Dimensões: `ClusterIdentifier` |
| `SchemaQuota` | A cota configurada para um esquema.<br><br>Unidades: megabytes<br><br>Dimensões: `ClusterIdentifier` , `Database`, `Schema`<br><br>Periódio/Push: `Periodic`<br><br>Frequência: `5 minutes`<br><br>Critérios de parada: esquema descartado ou cota removida |
| `NumExceededSchemaQuotas` | O número de esquemas com cotas excedidas.<br><br>Unidades: contagem<br><br>Dimensões: `ClusterIdentifier`<br><br>Periódio/Push: `Periodic`<br><br>Frequência: `5 minutes`<br><br>Critérios de parada: N/D |

| Métrica | Descrição |
| --- | --- |
| `StorageUsed` | O disco ou o espaço de armazenamento usado por um esquema.<br><br>Unidades: megabytes<br><br>Dimensões: `ClusterIdentifier` , `Database`, `Schema`<br><br>Periódio/Push: `Periodic`<br><br>Frequência: `5 minutes`<br><br>Critérios de parada: esquema descartado ou cota removida |
| `PercentageQuotaUsed` | A porcentagem de espaço em disco ou armazenamento usado em relação à cota de esquema configurada.<br><br>Unidades: percentual<br><br>Dimensões: `ClusterIdentifier` , `Database`, `Schema`<br><br>Periódio/Push: `Periodic`<br><br>Frequência: `5 minutes`<br><br>Critérios de parada: esquema descartado ou cota removida |

| Métrica | Descrição |
| --- | --- |
| `UsageLimitAvailable` | Dependendo de FeatureType, UsageLimitAvailable retorna o seguinte:<br>• Se FeatureType for `CONCURRENCY_SCALING` , UsageLimitAvailable retornará o tempo total que pode ser usado pela escala de simultaneidade em incrementos de 1 minuto.<br>• Se FeatureType for `CROSS_REGION_DATASHARING` , UsageLimitAvailable retornará o volume total de dados que pode ser examinado em incrementos de 1 TB.<br>• Se FeatureType for `SPECTRUM`, UsageLimitAvailable retornará o volume total de dados que pode ser examinado em incrementos de 1 TB.<br><br>Unidades: minutos ou TBs<br><br>Dimensões: `ClusterIdentifier` , `FeatureType` , `UsageLimitId` |
| `UsageLimitConsumed` | Dependendo de FeatureType, UsageLimitConsumed retorna o seguinte:<br>• Se FeatureType for `CONCURRENCY_SCALING` , UsageLimitAvailable retornará o tempo total usado pela escala de simultaneidade em incrementos de 1 minuto.<br>• Se FeatureType for `CROSS_REGION_DATASHARING` , UsageLimitAvailable retornará o volume total de dados examinado em incrementos de 1 TB.<br>• Se FeatureType for `SPECTRUM`, UsageLimitAvailable retornará o volume total de dados examinado em incrementos de 1 TB.<br><br>Unidades: minutos ou TBs<br><br>Dimensões: `ClusterIdentifier` , `FeatureType` , `UsageLimitId` |

# Dimensões para métricas do Amazon Redshift

Os dados do Amazon Redshift podem ser filtrados em qualquer uma das dimensões na tabela a seguir.

| Dimensão | Descrição |
| --- | --- |
| `latency` | Os valores possíveis são:<br>• curto - abaixo de 10 segundos<br>• médio - entre 10 segundos e 10 minutos<br>• longo - acima de 10 minutos |
| `NodeID` | Filtra os dados solicitados que são específicos para os nós de um cluster. `NodeID` é "Leader", "Shared" ou "Compute-N", sendo N 0, 1,... conforme o número de nós no cluster. "Shared" significa que o cluster tem apenas um nó, ou seja, o nó principal e o nó de computação são combinados.<br>As métricas só são relatadas pelo nó de liderança e pelos nós de computação para `CPUUtilization` , `NetworkTransmitThroughput` e `ReadIOPS`. Outras métricas que usam a dimensão `NodeId` são relatadas somente para nós de computação. |
| `ClusterIdentifier` | Filtra os dados solicitados que são específicos ao cluster. As métricas específicas a clusters incluem `HealthStatus` , `MaintenanceMode` e `DatabaseConnections` . De modo geral, métricas para esta dimensão (por exemplo, `ReadIOPS`) que também são métricas de nós representam um conjunto dos dados na métrica do nó. Atente-se ao interpretar essas métricas porque elas reúnem o comportamento de nós principais e de computação. |
| `service class` | O identificador de uma classe de serviço `WLM`. |
| `stage` | Os estágios de execução de uma consulta. Os valores possíveis são: |

| Dimensão | Descrição |
| --- | --- |
| | • QueryPlanning: tempo gasto analisando e otimizando comandos de SQL.<br>• QueryWaiting: tempo gasto esperando na fila de WLM.<br>• QueryExecutingRead: Tempo gasto executando leitura de consultas.<br>• QueryExecutingInsert: Tempo gasto executando inserção de consultas.<br>• QueryExecutingDelete: Tempo gasto executando exclusão de consultas.<br>• QueryExecutingUpdate: Tempo gasto executando atualização de consultas.<br>• QueryExecutingCtas: Tempo gasto executando consultas de "criar tabela como".<br>• QueryExecutingUnload: Tempo gasto executando descarreg amento de consultas.<br>• QueryExecutingCopy: Tempo gasto executando cópia de consultas.<br>• QueryCommit: Confirmar tempo gasto. |
| `wlmid` | O identificador para uma fila de gerenciamento do workload. |
| `QueryPriority` | A prioridade da consulta. Os valores possíveis são `CRITICAL`, `HIGHEST`, `HIGH`, `NORMAL`, `LOW` e `LOWEST`. |
| `QueueName` | O nome da fila de gerenciamento de workload. |
| `FeatureType` | O recurso limitado por um limite de uso. Os valores possíveis são `CONCURRENCY_SCALING` , `CROSS_REGION_DATAS HARING` e `SPECTRUM`. |
| `UsageLimitId` | O identificador de um limite de uso. |

# Dados de performance de consulta e carga do Amazon Redshift

Além das métricas do CloudWatch, o Amazon Redshift fornece dados de performance de consulta e carga. Os dados de consulta e carga podem ser usados para ajudar a entender a relação entre a performance do banco de dados e as métricas do cluster. Por exemplo, se perceber que a CPU de um cluster atingiu o pico, você poderá saber o pico no gráfico de CPU do cluster e ver as consultas que estavam em execução nesse momento. Por outro lado, se você estiver avaliando uma consulta específica, os dados da métrica (como CPU) serão exibidos no contexto, de maneira que possa compreender o impacto da consulta sobre as métricas do cluster.

Os dados de performance de consulta e carga não são publicados como métricas do CloudWatch e só podem ser visualizados no console do Amazon Redshift. Os dados de performance de consulta e carga são gerados consultando-se as tabelas do sistema do banco de dados (para obter mais informações, consulte Referência de tabelas do sistema no Guia do desenvolvedor do Amazon Redshift). Você também pode gerar as próprias consultas de performance do banco de dados personalizadas, mas recomendamos começar com os dados de performance de consulta e carga apresentados no console. Para obter mais informações sobre como medir e monitorar a performance do banco de dados por conta própria, consulte Gerenciar a performance, no Guia do desenvolvedor do Amazon Redshift.

A tabela a seguir descreve diferentes aspectos de consulta e carregamento de dados que você pode acessar no console do Amazon Redshift.

| Dados de consulta/ carga | Descrição |
| --- | --- |
| Resumo da consulta | Uma lista de consultas em um período especificado. A lista pode ser classificada em valores como ID de consulta, tempo de execução da consulta e status. Visualize esses dados na guia Monitoramento de consulta da página de detalhes do cluster. |
| Detalhes da consulta | Dá detalhes sobre uma consulta específica, inclusive:<br>• Propriedades de consulta como o ID de consulta, o tipo, o cluster no qual a consulta foi executada e o tempo de execução.<br>• Detalhes como o status da consulta e o número de erros.<br>• O comando SQL que foi executado.<br>• Um plano de explicação, se disponível. |

| Dados de consulta/ carga | Descrição |
| --- | --- |
| | • Dados de performance do cluster durante a execução da consulta (para obter mais informações, consulte Visualizar dados do histórico de consultas). |
| Resumo da carga | Lista todas as cargas em um período especificado. A lista pode ser classificada em valores como ID de consulta, tempo de execução da consulta e status. Visualize esses dados na guia Monitoramento de consulta da página de detalhes do cluster. |
| Detalhes da carga | Dá detalhes sobre uma operação de carga específica, inclusive:<br>• Propriedades de carga como o ID de consulta, o tipo, o cluster no qual a consulta foi executada e o tempo de execução.<br>• Detalhes como o status da carga e o número de erros.<br>• O comando SQL que foi executado.<br>• Uma lista de arquivos carregados.<br>• Dados de performance de cluster durante a operação de carga (para obter mais informações, consulte Visualizar dados do histórico de consultas). |

# Trabalhar com dados de performance no console do Amazon Redshift

Nesta seção, você pode descobrir como visualizar os dados de performance no console do Amazon Redshift, que inclui informações sobre cluster e performance de consulta. Além disso, você pode criar alarmes nas métricas do cluster diretamente do console do Amazon Redshift.

Ao visualizar os dados de performance no console do Amazon Redshift, você os visualiza por cluster. Os gráficos de dados de performance de um cluster foram projetados para dar acesso a dados para responder às dúvidas de performance mais comuns. Para alguns dados de performance (consulte Monitorar o Amazon Redshift usando métricas do CloudWatch), você também pode usar o CloudWatch para personalizar ainda mais seus gráficos de métricas. Por exemplo, você pode escolher tempos maiores ou combinar métricas entre clusters. Para obter mais informações sobre

como trabalhar com o console do CloudWatch, consulte Trabalhar com métricas de performance no console do CloudWatch.

Assista ao vídeo a seguir para aprender como monitorar, isolar e otimizar suas consultas usando os recursos de monitoramento de consultas no console do Amazon Redshift: Monitoramento de consultas com Amazon Redshift.

Tópicos


- Visualizar dados de performance do cluster
- Visualizar dados do histórico de consultas
- Visualizar dados de performance do banco de dados
- Visualizar dados de escalabilidade da simultaneidade e simultaneidade do workload
- Visualizar consultas e cargas
- Visualizar métricas do cluster durante as operações de carga
- Analisar a performance do workload
- Gerenciar alarmes
- Trabalhar com métricas de performance no console do CloudWatch


## Visualizar dados de performance do cluster

Ao usar métricas de cluster no Amazon Redshift, você pode fazer as seguintes tarefas de performance comuns:

- Determine se as métricas de cluster são anormais em um período especificado e, em caso afirmativo, identifique as consultas responsáveis pela ocorrência de performance.
- Verifique se as consultas históricas ou atuais estão afetando a performance do cluster. Se identificar uma consulta problemática, você poderá visualizar detalhes sobre ela, incluindo a performance do cluster durante a execução da consulta. Você pode usar essas informações para diagnosticar o motivo da lentidão da consulta e ver o que pode ser feito para melhorar a performance dela.

Para visualizar os dados de performance

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

2. No menu de navegação, escolha Clusters e, em seguida, o nome de um cluster na lista para abrir os detalhes. Os detalhes do cluster são exibidos, incluindo as guias Performance do cluster, Monitoramento de consultas, Banco de dados, Datashares, Programações, Manutenção e Propriedades.
3. Escolha a guia Cluster performance (Performance do cluster) para obter informações que incluem o seguinte:

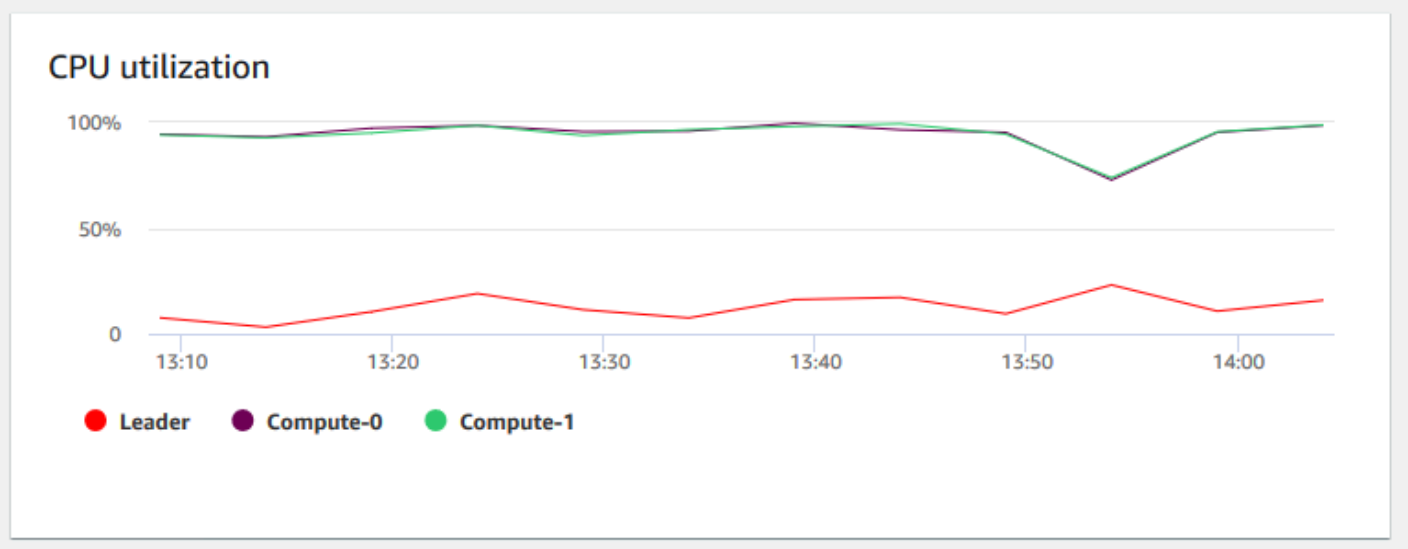
   - Utilização da CPU
   - Percentage disk space used (Porcentagem utilizada de espaço em disco)
   - Conexões de banco de dados
   - Status de integridade
   - Query duration (Duração de consultas)
   - Query throughput (Taxa de transferência de consultas)
   - Ação de escalabilidade da simultaneidade

   Muitas métricas novas estão disponíveis. Para ver as métricas disponíveis e escolher quais são exibidas, escolha o ícone Preferences (Preferências)

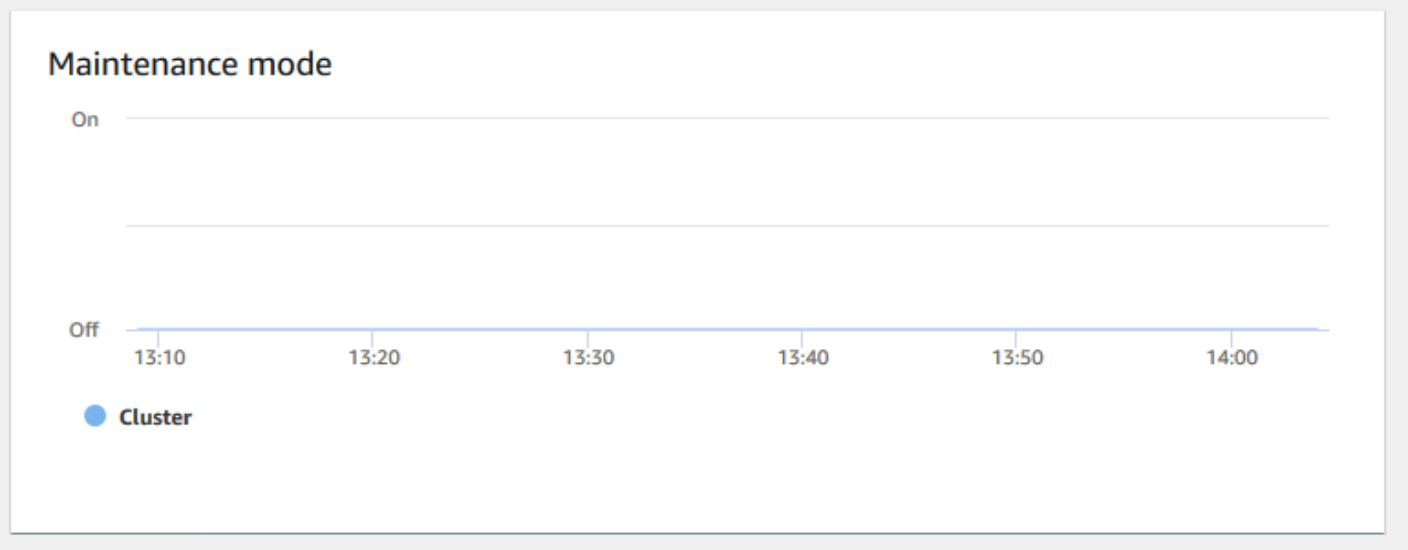
## Gráficos de performance de cluster

Os exemplos a seguir mostram alguns dos gráficos exibidos no novo console do Amazon Redshift.

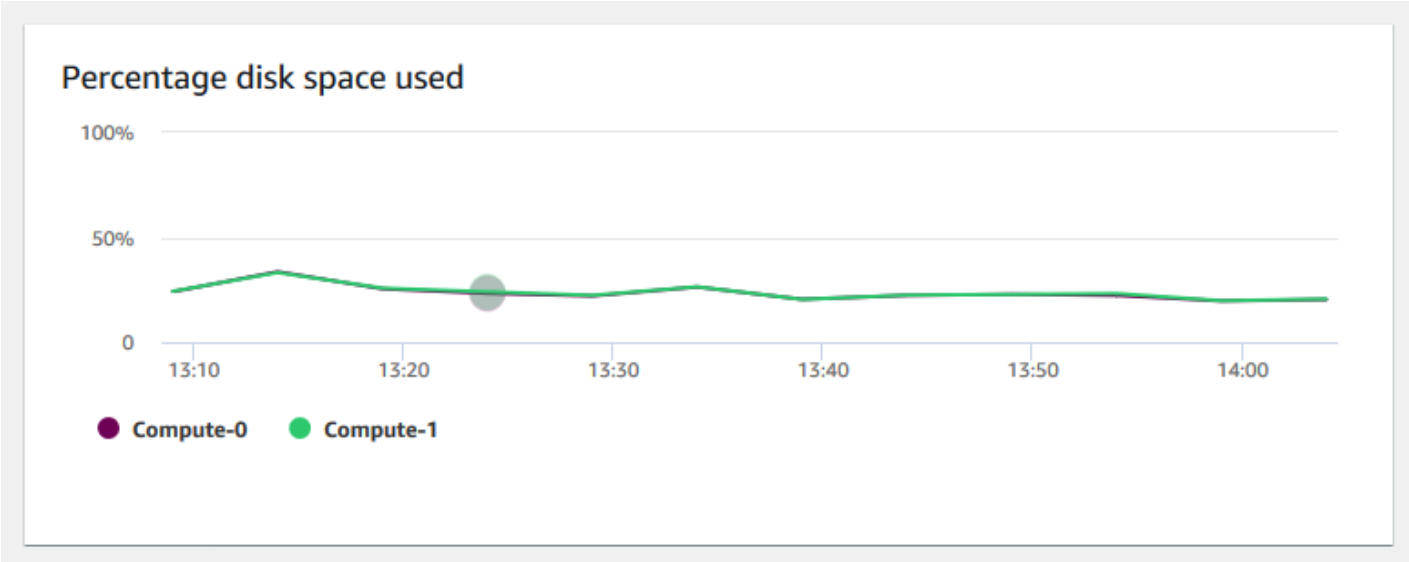
- Utilização da CPU – Mostra a porcentagem de utilização da CPU para todos os nós (líder e computação). Para localizar um horário em que o uso do cluster seja mais baixo antes de agendar a migração do cluster ou outras operações que consomem recursos, monitore este gráfico para ver a utilização da CPU por nó individual ou por todos os nós.



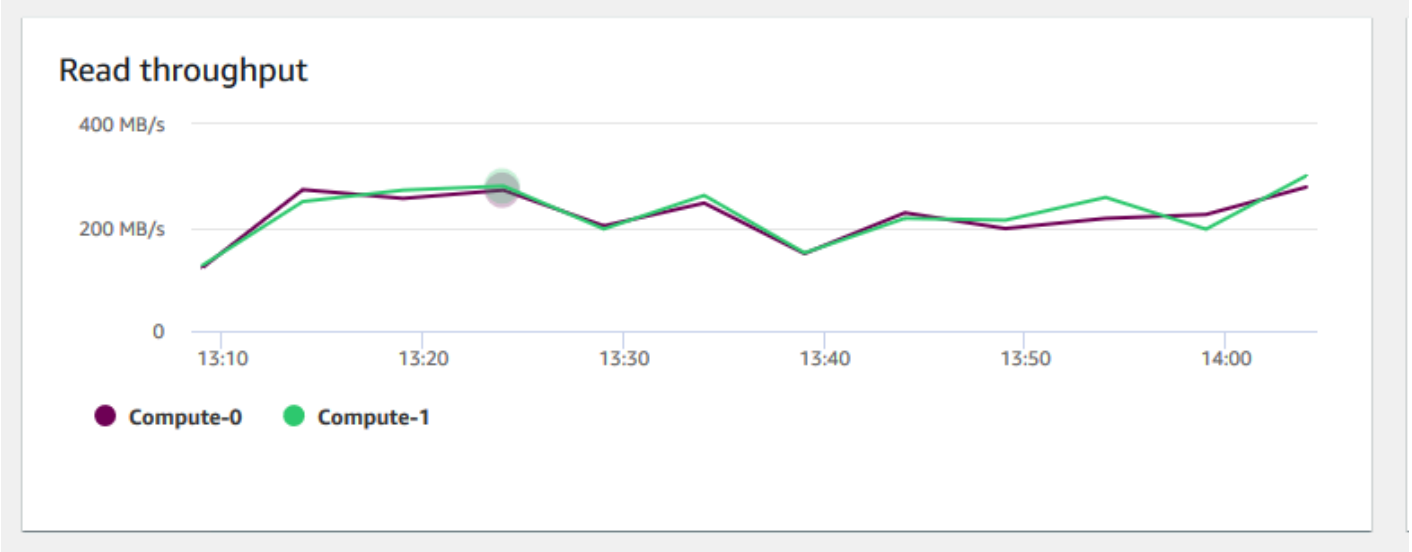

- Modo de manutenção – Mostra se o cluster está no modo de manutenção em um horário escolhido usando os indicadores `On` e `Off`. É possível ver a hora em que o cluster está passando por manutenção. Depois, é possível correlacionar esse tempo com as operações realizadas no cluster para estimar seus tempos de inatividade futuros para eventos recorrentes.



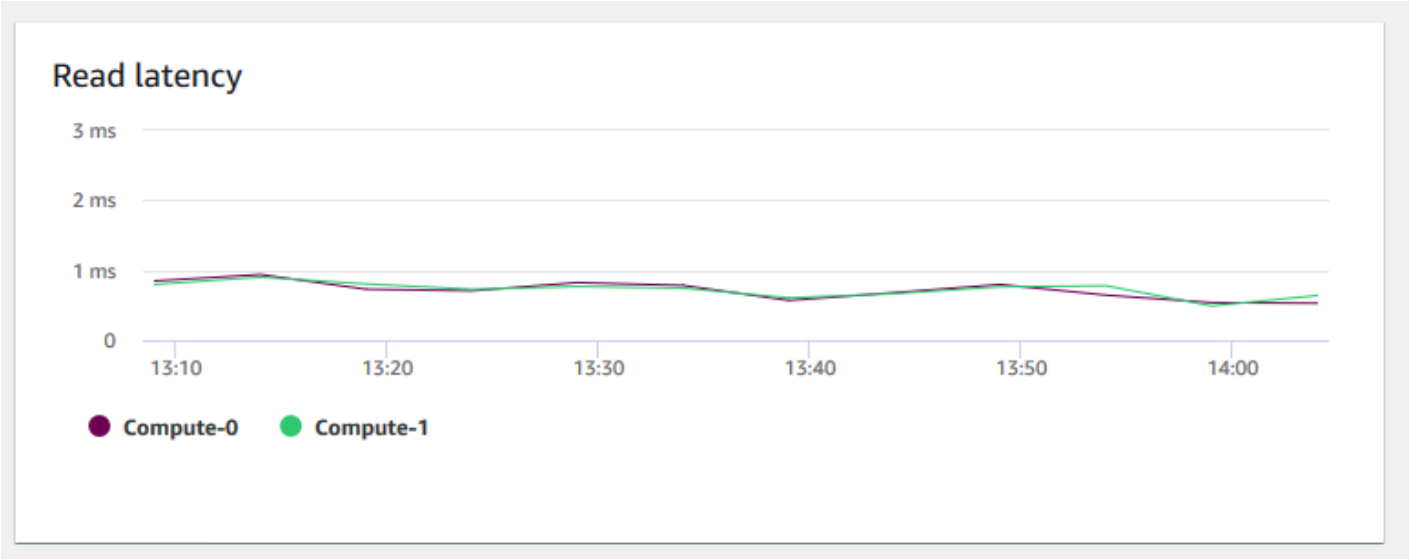

- Porcentagem de espaço em disco usado – Mostra a porcentagem de uso de espaço em disco por cada nó de computação, e não para o cluster como um todo. É possível explorar esse gráfico para monitorar a utilização do disco. Operações de manutenção, como VACUUM e COPY, usam espaço de armazenamento temporário intermediário para suas operações de classificação, portanto, é esperado um pico no uso do disco.



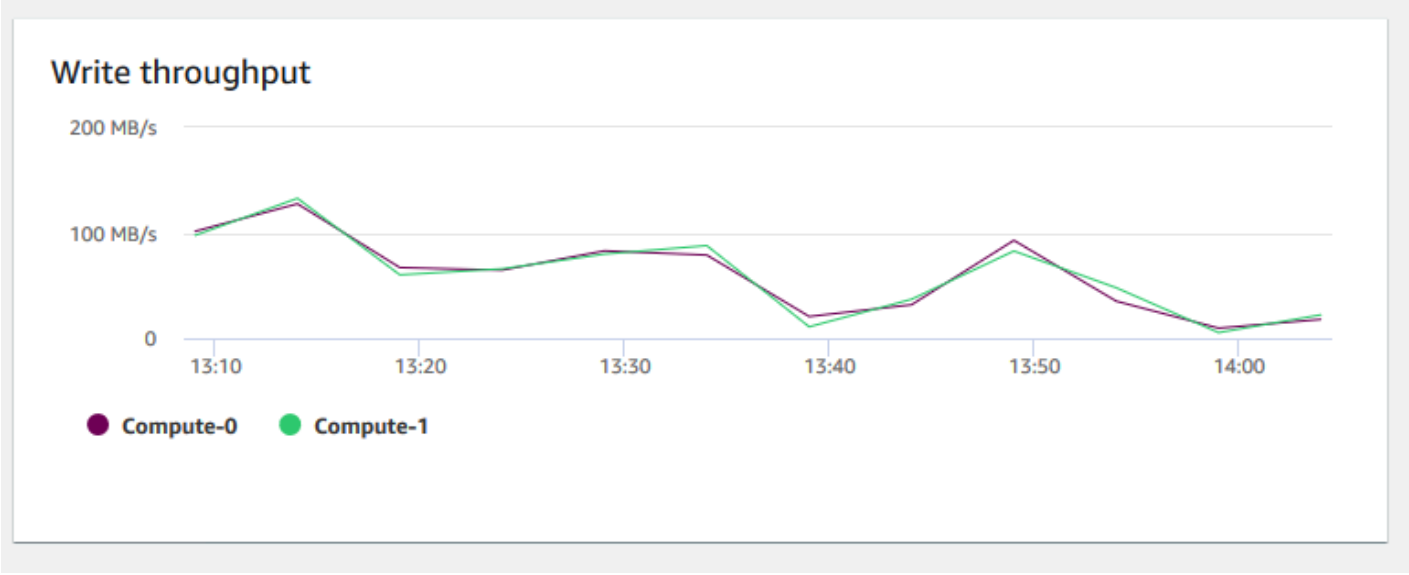

- Taxa de transferência de leitura – Mostra o número médio de megabytes lidos do disco por segundo. É possível avaliar esse gráfico para monitorar o aspecto físico correspondente do cluster. Essa taxa de transferência não inclui o tráfego de rede entre instâncias no cluster e o seu volume.



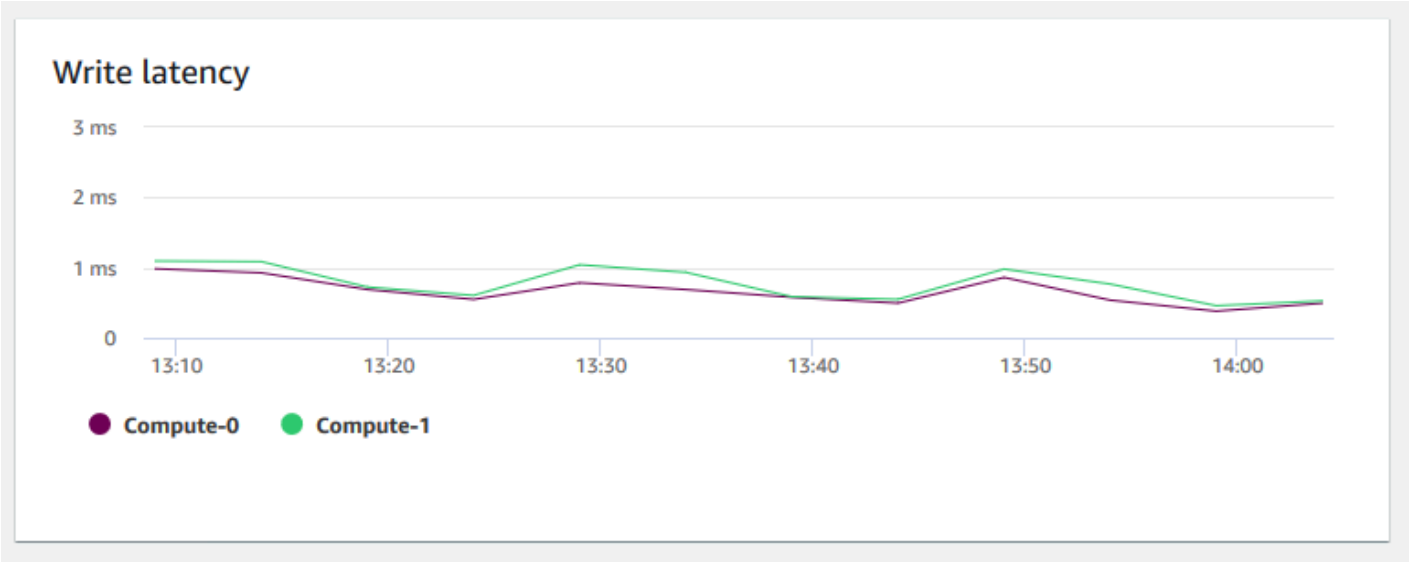

- Latência de leitura – Mostra a quantidade média de tempo gasto para operações de E/S de leitura de disco por milissegundo. É possível visualizar os tempos de resposta dos dados a serem retornados. Quando a latência é alta, isso significa que o remetente gasta mais tempo ocioso (não enviando novos pacotes), o que reduz a rapidez com que a taxa de transferência aumenta.



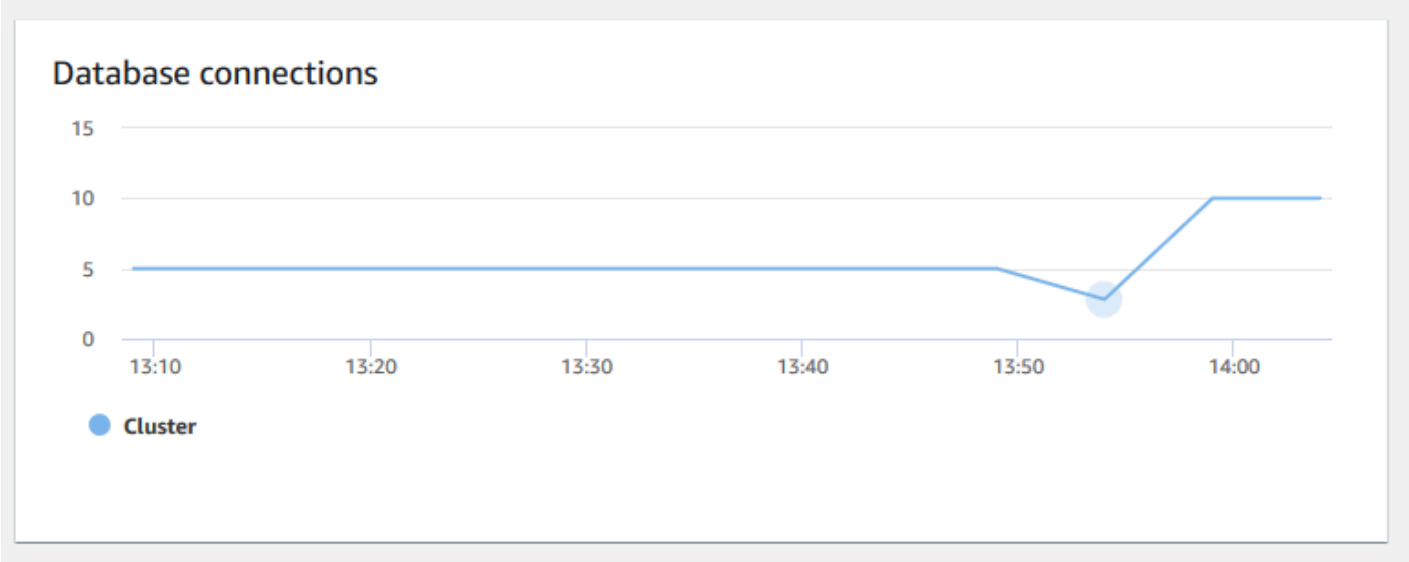

- Taxa de transferência de gravação – Mostra o número médio de megabytes gravados no disco por segundo. É possível avaliar essa métrica para monitorar o aspecto físico correspondente do cluster. Essa taxa de transferência não inclui o tráfego de rede entre instâncias no cluster e o seu volume.



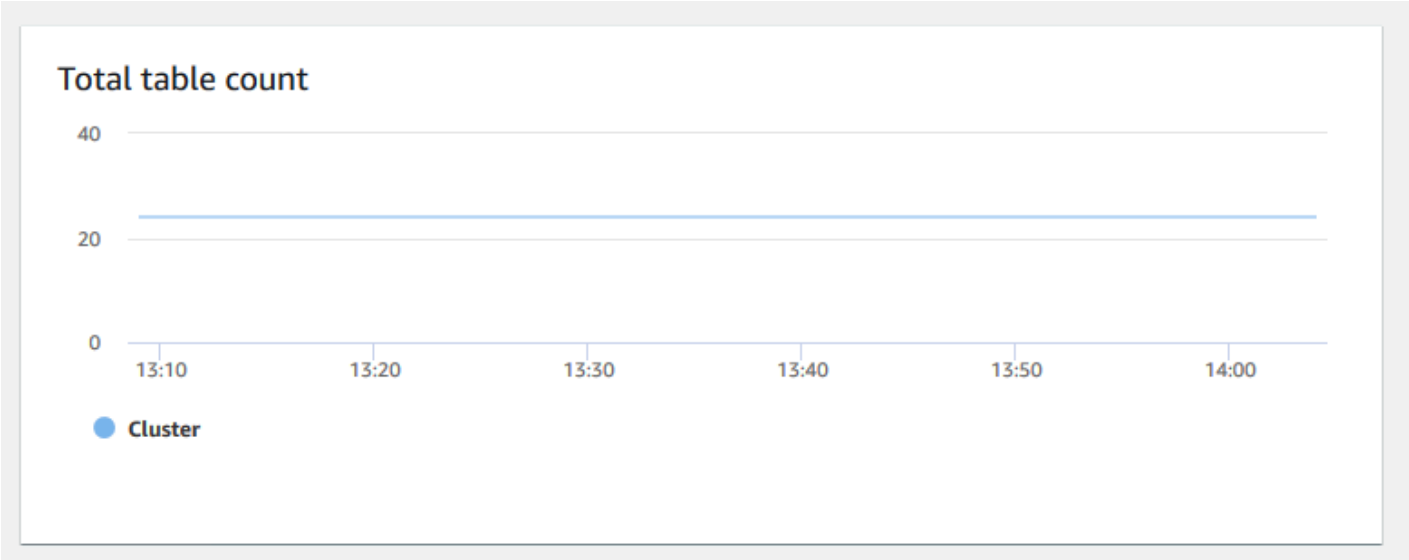

- Latência de gravação – Mostra o tempo médio em milissegundos gasto para operações de E/S de gravação de disco. É possível avaliar o tempo para que a confirmação de gravação seja retornada. Quando a latência é alta, isso significa que o remetente gasta mais tempo ocioso (não enviando novos pacotes), o que reduz a rapidez com que a taxa de transferência aumenta.



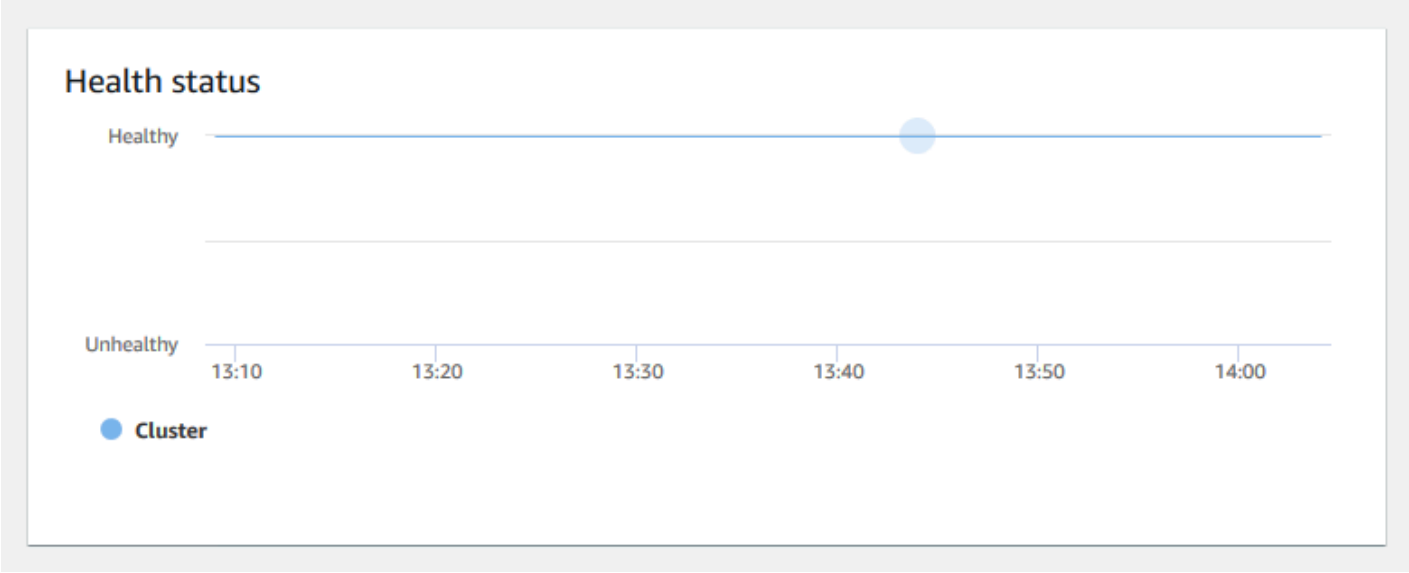

- Conexões de banco de dados – Mostra o número de conexões de banco de dados a um cluster. É possível usar esse gráfico para ver quantas conexões são estabelecidas com o banco de dados e encontrar um horário em que o uso do cluster é menor.



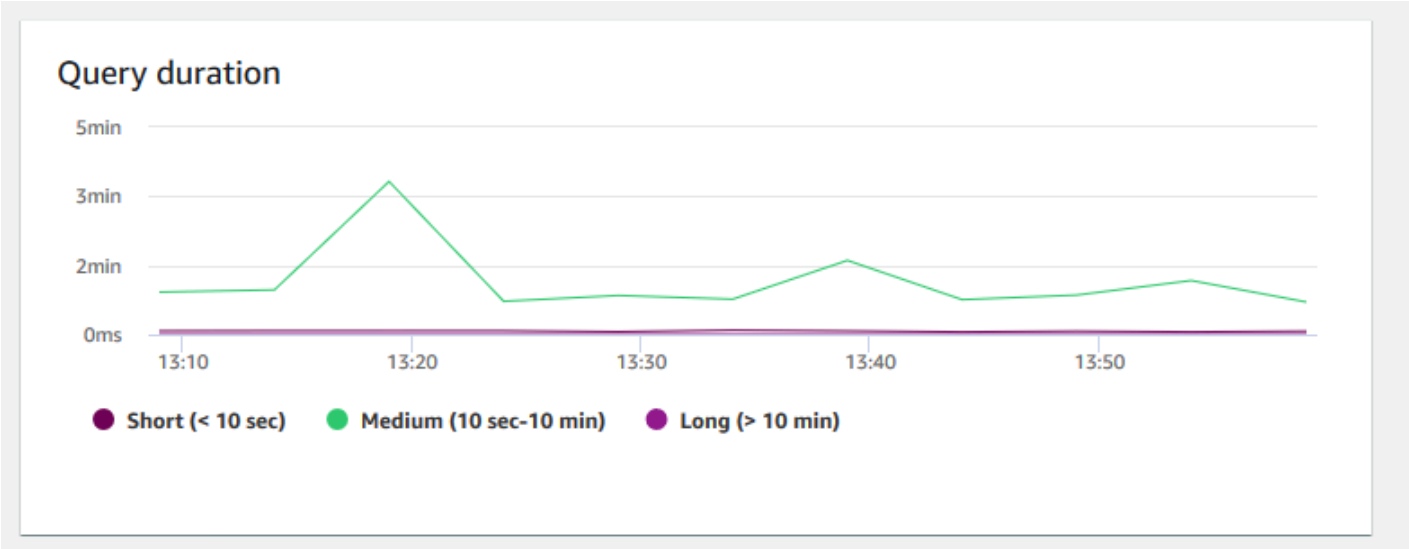

- Contagem total de tabelas – Mostra o número de tabelas de usuário abertas em um determinado momento dentro de um cluster. É possível monitorar a performance do cluster quando a contagem de tabelas abertas é alta.



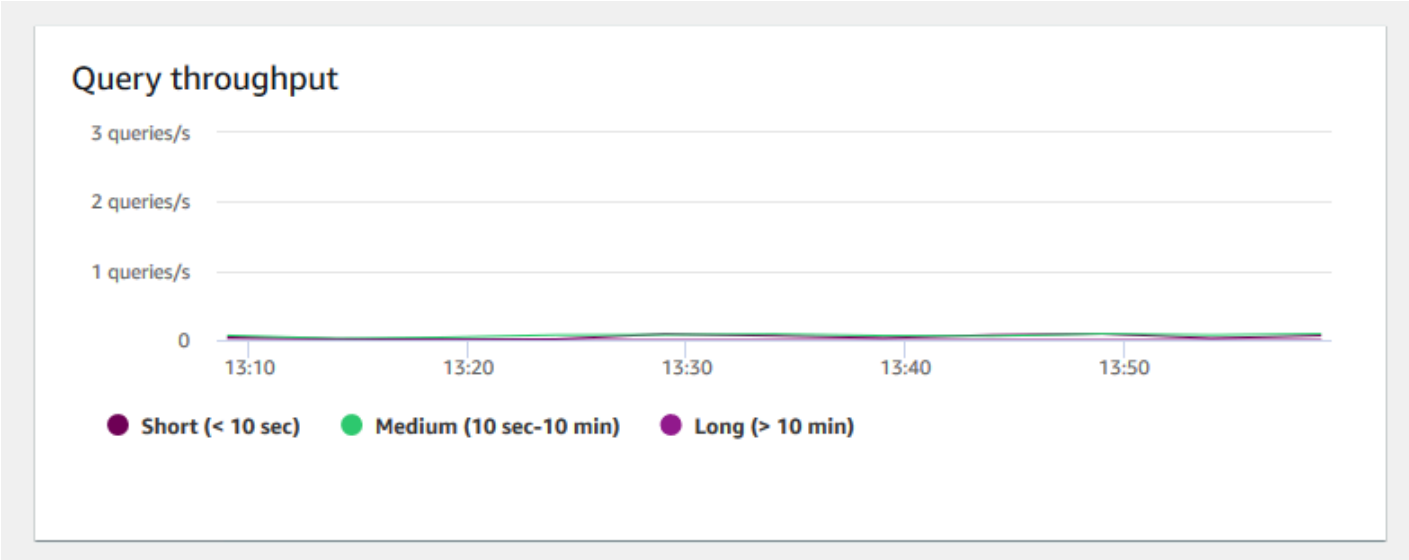

- Status de integridade – Indica a integridade do cluster como `Healthy` ou `Unhealthy`. Se o cluster puder se conectar ao banco de dados e executar uma consulta simples com êxito, o cluster será considerado íntegro. Caso contrário, o cluster está com problemas. Um status não saudável pode ocorrer quando o banco de dados do cluster está sob carga extremamente pesada ou se houver um problema de configuração com um banco de dados no cluster.



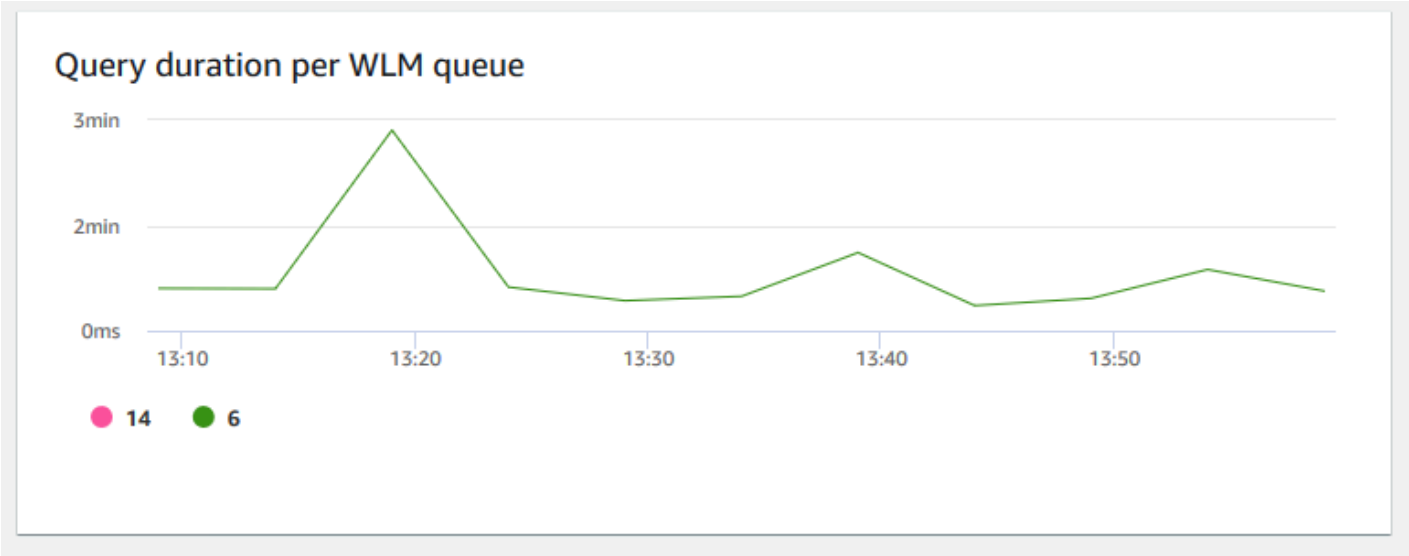

- Duração de consultas – Mostra a quantidade média de tempo para concluir uma consulta em microssegundos. É possível comparar os dados nesse gráfico para medir a performance de E/S dentro do cluster e ajustar suas consultas mais demoradas, se necessário.



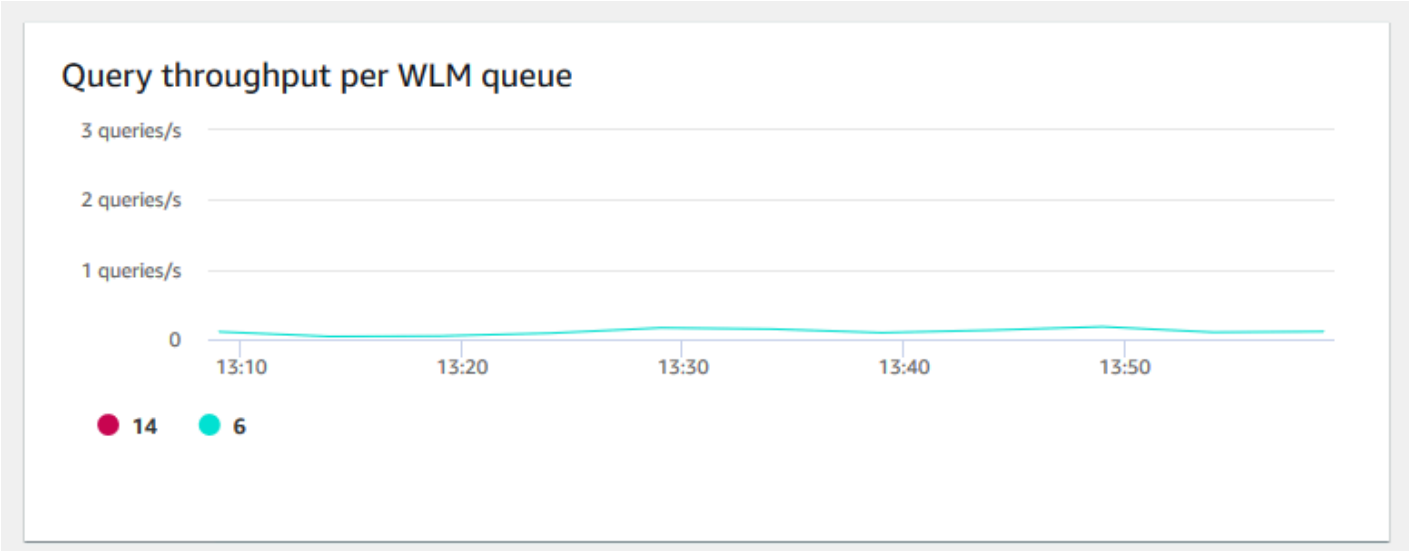

- Taxa de transferência de consultas – Mostra o número médio de consultas concluídas por segundo. É possível analisar dados nesse gráfico para medir a performance do banco de dados e caracterizar a capacidade do sistema de oferecer suporte a um workload multiusuário de forma equilibrada.



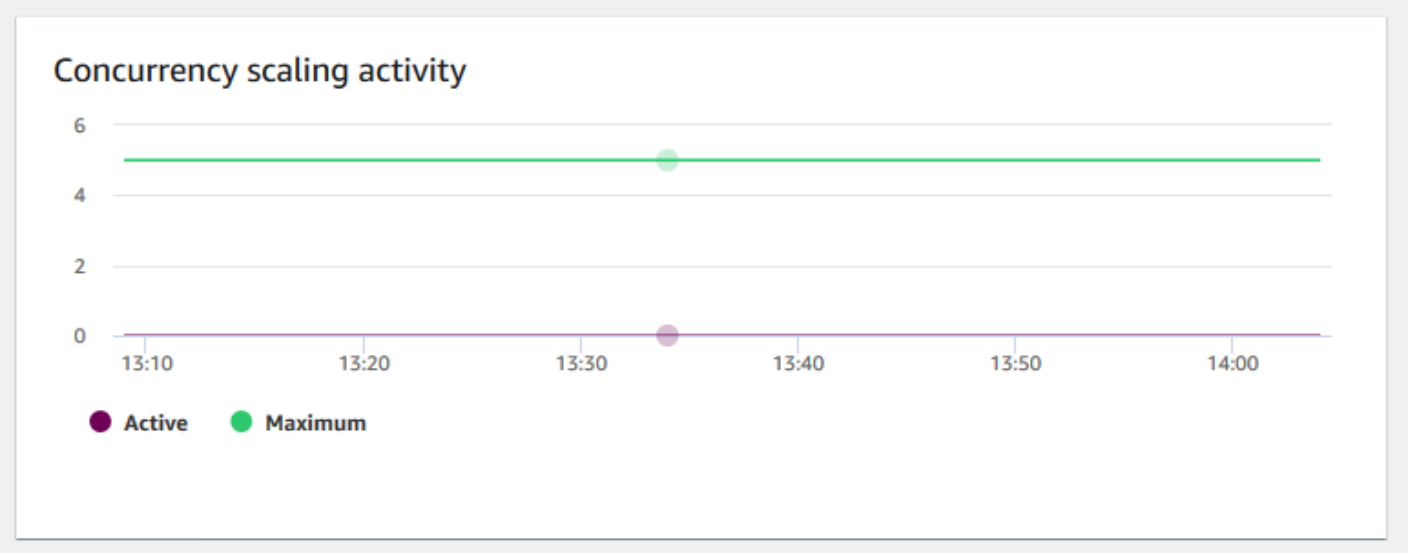

- Duração de consultas por fila WLM – Mostra a quantidade média de tempo para concluir uma consulta em microssegundos. É possível comparar os dados nesse gráfico para medir a performance de E/S por fila de WLM e ajustar suas consultas mais demoradas, se necessário.




- Taxa de transferência de consulta por fila WLM – Mostra o número médio de consultas concluídas por segundo. É possível analisar dados nesse gráfico para medir a performance do banco de dados por fila do WLM.




- Atividade de escalabilidade de simultaneidade – Mostra o número de clusters de escalabilidade de simultaneidade ativos. Quando a escalabilidade de simultaneidade está habilitado, o Amazon Redshift adiciona automaticamente capacidade de cluster adicional quando você precisa para processar um aumento nas consultas de leitura simultâneas.




## Visualizar dados do histórico de consultas

Você pode usar as métricas de histórico de consulta no Amazon Redshift para fazer o seguinte:

- Isolar e diagnosticar problemas de performance de consulta.
- Comparar métricas de tempo de execução de consulta e métricas de performance de cluster na mesma linha de tempo para ver como as duas podem estar relacionadas. Isso ajuda a identificar consultas com baixa performance, procurar consultas em gargalo e saber se você precisa redimensionar seu cluster para seu workload.
- Fazer busca detalhada nos detalhes de uma consulta específica escolhendo-a na linha do tempo. Quando o ID da consulta e outras propriedades são exibidas em uma linha abaixo do gráfico, é possível selecionar a consulta para ver os detalhes dela. Os detalhes incluem, por exemplo, a instrução SQL da consulta, os detalhes de execução e o plano de consulta. Para obter mais informações, consulte Visualizar detalhes da consulta.
- Determine se seus trabalhos de carga foram concluídos com êxito e atendem aos contratos de nível de serviço (SLAs).

Como exibir dados de histórico de consultas

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters e o nome do cluster na lista para abrir os respectivos detalhes. Os detalhes do cluster são exibidos, incluindo as guias Performance do cluster,

Monitoramento de consultas, Banco de dados, Datashares, Programações, Manutenção e Propriedades.

3. Escolha a guia Query monitoring (Monitoramento de consultas) para obter as métricas sobre suas consultas.
4. Na seção Monitoramento de consultas escolha a guia Histórico de consultas.

   Usando controles na janela, você pode alternar entre Lista de Consultas e Métricas de cluster.

   Quando Lista de consultas é escolhido, a guia inclui os seguintes gráficos:

   - Tempo de execução da consulta – A atividade de consulta em uma linha do tempo. Use esse gráfico para ver quais consultas estão sendo executadas no mesmo período. Escolha uma consulta para visualizar mais detalhes de execução de consulta. O eixo x mostra o período selecionado. É possível filtrar as consultas gráficas em execução, concluídas, cargas, etc. Cada barra representa uma consulta, e o tamanho da barra representa o tempo de execução desde o início da barra até o fim. As consultas podem incluir instruções de manipulação de dados SQL (como SELECT, INSERT, DELETE) e cargas (como COPY). Por padrão, as 100 consultas mais longas em execução são mostradas para o período selecionado.
   - Consultas e cargas – Lista de consultas e cargas executadas no cluster. A janela inclui uma opção para Encerrar consulta se uma consulta estiver em execução no momento.

   Quando Métricas do cluster é escolhido, a guia inclui os seguintes gráficos:

   - Tempo de execução da consulta – A atividade de consulta em uma linha do tempo. Use esse gráfico para ver quais consultas estão sendo executadas no mesmo período. Escolha uma consulta para visualizar mais detalhes de execução de consulta.
   - Utilização da CPU – A utilização da CPU do cluster por nó líder e média de nós de computação.
   - Capacidade de armazenamento usada – A porcentagem da capacidade de armazenamento usada.
   - Conexões de banco de dados ativas – O número de conexões de banco de dados ativas com o cluster.

Considere o seguinte ao trabalhar com os gráficos do histórico de consultas:

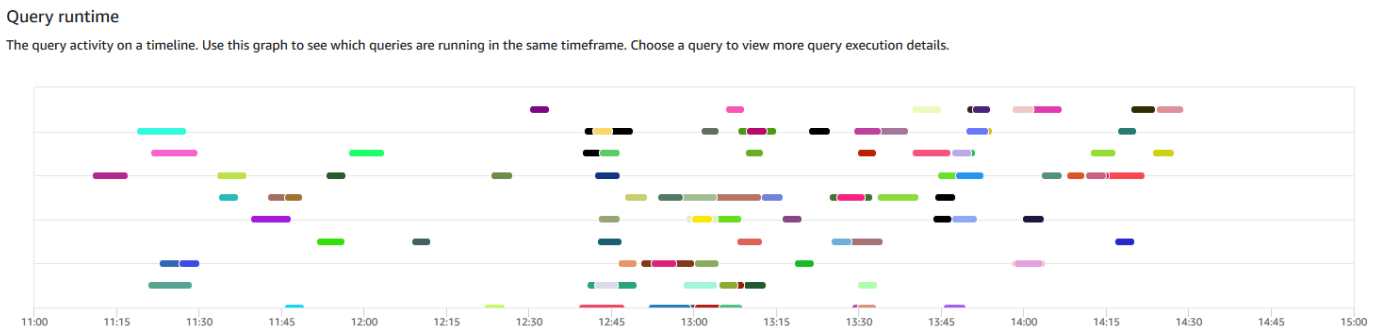
- Escolha uma barra que represente uma consulta específica no gráfico Tempo de execução da consulta para ver detalhes sobre essa consulta. Também é possível escolher um ID de consulta na lista Consultas e cargas para ver seus detalhes.
- Você pode deslizar para selecionar uma seção do gráfico Tempo de execução da consulta para ampliar e exibir um período específico.
- No gráfico Tempo de execução da consulta para que todos os dados sejam considerados pelo filtro escolhido, avance por todas as páginas indicadas na lista Consultas e cargas.
- É possível alterar quais colunas e o número de linhas exibidas na lista Consultas e cargas usando a janela de preferências exibida pelo ícone de engrenagem de configurações.
- A lista Consultas e cargas também pode ser exibida navegando a partir do ícone Consultas do navegador esquerdo, Consultas e cargas. Para obter mais informações, consulte Visualizar consultas e cargas.

## Gráficos de histórico de consultas

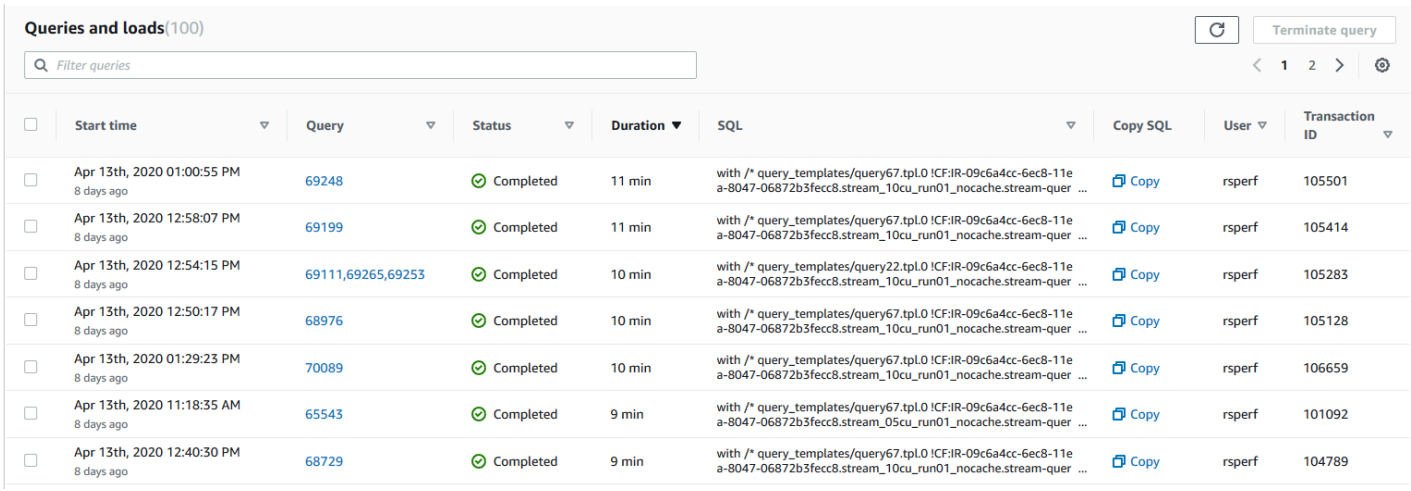
Os exemplos a seguir mostram gráficos que são exibidos no novo console do Amazon Redshift.

> **Note**
>
> Os gráficos do console do Amazon Redshift contêm apenas dados para as 100.000 consultas mais recentes.

- Tempo de execução da consulta




- Consultas e cargas



**Queries and loads**(100)

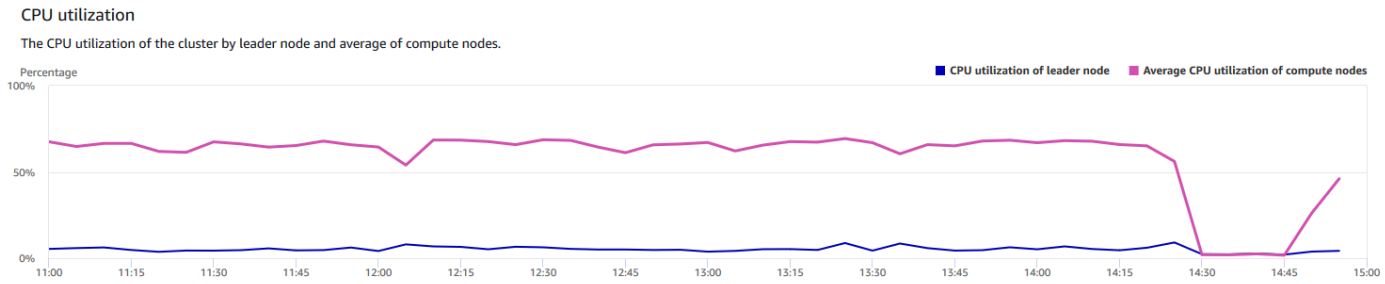
Filter queries

Terminate query

1 2

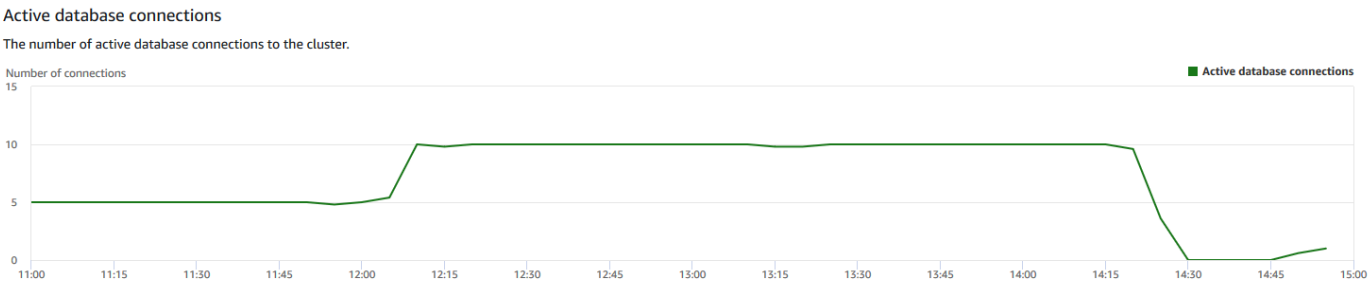
| Start time | Query | Status | Duration | SQL | Copy SQL | User | Transaction ID |
|---|---|---|---|---|---|---|---|
| Apr 13th, 2020 01:00:55 PM 8 days ago | 69248 | Completed | 11 min | with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ... | Copy | rsperf | 105501 |
| Apr 13th, 2020 12:58:07 PM 8 days ago | 69199 | Completed | 11 min | with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ... | Copy | rsperf | 105414 |
| Apr 13th, 2020 12:54:15 PM 8 days ago | 69111,69265,69253 | Completed | 10 min | with /* query_templates/query22.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ... | Copy | rsperf | 105283 |
| Apr 13th, 2020 12:50:17 PM 8 days ago | 68976 | Completed | 10 min | with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ... | Copy | rsperf | 105128 |
| Apr 13th, 2020 01:29:23 PM 8 days ago | 70089 | Completed | 10 min | with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ... | Copy | rsperf | 106659 |
| Apr 13th, 2020 11:18:35 AM 8 days ago | 65543 | Completed | 9 min | with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_05cu_run01_nocache.stream-quer ... | Copy | rsperf | 101092 |
| Apr 13th, 2020 12:40:30 PM 8 days ago | 68729 | Completed | 9 min | with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ... | Copy | rsperf | 104789 |

- Utilização da CPU




- Capacidade de armazenamento utilizada

- Conexões de banco de dados ativas



# Visualizar dados de performance do banco de dados

Você pode usar as métricas de performance do banco de dados no Amazon Redshift para fazer o seguinte:

- Analise o tempo gasto pelas consultas por etapas de processamento. É possível procurar tendências incomuns na quantidade de tempo gasto em uma etapa.
- Analise o número de consultas, duração e taxa de transferência de consultas por intervalos de duração (curto, médio, longo).
- Procure tendências no tempo de espera de consulta por prioridade de consulta (Menor, Baixa, Normal, Alta, Maior, Crítica).
- Procure tendências na duração da consulta, na taxa de transferência ou no tempo de espera por fila do WLM.

Como exibir dados de performance do banco de dados

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters e o nome do cluster na lista para abrir os respectivos detalhes. Os detalhes do cluster são exibidos, incluindo as guias Performance do cluster, Monitoramento de consultas, Banco de dados, Datashares, Prograções, Manutenção e Propriedades.
3. Escolha a guia Query monitoring (Monitoramento de consultas) para obter as métricas sobre suas consultas.
4. Na seção Monitoramento de consultas, escolha a guia Performance do banco de dados.

   Usando controles na janela, você pode alternar entre Métricas do cluster e Métricas da fila do WLM.

   Quando Métricas do cluster é escolhido, a guia inclui os seguintes gráficos:

   - Quebra de execução do workload – O tempo usado nos estágios de processamento de consulta.
   - Consultas por intervalo de duração – O número de consultas curtas, médias e longas.
   - Taxa de transferência de consultas – O número médio de consultas concluídas por segundo.
   - Duração da consulta – O tempo médio para concluir uma consulta.

- Tempo médio de espera da fila por prioridade – O tempo total gasto pelas consultas esperando na fila do WLM por prioridade da consulta.

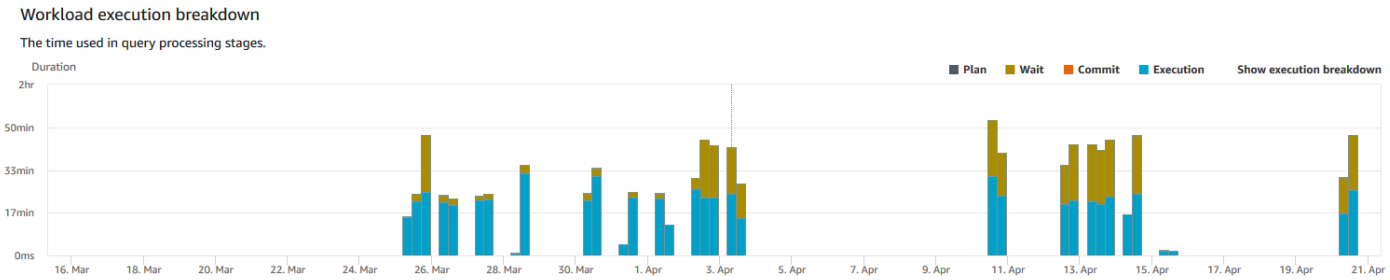
Quando Métricas da fila do WLM, a guia inclui os seguintes gráficos:

- Duração da consulta por fila – A duração média da consulta por fila WLM.
- Taxa de transferência da consulta por fila – O número médio de consultas concluídas por segundo pela fila WLM.
- Tempo de espera da consulta por fila – A duração média de consultas gastas esperando por fila WLM.

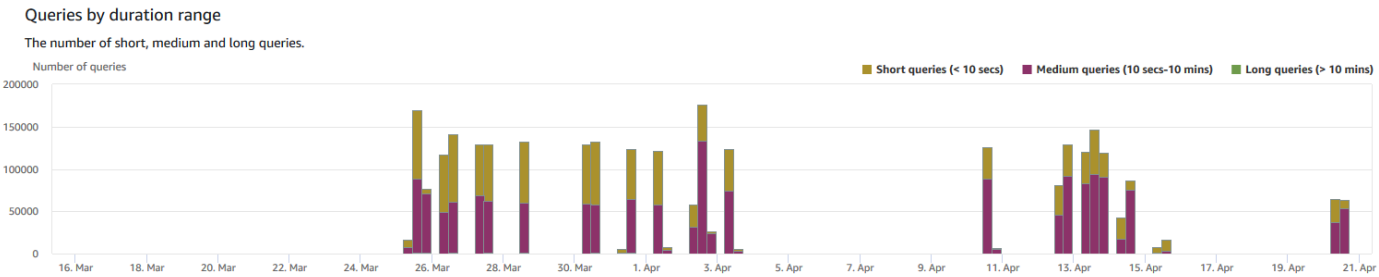
## Gráficos de performance do banco de dados

Os exemplos a seguir mostram gráficos que são exibidos no novo console do Amazon Redshift.

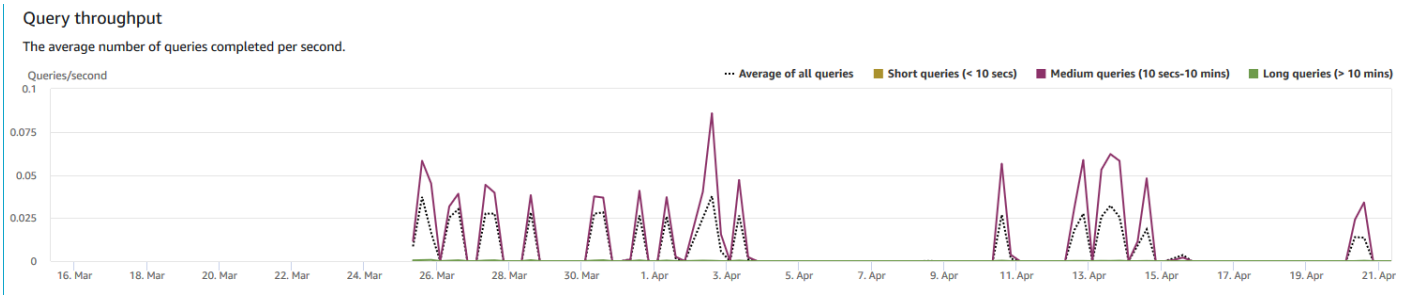
- Detalhamento da execução da carga de trabalho



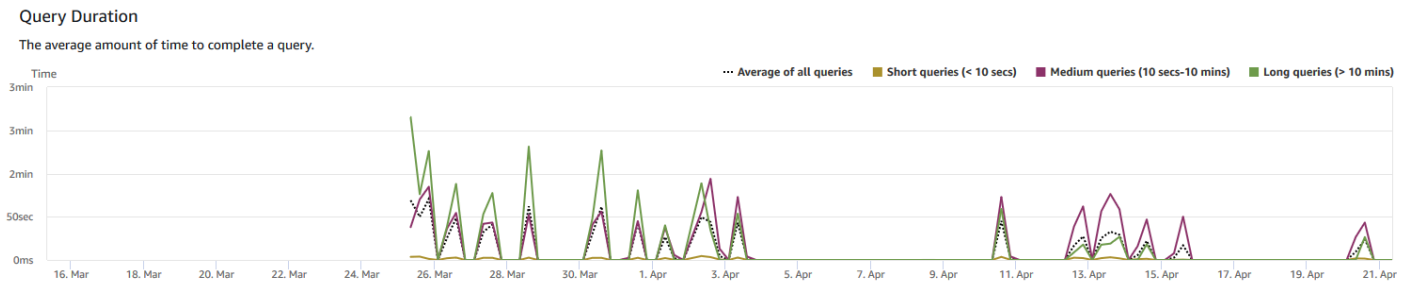

- Consultas por intervalo de duração



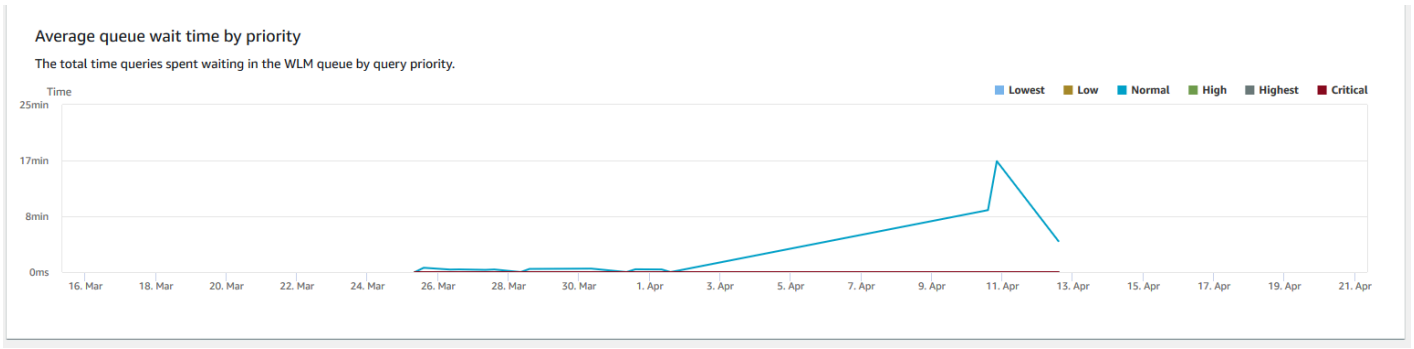

- Query throughput (Taxa de transferência de consultas)



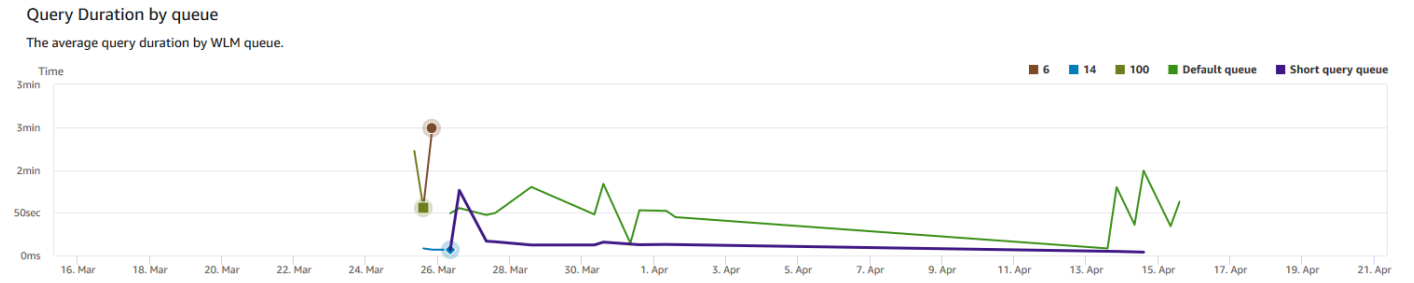

- Query duration (Duração de consultas)



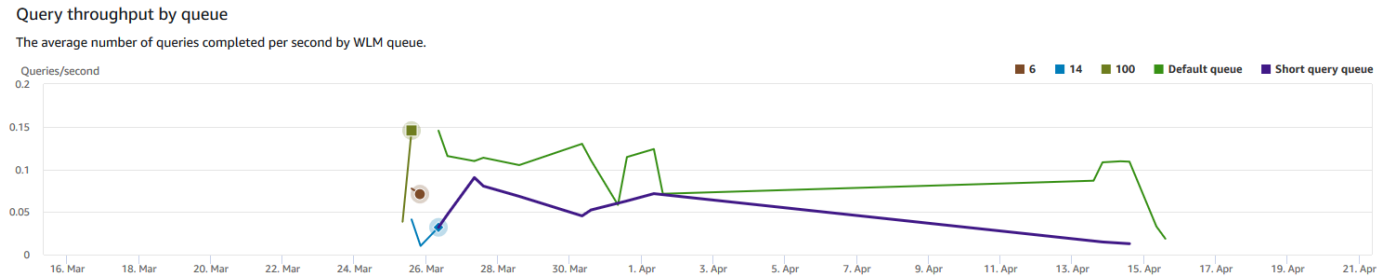

- Tempo médio de espera da fila por prioridade



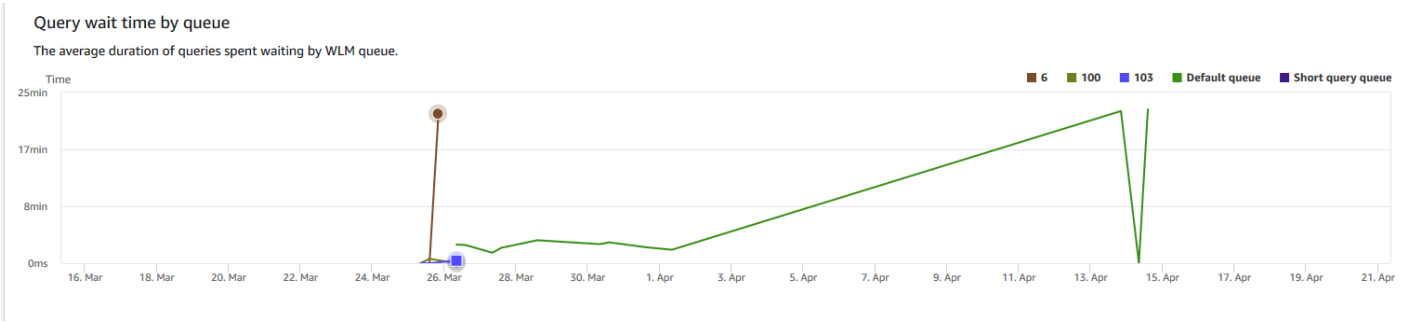

- Duração da consulta por fila




- Taxa de transferência de consulta por fila




- Tempo de espera da consulta por fila




# Visualizar dados de escalabilidade da simultaneidade e simultaneidade do workload

Ao usar métricas de escalabilidade de simultaneidade no Amazon Redshift, você pode fazer o seguinte:

- Analise se é possível reduzir o número de consultas em fila habilitando a escalabilidade da simultaneidade. É possível comparar por fila do WLM ou por todas as filas do WLM.
- Visualize a ação de escalabilidade da simultaneidade nos clusters de escalabilidade da simultaneidade. Isso pode informá-lo se a escalabilidade da simultaneidade é limitada por `max_concurrency_scaling_clusters`. Se esse for o caso, você pode aumentar `max_concurrency_scaling_clusters` no parâmetro de banco de dados.
- Visualize o uso total da escalabilidade da simultaneidade somada em todos os clusters de escalabilidade da simultaneidade.

Para exibir da escalabilidade da simultaneidade

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

2. No menu de navegação, escolha Clusters e o nome do cluster na lista para abrir os respectivos detalhes. Os detalhes do cluster são exibidos, incluindo as guias Performance do cluster, Monitoramento de consultas, Banco de dados, Datashares, Programações, Manutenção e Propriedades.
3. Escolha a guia Query monitoring (Monitoramento de consultas) para obter as métricas sobre suas consultas.
4. Na seção Monitoramento de consultas, escolha a guia Simultaneidade do workload.

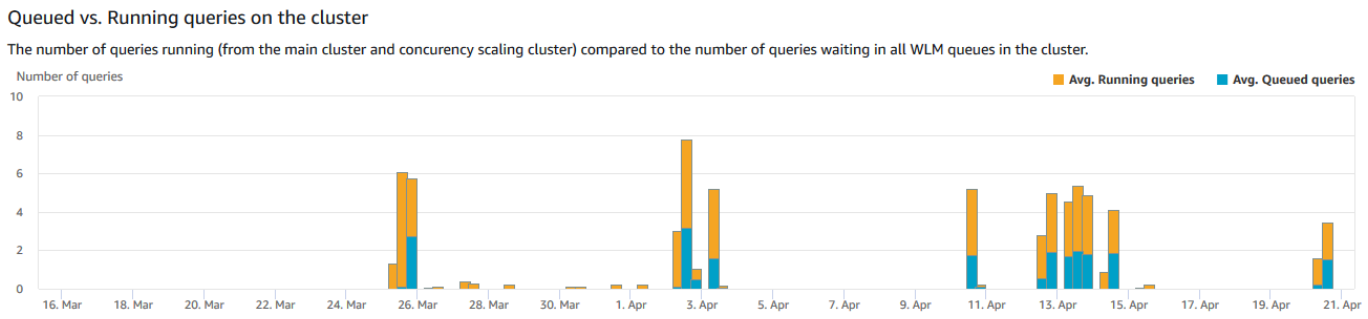
   A guia inclui os seguintes gráficos:

   - Consultas enfileiradas vs. em execução no cluster – O número de consultas em execução (do cluster principal e cluster de escalabilidade de simultaneidade) em comparação com o número de consultas aguardando em todas as filas WLM no cluster.
   - Consultas enfileiradas vs. em execução por fila – O número de consultas em execução (do cluster principal e cluster de escalabilidade de simultaneidade) em comparação com o número de consultas aguardando em cada fila WLM.
   - Atividade de escalabilidade de simultaneidade – O número de clusters de escalabilidade de simultaneidade que estão processando ativamente as consultas.
   - Uso de escalabilidade de simultaneidade – O uso de clusters de escalabilidade de simultaneidade que têm atividade de processamento de consulta ativa.

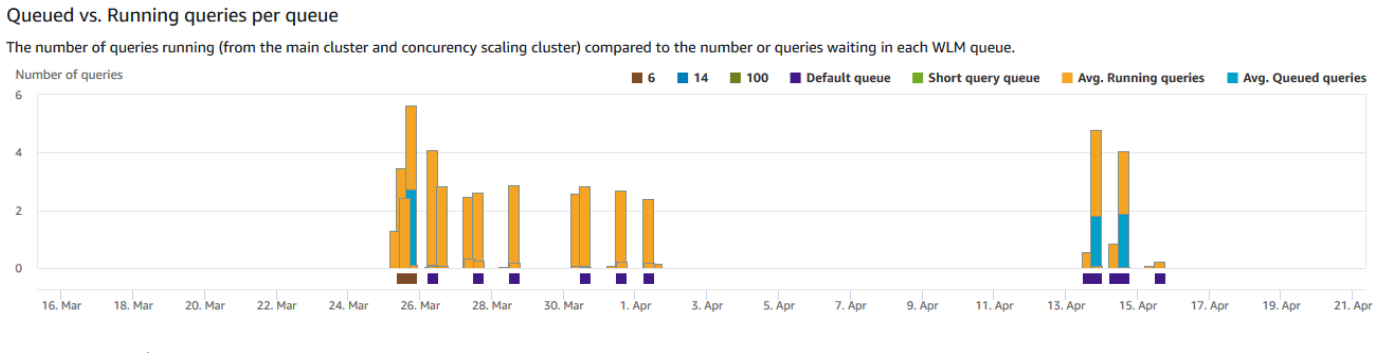
## Gráficos de simultaneidade do workload

Os exemplos a seguir mostram gráficos que são exibidos no novo console do Amazon Redshift. Para criar grafos semelhantes no Amazon CloudWatch, você pode usar a escalabilidade simultânea e as métricas de WLM do CloudWatch. Para obter mais informações sobre as métricas do CloudWatch para o Amazon Redshift, consulte Monitorar o Amazon Redshift usando métricas do CloudWatch.

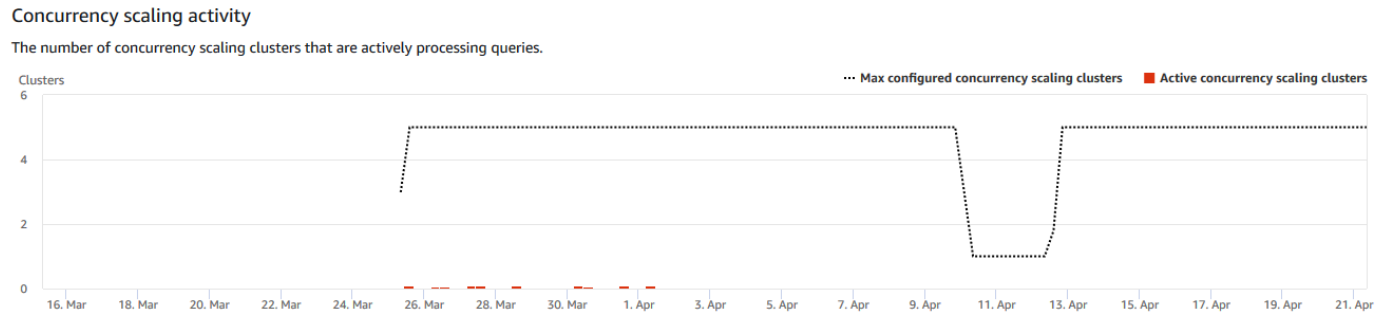
- Consultas em fila vs. em execução no cluster



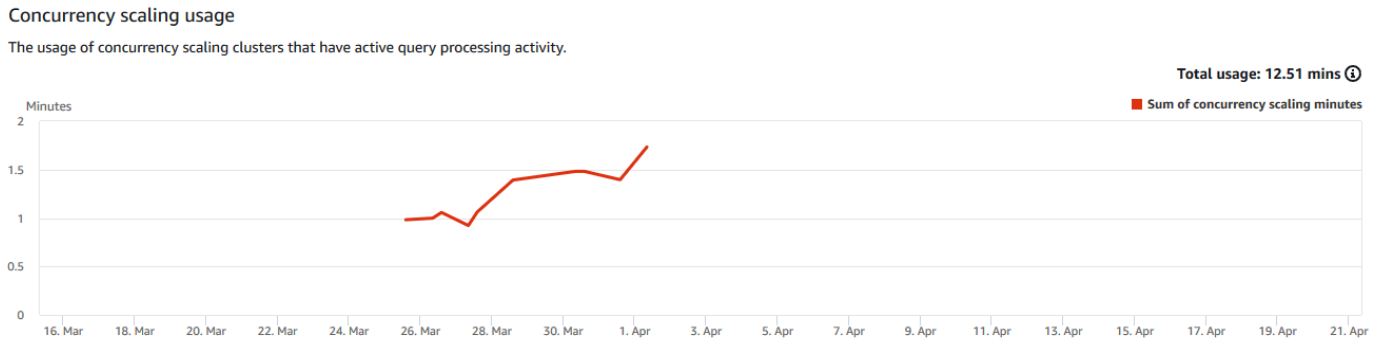
- Consultas em fila vs. em execução por fila




- Ação de escalabilidade da simultaneidade




- Concurrency scaling usage (Uso de escalabilidade da simultaneidade)




# Visualizar consultas e cargas

O console do Amazon Redshift fornece informações sobre consultas e cargas que são executadas no banco de dados. Você pode usar essas informações para identificar e solucionar problemas de consultas que demoram muito para serem processadas e criam gargalos que impedem outras consultas de serem processadas de maneira eficiente. Você pode usar as informações de consultas no console do Amazon Redshift para monitorar o processamento de consultas.

Para exibir dados de performance de consultas

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Queries and loads (Consultas e cargas) para exibir a lista de consultas de sua conta.

   Por padrão, a lista exibe consultas de todos os seus clusters nas últimas 24 horas. É possível alterar o escopo da data exibida no console.

   > **Important**
   >
   > A guia Queries and loads (Consultas e cargas) exibe as consultas executadas por mais tempo no sistema, até 100 consultas.

## Encerrar uma consulta em execução

Você também pode usar a página Queries (Consultas) para encerrar uma consulta em andamento no momento.

> **Note**
>
> A capacidade de encerrar consultas e carregamentos no console do Amazon Redshift requer permissão específica. Se você quiser que os usuários tenham permissão para encerrar consultas e carregamentos, certifique-se de adicionar a ação `redshift:CancelQuerySession` à sua política do AWS Identity and Access Management (IAM). Este requisito se aplica se você selecionar a política gerenciada da AWS somente leitura do Amazon Redshift ou criar uma política personalizada no IAM. Os usuários que têm a política de acesso total do Amazon Redshift já têm a permissão necessária para encerrar consultas e carregamentos. Para obter mais informações sobre ações em políticas do IAM para Amazon Redshift, consulte Gerenciamento de acesso aos recursos.

Para encerrar uma consulta em execução

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

2. No menu de navegação, escolha Queries and loads (Consultas e cargas) para exibir a lista de consultas de sua conta.
3. Escolha a consulta em execução que você deseja encerrar na lista e escolha Terminate query (Encerrar consulta).

## Visualizar detalhes da consulta

Você pode analisar os detalhes da consulta no console do Amazon Redshift. Com um identificador de consulta, é possível visualizar os detalhes de uma consulta. Os detalhes podem incluir, por exemplo, o status de conclusão da consulta, duração, instrução SQL e se é uma consulta do usuário ou uma que foi reescrita pelo Amazon Redshift. A consulta do usuário é uma consulta que é enviada para o Amazon Redshift, seja de um cliente SQL ou gerada por uma ferramenta de business intelligence. O Amazon Redshift pode regravar a consulta para otimizá-la, e isso pode resultar em várias consultas regravadas. Embora o processo seja feito pelo Amazon Redshift, você vê as consultas reescritas na página de detalhes da consulta junto com a consulta do usuário.

Para visualizar uma consulta

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Queries and loads (Consultas e cargas) para exibir a lista de consultas de sua conta. Você pode precisar alterar as configurações nessa página para encontrar a sua consulta.
3. Escolha o identificador da Query (Consulta) na lista para exibir Query details (Detalhes da consulta).

   A página Query details (Detalhes da consulta) inclui as guias Query details (Detalhes da consulta) e Query plan (Plano de consulta) com métricas sobre a consulta.

   As métricas incluem detalhes sobre uma consulta, como hora de início, ID da consulta, status e duração. Outros detalhes incluem se uma consulta foi executada em um cluster principal ou em um cluster de escalabilidade de simultaneidade e se ela é uma consulta pai ou regravada.

## Analisar a execução da consulta

### Para analisar uma consulta

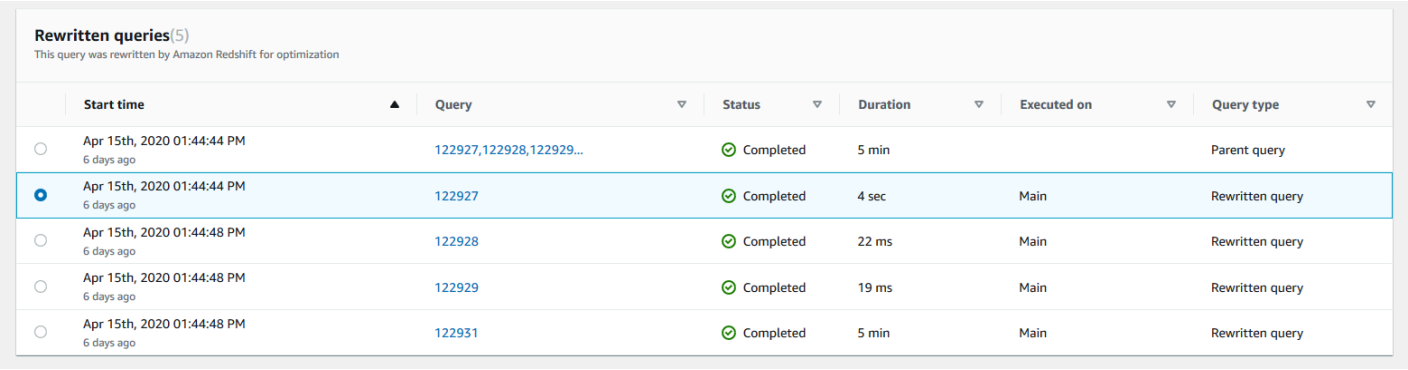
1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Queries and loads (Consultas e cargas) para exibir a lista de consultas de sua conta. Você pode precisar alterar as configurações nessa página para encontrar a sua consulta.
3. Escolha o identificador da Query (Consulta) na lista para exibir Query details (Detalhes da consulta).

   A página Query details (Detalhes da consulta) inclui as guias Query details (Detalhes da consulta) e Query plan (Plano de consulta) com métricas sobre a consulta.

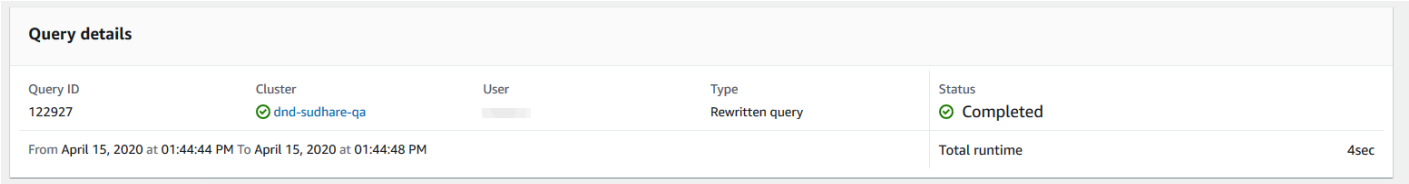
> **Note**
>
> Você também pode navegar para a página de Detalhes da consulta a partir de uma página de Detalhes do cluster no guia Histórico de consultas, ao fazer uma busca detalhada em uma consulta em um gráfico de Tempo de execução da consulta .

A página Detalhes da consulta contém as seguintes seções:

- Uma lista de Consultas regravadas, como mostrado no screenshot seguinte.



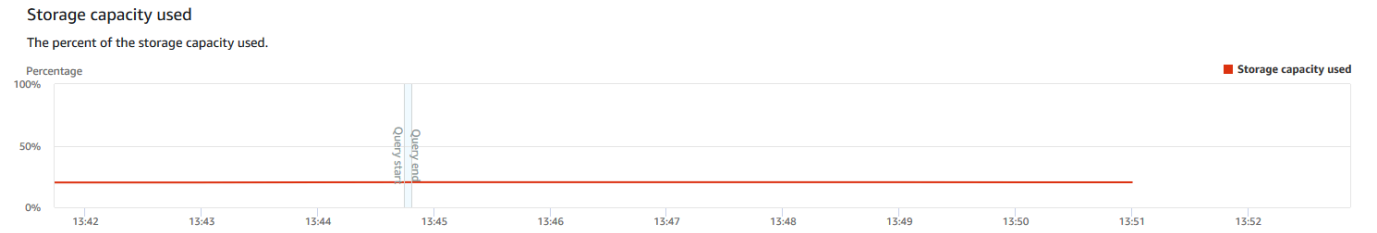

- Uma seção de Detalhes da consulta, como mostrado no screenshot a seguir.



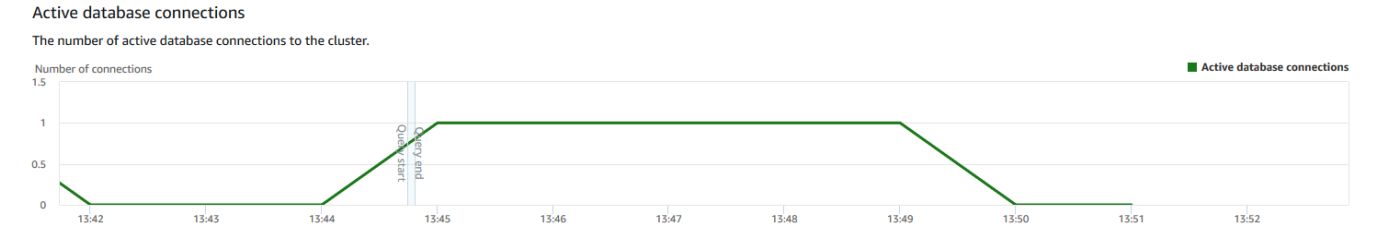

- Uma guia Detalhes da consulta que contém o SQL executado e Detalhes de execução sobre a execução.
- Uma guia Plano de consulta que contém as etapas do Plano de consulta e outras informações sobre ele. Esta tabela também contém gráficos sobre o cluster quando a consulta foi executada.
  - Status de integridade do cluster

  - Utilização da CPU

  - Capacidade de armazenamento utilizada




  - Conexões de banco de dados ativas



Visualizar a performance do cluster como consultas executadas

Para exibir a performance do cluster como consultas executadas

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Clusters e o nome do cluster na lista para abrir os respectivos detalhes. Os detalhes do cluster são exibidos, incluindo as guias Performance do cluster, Monitoramento de consultas, Banco de dados, Datashares, Programações, Manutenção e Propriedades.
3. Escolha a guia Query monitoring (Monitoramento de consultas) para mais detalhes.

   Para obter mais informações, consulte Visualizar dados do histórico de consultas.

## Visualizar métricas do cluster durante as operações de carga

Ao visualizar a performance do cluster durante operações de carga, é possível identificar consultas que estejam consumindo recursos e agir para atenuar o efeito. Você poderá encerrar uma carga se não quiser que ela seja executada até a conclusão.

> **Note**
>
> A capacidade de encerrar consultas e carregamentos no console do Amazon Redshift requer permissão específica. Se você quiser que os usuários tenham permissão para encerrar consultas e carregamentos, certifique-se de adicionar a ação `redshift:CancelQuerySession` à sua política do AWS Identity and Access Management (IAM). Este requisito se aplica se você selecionar a política gerenciada pela AWS somente leitura do Amazon Redshift ou criar uma política personalizada no IAM. Os usuários que têm a política de acesso total do Amazon Redshift já têm a permissão necessária para encerrar consultas e carregamentos. Para obter mais informações sobre ações em políticas do IAM para Amazon Redshift, consulte Gerenciamento de acesso aos recursos.

Para exibir a performance do cluster durante operações de carga

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

2. No menu de navegação, escolha Clusters e o nome do cluster na lista para abrir os respectivos detalhes. Os detalhes do cluster são exibidos, incluindo as guias Performance do cluster, Monitoramento de consultas, Banco de dados, Datashares, Programações, Manutenção e Propriedades.
3. Escolha a guia Query monitoring (Monitoramento de consultas) para mais detalhes.
4. Na seção Queries and loads (Consultas e cargas), escolha Loads (Cargas) para visualizar as operações de carga de um cluster. Se a carga estiver em execução, você poderá encerrá-la escolhendo Terminate query (Encerrar consulta).

## Analisar a performance do workload

É possível obter uma visualização detalhada da performance de seu workload observando o gráfico Detalhamento da execução do workload no console. Criamos o gráfico com os dados fornecidos pela métrica QueryRuntimeBreakdown. Com esse gráfico, você pode visualizar quanto tempo as consultas passam nos diversos estágios de processamento, como em espera e planejamento.

> **Note**
>
> O gráfico Detalhamento da execução do workload não é mostrado para clusters de nó único.

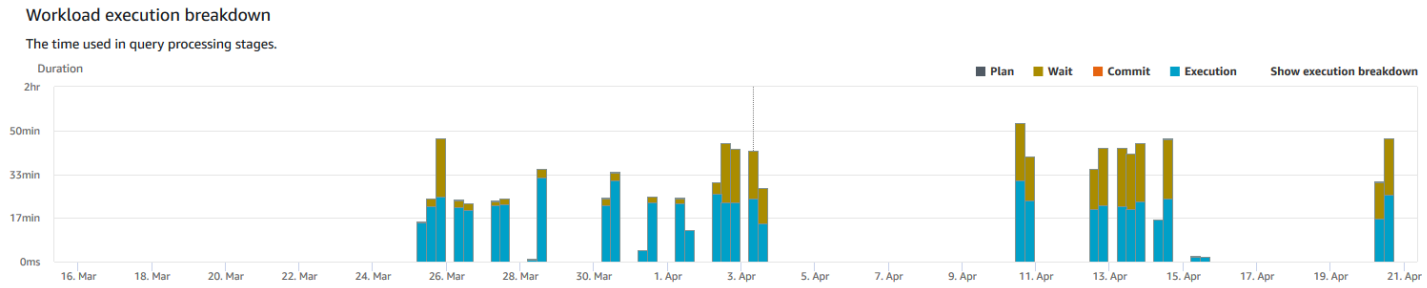
A lista de métricas a seguir descreve os diversos estágios de processamento:

- `QueryPlanning`: tempo gasto analisando e otimizando instruções SQL.
- `QueryWaiting`: tempo gasto em espera na fila de gerenciamento do workload (WLM).
- `QueryExecutingRead`: tempo gasto executando consultas de leitura.
- `QueryExecutingInsert`: tempo gasto executando consultas de inserção.
- `QueryExecutingDelete`: tempo gasto executando consultas de exclusão.
- `QueryExecutingUpdate`: tempo gasto executando consultas de atualização.
- `QueryExecutingCtas`: tempo gasto executando consultas CREATE TABLE AS.
- `QueryExecutingUnload`: tempo gasto executando consultas de descarregamento.
- `QueryExecutingCopy`: tempo gasto executando consultas de cópia.

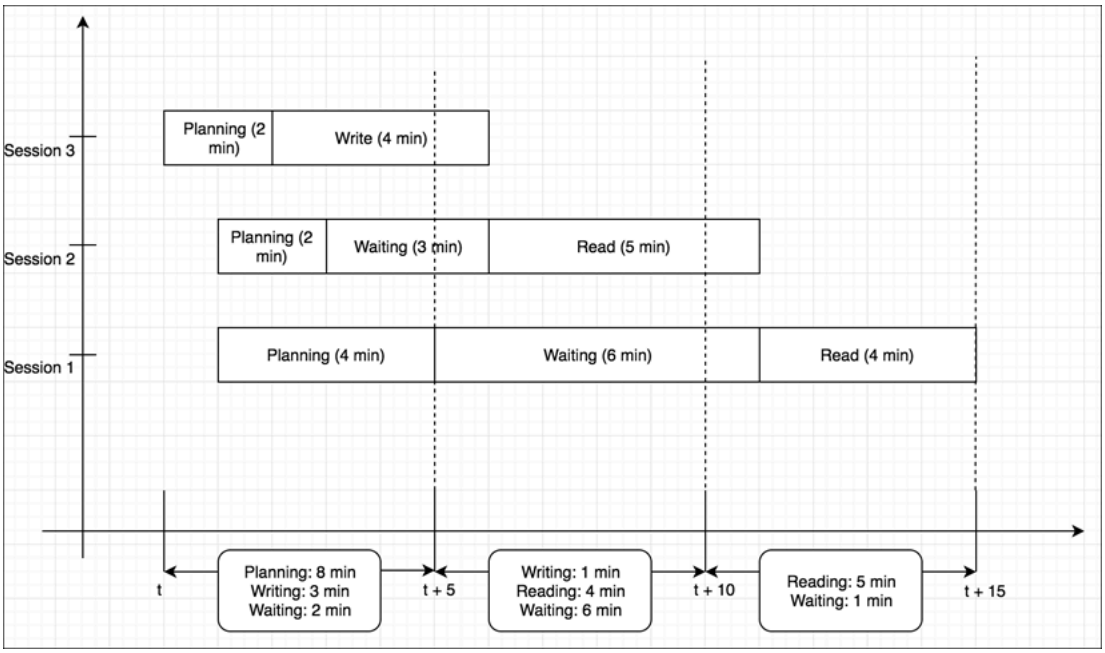
Por exemplo, o gráfico a seguir no console do Amazon Redshift mostra a quantidade de tempo que as consultas passaram nos estágios de plano, espera, leitura e gravação. Você pode combinar

as descobertas desse gráfico com outras métricas para obter análises adicionais. Em alguns casos, o gráfico pode mostrar que as consultas de curta duração (conforme medido pela métrica `QueryDuration`) estão passando muito tempo no estágio de espera. Nesses casos, você pode aumentar a taxa de simultaneidade do WLM para uma fila específica para aumentar a taxa de transferência.

Veja a seguir um exemplo do gráfico de detalhamento da execução do workload. No gráfico, o valor do eixo y é a duração média de cada estágio no tempo especificado mostrado como um gráfico de barras empilhadas.




O diagrama a seguir ilustra como o Amazon Redshift agrega o processamento de consultas para sessões simultâneas.




Para exibir o gráfico da análise do workload do cluster

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

2. No menu de navegação, escolha Clusters e o nome do cluster na lista para abrir os respectivos detalhes. Os detalhes do cluster são exibidos, incluindo as guias Performance do cluster, Monitoramento de consultas, Banco de dados, Datashares, Programações, Manutenção e Propriedades.
3. Escolha a guia Query monitoring (Monitoramento de consultas) para obter as métricas sobre suas consultas.
4. Na seção Monitoramento de consultas, escolha Performance do banco de dados e Métricas do cluster.

   As seguintes métricas são exibidas em gráfico para o período escolhido, como um gráfico de barras empilhadas.

   - Tempo de Plan (Planejamento)
   - Tempo de Wait (Espera)
   - Tempo deConfirmação
   - Tempo de Execução

## Gerenciar alarmes

Os alarmes criados por você no console do Amazon Redshift são alarmes do CloudWatch. Eles são úteis porque ajudam a tomar decisões proativas sobre o cluster ou instância com tecnologia sem servidor. Você pode definir um ou mais alarmes em qualquer uma das métricas listadas em Monitorar o Amazon Redshift usando métricas do CloudWatch. Por exemplo, definir um alarme para `CPUUtilization` alto em um nó de cluster ajudará a indicar quando o nó foi superutilizado. Um alarme para alto nível de `DataStorage` monitoraria o espaço de armazenamento que seu namespace com tecnologia sem servidor está usando para seus dados.

Em Ações, você pode modificar ou excluir alarmes. Você também pode criar um alerta de sinal ou folga para enviar um alerta do CloudWatch para o Slack ou o Amazon Chime especificando um URL do webhook do Slack ou do Amazon Chime.

Nesta seção, você pode descobrir como criar um alarme usando o console do Amazon Redshift. Você pode criar um alarme usando o console do CloudWatch ou qualquer outra maneira de trabalhar com métricas, como com o AWS CLI ou um AWS SDK.

Para criar um alarme do CloudWatch com o console do Amazon Redshift

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.

   Se você estiver usando o Amazon Redshift Serverless, escolha Go to Serverless (Acessar o Serverless) no canto superior direito do painel.
2. No menu de navegação, escolha Alarms (Alarmes) e Create alarm (Criar alarme).
3. Na página Criar alarme, insira as propriedades para criar um alarme do CloudWatch.
4. Selecione Criar alarme.

## Trabalhar com métricas de performance no console do CloudWatch

Ao trabalhar com métricas do Amazon Redshift no console do CloudWatch, tenha algumas coisas em mente:

- Os dados de performance de consulta e carga estão disponíveis apenas no console do Amazon Redshift.
- Algumas métricas no CloudWatch têm unidades diferentes daquelas usadas no console do Amazon Redshift. Por exemplo, `WriteThroughput` é exibido em GB/s (em comparação com Bytes/s no CloudWatch), que é uma unidade mais relevante para o espaço de armazenamento típico de um nó.

Ao trabalhar com métricas do Amazon Redshift no console do CloudWatch, ferramentas de linha de comando ou um SDK da Amazon, mantenha estes conceitos em mente:

1. Primeiro, você especifica a dimensão da métrica com a qual trabalhar. Uma dimensão é um par nome/valor, que ajuda a identificar com exclusividade uma métrica. As dimensões do Amazon Redshift são `ClusterIdentifier` e `NodeID`. No console do CloudWatch, as visualizações `Redshift Cluster` e `Redshift Node` são fornecidas para selecionar facilmente as dimensões específicas do cluster e do nó. Para obter mais informações sobre dimensões, consulte Dimensões no Guia do Desenvolvedor do CloudWatch.
2. Depois, você especifica o nome da métrica, como `ReadIOPS`.

A tabela a seguir resume os tipos de dimensões métricas do Amazon Redshift que estão disponíveis para você. Dependendo da métrica, os dados são disponibilizados em intervalos de 1 minuto ou de 5 minutos sem custo. Para obter mais informações, consulte Métricas do Amazon Redshift.

| Namespace do CloudWatch | Dimensão | Descrição |
|---|---|---|
| `AWS/Redshift` | `NodeID` | Filtra os dados solicitados que são específicos para os nós de um cluster. `NodeID` é "Leader", “Shared” ou “Compute-N”, sendo N 0, 1,... conforme o número de nós no cluster. “Shared” significa que o cluster tem apenas um nó, ou seja, o nó principal e o nó de computação são combinados. |
| | `ClusterIdentifier` | Filtra os dados solicitados que são específicos ao cluster. As métricas específicas a clusters incluem `HealthStatus` , `MaintenanceMode` e `DatabaseConnections` . De modo geral, métricas para esta dimensão (por exemplo, `ReadIOPS`) que também são métricas de nós representam um conjunto dos dados na métrica do nó. Atente-se ao interpretar essas métricas porque elas reúnem o comportamento de nós principais e de computação. |

Trabalhar com métricas de gateway e volume é semelhante a trabalhar com outras métricas de serviço. Muitas das tarefas comuns são descritas na documentação do CloudWatch, incluindo o seguinte:

- Visualizar métricas disponíveis
- Obter estatísticas de uma métrica
- Criar alarmes do CloudWatch

# Eventos do Amazon Redshift

Tópicos


- Visão geral dos eventos de cluster
- Trabalhar com o Amazon Simple Notification Service
- Assinar notificações de eventos de cluster do Amazon Redshift
- Visualizar eventos de cluster usando o console
- Visualizar eventos de cluster usando a AWS CLI e a API do Amazon Redshift
- Gerenciar notificações de eventos de cluster
- Notificações de eventos do Amazon Redshift
- Notificações de eventos do Amazon Redshift sem servidor com o Amazon EventBridge
- Notificações de evento da integração ETL zero com o Amazon EventBridge


## Visão geral dos eventos de cluster

O Amazon Redshift rastreia eventos de cluster e retém informações sobre eles por um período de várias semanas em sua conta da AWS. Para cada evento, o Amazon Redshift registra informações como a data em que o evento ocorreu, uma descrição, a fonte do evento (por exemplo, um cluster, um grupo de parâmetros ou um snapshot) e a ID da fonte.

O Amazon Redshift fornece notificação antecipadamente para alguns eventos. Esses eventos têm uma categoria de evento de `pending`. Por exemplo, enviamos uma notificação prévia se uma atualização de hardware for necessária para um dos nós no cluster. Você pode assinar eventos pendentes da mesma forma que outros eventos do Amazon Redshift. Para ter mais informações, consulte Assinar notificações de eventos de cluster do Amazon Redshift.

Você pode usar o Console de Gerenciamento do Amazon Redshift, a API do Amazon Redshift ou SDKs da AWS para obter informações sobre eventos. É possível obter uma lista de todos os eventos ou aplicar filtros, como a duração do evento ou a data de início e a data de término, a fim de obter informações sobre eventos para um período específico.

Você também pode obter eventos que foram gerados por um tipo específico de origem, tais como eventos de cluster ou eventos de parameter group. A coluna Fonte mostra o nome e o tipo de recurso que aciona uma determinada ação.

Você pode criar assinaturas de notificação de eventos do Amazon Redshift que especificam um conjunto de filtros de eventos. Quando ocorre um evento que corresponde aos critérios do filtro, o Amazon Redshift usa o Amazon Simple Notification Service para informar ativamente que o evento ocorreu.

Para ver uma lista de eventos do Amazon Redshift por tipo de fonte e categoria, consulte the section called “Categorias de eventos e mensagens de eventos do Amazon Redshift”

## Trabalhar com o Amazon Simple Notification Service

O Amazon Redshift usa o Amazon Simple Notification Service (Amazon SNS) para comunicar notificações de eventos do Amazon Redshift. Você habilita notificações criando uma assinatura de evento do Amazon Redshift. Na assinatura do Amazon Redshift, você especifica um conjunto de filtros para eventos do Amazon Redshift e um tópico Amazon SNS. Sempre que um evento que corresponda aos critérios do filtro ocorre, o Amazon Redshift publica uma mensagem de notificação para o tópico do Amazon SNS. Em seguida, o Amazon SNS transmite a mensagem para qualquer consumidor do Amazon SNS que tenha uma assinatura do Amazon SNS para o tópico. As mensagens enviadas aos consumidores do Amazon SNS podem estar em qualquer formato compatível com o Amazon SNS para uma região da AWS, como um e-mail, uma mensagem de texto ou uma chamada para um endpoint HTTP. Por exemplo, todas as regiões são compatíveis com notificações por e-mail, mas as notificações por SMS só podem ser criadas na região Leste dos EUA (Norte da Virgínia).

> **Note**
>
> Atualmente, você só pode criar uma assinatura de evento para um tópico padrão do Amazon SNS (não para um tópico FIFO do Amazon SNS). Para obter mais informações, consulte Fontes de eventos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

Ao criar uma assinatura de notificação de evento, você especifica um ou mais filtros de evento. O Amazon Redshift envia notificações através da assinatura sempre que um evento que corresponda a todos os critérios do filtro ocorrer. Os critérios de filtro incluem tipo de origem (tal como cluster ou snapshot), ID de origem (tal como o nome de um cluster ou snapshot), categoria do evento (tal como monitoramento ou segurança) e os problemas de segurança do evento (tal como INFO ou ERRO).

Você pode facilmente desativar as notificações sem excluir uma assinatura ao configurar o botão de opção Habilitado como No no AWS Management Console ou ao configurar o parâmetro `Enabled` como `false` usando a CLI ou API do Amazon Redshift.

O faturamento da notificação de eventos do Amazon Redshift é feito por meio do Amazon Simple Notification Service (Amazon SNS). As taxas do Amazon SNS se aplicam quando você usa as notificações de eventos. Para obter mais informações sobre o faturamento do Amazon SNS, consulte Preço do Amazon Simple Notification Service.

Você também pode visualizar eventos do Amazon Redshift que ocorreram usando o console de gerenciamento. Para ter mais informações, consulte Eventos do Amazon Redshift.

## Assinar notificações de eventos de cluster do Amazon Redshift

Você pode criar uma assinatura de notificação de evento do Amazon Redshift para ser notificado quando um evento ocorrer para um determinado cluster, snapshot, grupo de segurança ou grupo de parâmetros. A maneira mais simples de criar uma assinatura é com o console do Amazon SNS. Para obter informações sobre como criar um tópico do Amazon SNS e se inscrever nele, consulte Conceitos básicos do Amazon SNS.

Você pode criar uma assinatura de notificação de evento do Amazon Redshift para ser notificado quando um evento ocorrer para um determinado cluster, snapshot, grupo de segurança ou grupo de parâmetros. A forma mais fácil de criar uma assinatura é com o AWS Management Console. Se você preferir criar assinaturas de notificações de eventos usando a CLI ou API, é necessário criar um tópico do Amazon Simple Notification Service e fazer a assinatura desse tópico com o console do Amazon SNS ou a API do Amazon SNS. Você também precisará reter o nome de recurso da Amazon (ARN) do tópico, pois ele é usado ao enviar comandos da CLI ou ações da API. Para obter informações sobre como criar um tópico do Amazon SNS e se inscrever nele, consulte Conceitos básicos do Amazon SNS.

Uma assinatura de evento do Amazon Redshift pode especificar estes critérios de evento:

- O tipo de origem, os valores são cluster, snapshot, parameter-groups e security-groups.
- ID de origem de um recurso, tal como `my-cluster-1` ou `my-snapshot-20130823`. O ID deve ser para um recurso na mesma região da AWS da assinatura do evento.
- Categoria de evento: os valores são configuração, gerenciamento, monitoramento, segurança e pendente.
- Problemas de segurança do evento, os valores são INFO ou ERRO.

Os critérios de evento podem ser especificados de forma independente, mas você deve especificar um tipo de origem antes de poder especificar IDs de origem no console. Por exemplo, você pode especificar uma categoria de evento sem ter que especificar um tipo de origem, ID de origem ou problemas de segurança. Embora você possa especificar IDs de origem para recursos que não são do tipo especificado no tipo de origem, nenhuma notificação será enviada para eventos desses recursos. Por exemplo, se você especificar um tipo de origem de cluster e o ID de um security group, nenhum dos eventos levantados por aquele security group corresponderia ao critério de filtro para tipo de origem, portanto nenhuma notificação seria enviada para tais eventos.

O Amazon Redshift envia uma notificação para qualquer evento que corresponda a todos os critérios especificados em uma assinatura. Alguns exemplos de conjuntos de eventos retornados:

- A assinatura especifica um tipo de origem de cluster, um ID de origem de my-cluster-1, uma categoria de monitoramento e um problema de segurança de ERRO. A assinatura enviará notificações somente para eventos de monitoramento com um problema de segurança ERRO do my-cluster-1.
- A assinatura especifica um tipo de origem de cluster, uma categoria de configuração e um problema de segurança de INFO. A assinatura enviará notificações para eventos de configuração com gravidade INFO de qualquer cluster do Amazon Redshift na conta da AWS.
- A assinatura especifica uma categoria de configuração e um problema de segurança de INFO. A assinatura enviará notificações para eventos de configuração com gravidade INFO de qualquer recurso do Amazon Redshift na conta da AWS.
- A assinatura especifica um problema de segurança de ERRO. A assinatura enviará notificações para todos os eventos com gravidade ERROR de qualquer recurso do Amazon Redshift na conta da AWS.

Se você excluir ou renomear um objeto cujo o nome é mencionado como um ID de origem em uma assinatura existente, a assinatura permanecerá ativa, mas não terá eventos para enviar a partir desse objeto. Se você mais tarde criar um novo objeto com o mesmo nome mencionado no ID de origem da assinatura, a assinatura começará a enviar notificações para eventos a partir do novo objeto.

O Amazon Redshift publica notificações de eventos para um tópico do Amazon SNS, que é identificado por seu nome do recurso da Amazon (ARN). Ao criar uma assinatura de evento usando o console do Amazon Redshift, você pode especificar um tópico existente do Amazon SNS ou solicitar que o console crie o tópico ao criar a assinatura. Todas as notificações de eventos do Amazon Redshift enviadas para o tópico do Amazon SNS são, por sua vez, transmitidas para todos

os consumidores do Amazon SNS que estão inscritos nesse tópico. Use o console do Amazon SNS para fazer alterações no tópico do Amazon SNS, como adicionar ou remover assinaturas do consumidor para o tópico. Para obter mais informações sobre como criar e assinar tópicos do Amazon SNS, acesse Conceitos básicos do Amazon Simple Notification Service.

A seção a seguir lista todas as categorias e eventos sobre os quais você pode ser receber notificações. Ele também fornece informações sobre como assinar e trabalhar com assinaturas de eventos do Amazon Redshift.

## Visualizar eventos de cluster usando o console

Para visualizar eventos

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Events (Eventos).

## Visualizar eventos de cluster usando a AWS CLI e a API do Amazon Redshift

É possível usar as seguintes operações da CLI do Amazon Redshift para visualizar eventos.

- describe-events

O Amazon Redshift fornece a API a seguir para visualização de eventos.

- DescribeEvents

## Gerenciar notificações de eventos de cluster

Você pode criar uma assinatura de notificação de evento do Amazon Simple Notification Service (Amazon SNS) para enviar notificações quando um evento ocorre para um determinado cluster, snapshot, grupo de segurança ou grupo de parâmetros do Amazon Redshift. Essas notificações são enviadas para um tópico SNS que, por sua vez, transmite as mensagens para todos os consumidores do SNS inscritos no tópico. As mensagens SNS para os consumidores podem ser em qualquer formulário de notificação aceito pelo Amazon SNS para uma região da AWS, como

um e-mail, uma mensagem de texto ou uma chamada para um endpoint HTTP. Por exemplo, todas as regiões oferecem suporte a notificações por e-mail, mas as notificações por SMS só podem ser criadas na região Leste dos EUA (Norte da Virgínia). Para ter mais informações, consulte Notificações de eventos do Amazon Redshift.

# Gerenciar notificações de eventos de cluster usando o console do Amazon Redshift

## Criação de uma assinatura de notificação de evento

Para criar uma assinatura de evento

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Events (Eventos).
3. Selecione a guia Event subscription (Assinatura de evento) e Create event subscriptions (Criar assinaturas de eventos).
4. Insira as propriedades de sua assinatura de evento, como nome, tipo de origem, categoria e gravidade. Também é possível habilitar os tópicos do Amazon SNS para ser notificado sobre eventos.
5. Escolha Create event subscriptions (Criar assinaturas de eventos) para criar sua assinatura.

# Gerenciar notificações de eventos de cluster usando a AWS CLI e a API do Amazon Redshift

É possível usar as operações da CLI do Amazon Redshift a seguir para gerenciar notificações de eventos de cluster.

- create-event-subscription
- delete-event-subscription
- describe-event-categories
- describe-event-subscriptions
- describe-events
- modify-event-subscription

Você pode usar as ações da API do Amazon Redshift a seguir para gerenciar notificações de eventos.

- CreateEventSubscription
- DeleteEventSubscription
- DescribeEventCategories
- DescribeEventSubscriptions
- DescribeEvents
- ModifyEventSubscription

Para obter mais informações sobre notificações de eventos do Amazon Redshift, consulte Notificações de eventos do Amazon Redshift.

# Notificações de eventos do Amazon Redshift

## Categorias de eventos e mensagens de eventos do Amazon Redshift

Esta seção mostra os IDs de eventos e categorias para cada tipo de fonte do Amazon Redshift.

A tabela a seguir mostra a categoria de evento e uma lista de eventos quando um cluster é o tipo de origem.

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Configuração | REDSHIFT-EVENT-1000 | INFO | O parameter group [nome do parameter group] foi atualizado às [hora]. Se você alterou apenas os parâmetros dinâmicos, os clusters associados estão sendo modificados agora. Se você alterou os parâmetros estáticos, todas as atualizações, incluindo parâmetros dinâmicos, serão aplicadas quando você reinicializar os clusters associados. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Configuração | REDSHIFT-EVENT-1001 | INFO | Seu cluster do Amazon Redshift [nome do cluster] foi modificado para usar o grupo de parâmetros [nome do grupo de parâmetros] às [hora]. |
| Configuração | REDSHIFT-EVENT-1500 | ERRO | O Amazon VPC [nome da VPC] não existe. Suas alterações de configuração para o cluster [nome do cluster] não foram aplicadas . Visite o AWS Management Console para corrigir o problema. |
| Configuração | REDSHIFT-EVENT-1501 | ERRO | As sub-redes do cliente [nome da sub-rede] que você especificou para Amazon VPC [nome da VPC] não existem ou são inválidas . Suas alterações de configuração para o cluster [nome do cluster] não foram aplicadas . Visite o AWS Management Console para corrigir o problema. |
| Configuração | REDSHIFT-EVENT-1502 | ERRO | As sub-redes no grupo de sub-redes do cluster [nome do grupo de sub-redes] não possuem endereços IP disponíveis. O cluster [nome do cluster] não pôde ser criado. |
| Configuração | REDSHIFT-EVENT-1503 | ERRO | O Amazon VPC [nome da VPC] não tem gateway da Internet anexado a ele. Suas alterações de configuração para o cluster [nome do cluster] não foram aplicadas. Visite o AWS Management Console para corrigir o problema. |
| Configuração | REDSHIFT-EVENT-1504 | ERRO | O HSM para o cluster [nome do cluster] está inacessível. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Configuração | REDSHIFT-EVENT-1505 | ERRO | O HSM para o cluster [nome do cluster] não pode ser registrado. Tente uma configuração diferente. |
| Configuração | REDSHIFT-EVENT-1506 | ERRO | O Amazon Redshift excedeu o limite de interface de rede elástica da sua conta. Exclua até [número máximo de interfaces de rede elásticas] interfaces de rede elástica ou solicite um aumento de limite do número de interfaces de rede por região da AWS com EC2. |
| Configuração | REDSHIFT-EVENT-1509 | ERRO | O cluster [nome do cluster] do Amazon Redshift não pode ser criado porque o limite de endpoint da VPC da sua conta foi atingido. Exclua endpoints da VPC não utilizados ou solicite um aumento no limite de endpoints da VPC.<br><br>Para obter mais informações, consulte Endpoints da VPC no Manual do usuário do Amazon VPC. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Configuração | REDSHIFT-EVENT-1510 | ERRO | Detectamos que a tentativa de carregar exemplos de dados em seu cluster [nome do cluster] do Amazon Redshift não foi bem-sucedida. Para carregar exemplos de dados, primeiro configure a VPC para ter acesso aos buckets do Amazon S3 e, em seguida, crie um novo cluster e carregue os exemplos de dados.<br><br>Para obter mais informações, consulte "Habilitar o roteamento aprimorado de VPC" no Guia de gerenciamento de clusters do Amazon Redshift. |
| Configuração | REDSHIFT-EVENT-1511 | ERRO | Não é possível criar o cluster do Amazon Redshift [nome do cluster] porque você excedeu o limite de endereços IP elásticos da sua conta. Exclua os endereços IP elásticos não utilizados ou solicite um aumento de limite do Amazon EC2. |
| Gerenciamento | REDSHIFT-EVENT-2000 | INFO | Seu cluster do Amazon Redshift: [nome do cluster] foi criado e está pronto para uso. |
| Gerenciamento | REDSHIFT-EVENT-2001 | INFO | Seu cluster Amazon Redshift [nome do cluster] foi excluído às [hora]. Um snapshot final [foi/não foi] salvo. |
| Gerenciamento | REDSHIFT-EVENT-2002 | INFO | Grupos de segurança da VPC do cluster [nome do cluster] atualizados em [horário em UTC]. |
| Gerenciamento | REDSHIFT-EVENT-2003 | INFO | A manutenção iniciou no cluster [nome do cluster] às [hora em UTC]. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Gerenciamento | REDSHIFT-EVENT-2004 | INFO | A manutenção do cluster [nome do cluster] foi concluída às [hora em UTC]. |
| Gerenciamento | REDSHIFT-EVENT-2006 | INFO | O redimensionamento do cluster [nome do cluster] iniciou às [hora em UTC]. O cluster está no modo somente leitura. |
| Gerenciamento | REDSHIFT-EVENT-2007 | INFO | Uma solicitação de redimensionamento para o cluster [nome do cluster] foi confirmada. |
| Gerenciamento | REDSHIFT-EVENT-2008 | INFO | Sua operação de restauração para criar um novo snapshot [nome do snapshot] do cluster do Amazon Redshift [nome do cluster] foi iniciada às [hora]. Para monitorar o progresso de restauração, acesse o AWS Management Console. |
| Gerenciamento | REDSHIFT-EVENT-2013 | INFO | Seu cluster Amazon Redshift [nome do cluster] foi renomeado às [hora]. |
| Gerenciamento | REDSHIFT-EVENT-2014 | INFO | Uma solicitação de restauração de tabela para o cluster do Amazon Redshift [nome do cluster] foi recebida. |
| Gerenciamento | REDSHIFT-EVENT-2015 | INFO | A restauração da tabela foi cancelada para o cluster do Amazon Redshift [nome do cluster] às [hora]. |
| Gerenciamento | REDSHIFT-EVENT-2016 | INFO | A substituição de seu cluster do Amazon Redshift [nome do cluster] foi iniciada às [hora]. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Gerenciamento | REDSHIFT-EVENT-2017 | INFO | A manutenção iniciada pelo cliente começou em seu cluster [nome do cluster] do Amazon Redshift às [horário]. O cluster pode não estar disponível durante a manutenção. |
| Gerenciamento | REDSHIFT-EVENT-2018 | INFO | A manutenção iniciada pelo cliente foi concluída em seu cluster [nome do cluster] do Amazon Redshift às [horário]. |
| Gerenciamento | REDSHIFT-EVENT-2019 | ERRO | A manutenção iniciada pelo cliente falhou em seu cluster [nome do cluster] do Amazon Redshift às [horário]. Retornar o cluster de volta ao estado original. |
| Gerenciamento | REDSHIFT-EVENT-2020 | INFO | A trilha do seu cluster [cluster name] do Amazon Redshift foi modificada de [de trilha] para [para trilha]. |
| Gerenciamento | REDSHIFT-EVENT-2021 | ERRO | A [operação] do cluster do Amazon Redshift [nome do cluster] não obteve êxito ao adquirir capacidade do nosso grupo de capacidade. Estamos trabalhando para adquirir capacidade mas, por ora, cancelamos sua solicitação. Exclua este cluster e tente novamente mais tarde. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Gerenciamento | REDSHIFT-EVENT-2022 | ERRO | A [operação] do cluster do Amazon Redshift [nome do cluster] não obteve êxito ao adquirir capacidade do nosso grupo de capacidade. Estamos trabalhando para adquirir capacidade mas, por ora, cancelamos sua solicitação. A capacidade está disponível em [zonas de disponibilidade alternativas]. Exclua esse cluster e tente novamente em uma zona de disponibilidade alternativa. |
| Gerenciamento | REDSHIFT-EVENT-2023 | ERRO | Detectamos uma falha de hardware no cluster do Amazon Redshift de nó único [nome do cluster], que pode ter resultado em consultas com falha ou disponibilidade intermitente do cluster. A substituição do cluster não foi bem-sucedida durante a aquisição de capacidade do nosso grupo de capacidade. Você precisará restaurar um novo cluster de um snapshot. Exclua este cluster, selecione o último snapshot disponível e restaure um novo cluster desse snapshot. Isso irá provisioná-lo automaticamente em um hardware íntegro. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Gerenciamento | REDSHIFT-EVENT-2024 | ERRO | Detectamos uma falha de hardware no cluster do Amazon Redshift de nó único [nome do cluster], que pode ter resultado em consultas com falha ou disponibilidade intermitente do cluster. A substituição do cluster não foi bem-sucedida durante a aquisição de capacidade do nosso grupo de capacidade. A capacidad e está disponível na zona de disponibilidade: [zonas de disponibilidade alternativas]. Exclua este cluster, selecione o último snapshot disponível e restaure um novo cluster desse snapshot. Isso irá provisioná-lo automatic amente em um hardware íntegro. |
| Gerenciamento | REDSHIFT-EVENT-3011 | INFO | Redimensionamento elástico para o cluster do Amazon Redshift “[nome do cluster]” começou às [hora]. Manteremos as conexões do banco de dados durante o redimensi onamento. Algumas consultas e conexões podem ser encerradas ou expiradas durante essa operação. |
| Gerenciamento | REDSHIFT-EVENT-3012 | INFO | Recebemos uma solicitação de redimensi onamento elástico para o cluster "[nome do cluster]" iniciado à(s) [hora]. Fornecere mos uma notificação de evento quando o redimensionamento começar. |
| Pendente | REDSHIFT-EVENT-2025 | INFO | Seu banco de dados para cluster <nome do cluster> será atualizado entre <hora inicial> e <hora final>. Seu cluster não estará acessível. Planeje adequadamente. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Pendente | REDSHIFT-EVENT-2026 | INFO | Seu cluster <nome do cluster> será atualizado entre <hora inicial> e <hora final>. Seu cluster não estará acessível. Planeje adequadam ente. |
| Monitoram ento | REDSHIFT-EVENT-2050 | INFO | Um problema de hardware for detectado no cluster [nome do cluster] do Amazon Redshift. Uma solicitação de substituição foi iniciada às [hora]. |
| Monitoram ento | REDSHIFT-EVENT-3000 | INFO | Seu cluster do Amazon Redshift [nome do cluster] foi reiniciado às [hora]. |
| Monitoram ento | REDSHIFT-EVENT-3001 | INFO | Um nó em seu cluster do Amazon Redshift: [nome do cluster] foi substituído automatic amente às [hora] e seu cluster está operando normalmente. |
| Monitoram ento | REDSHIFT-EVENT-3002 | INFO | O redimensionamento de seu cluster do Amazon Redshift [nome do cluster] está completo e seu cluster está disponível para leituras e gravações. O redimensionamento foi iniciado às [hora] e levou [horas] para ser concluído. |
| Monitoram ento | REDSHIFT-EVENT-3003 | INFO | O cluster do Amazon Redshift [nome do cluster] foi criado com êxito a partir do snapshot [nome do instantâneo] e está disponível para uso. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Monitoramento | REDSHIFT-EVENT-3007 | INFO | Seu snapshot do Amazon Redshift [nome do snapshot] foi copiado com sucesso de [região de origem da AWS] para [região de destino da AWS] às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3008 | INFO | A restauração da tabela foi iniciada para o cluster do Amazon Redshift [nome do cluster] às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3009 | INFO | A restauração da tabela foi concluída com êxito para o cluster do Amazon Redshift [nome do cluster] às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3010 | ERRO | A restauração da tabela falhou para o cluster do Amazon Redshift [nome do cluster] às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3013 | ERRO | A operação de redimensionamento elástico solicitada para o cluster do Amazon Redshift [nome do cluster] falhou às [hora] devido a [razão]. |
| Monitoramento | REDSHIFT-EVENT-3014 | INFO | O Amazon Redshift reiniciou o cluster [nome do cluster] às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3500 | ERRO | O redimensionamento do seu cluster do Amazon Redshift [nome do cluster] falhou. Uma nova tentativa de redimensionamento será realizada automaticamente em alguns minutos. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Monitoramento | REDSHIFT-EVENT-3501 | ERRO | Sua operação de restauração para criar o cluster do Amazon Redshift [nome do cluster] a partir do snapshot [nome do snapshot] falhou às [hora]. Tente sua operação novamente. |
| Monitoramento | REDSHIFT-EVENT-3504 | ERRO | O bucket do Amazon S3 [nome do bucket] não é válido para registro de cluster [nome do cluster]. |
| Monitoramento | REDSHIFT-EVENT-3505 | ERRO | O bucket do Amazon S3 [nome do bucket] não tem as políticas de IAM corretas para o cluster [nome do cluster]. |
| Monitoramento | REDSHIFT-EVENT-3506 | ERRO | O bucket do Amazon S3 [nome do bucket] não existe. O registro não pode continuar para o cluster [nome do cluster]. |
| Monitoramento | REDSHIFT-EVENT-3507 | ERRO | O cluster Amazon Redshift [nome do cluster] não pode ser criado usando EIP [endereço IP]. Este EIP já está em uso. |
| Monitoramento | REDSHIFT-EVENT-3508 | ERRO | O cluster Amazon Redshift [nome do cluster] não pode ser criado usando EIP [endereço IP]. O EIP não pode ser encontrado. |
| Monitoramento | REDSHIFT-EVENT-3509 | ERRO | A cópia de snapshots entre regiões não está habilitada para o cluster [nome do cluster]. |
| Monitoramento | REDSHIFT-EVENT-3510 | ERRO | A restauração da tabela falhou ao iniciar para o cluster do Amazon Redshift [nome do cluster] às [hora]. Razão: [razão]. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Monitoramento | REDSHIFT-EVENT-3511 | ERRO | A restauração da tabela falhou para o cluster do Amazon Redshift [nome do cluster] às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3512 | ERRO | O cluster do Amazon Redshift [nome do cluster] falhou devido a um problema de hardware. O cluster está sendo automaticamente restaurado a partir do último snapshot [nome do snapshot] criado às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3513 | ERRO | O cluster do Amazon Redshift [nome do cluster] falhou devido a um problema de hardware. O cluster está sendo automaticamente restaurado a partir do último snapshot [nome do snapshot] criado às [hora]. Todas as alterações no banco de dados realizadas após esta hora precisam ser reenviadas. |
| Monitoramento | REDSHIFT-EVENT-3514 | ERRO | O cluster do Amazon Redshift [nome do cluster] falhou devido a um problema de hardware. O cluster está sendo colocado no status de falha de hardware. Exclua o cluster e restaure a partir do último snapshot [nome do snapshot] criado às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3515 | ERRO | O cluster do Amazon Redshift [nome do cluster] falhou devido a um problema de hardware. O cluster está sendo colocado no status de falha de hardware. Exclua o cluster e restaure a partir do último snapshot [nome do snapshot] criado às [hora]. Todas as alterações no banco de dados realizadas após esta hora precisam ser reenviadas. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Monitoramento | REDSHIFT-EVENT-3516 | ERRO | O cluster do Amazon Redshift [nome do cluster] falhou devido a um problema de hardware e não há backups para o cluster. O cluster está sendo colocado no status de falha de hardware e pode ser excluído. |
| Monitoramento | REDSHIFT-EVENT-3519 | INFO | O cluster [nome do cluster] começou a reinicialização às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3520 | INFO | O cluster [nome do cluster] concluiu a reinicialização às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3521 | INFO | Detectamos um problema de conectividade no cluster “[nome do cluster]”. Uma verificação de diagnóstico automatizada foi iniciada às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3522 | INFO | A ação de recuperação no cluster “[nome de cluster]” falhou às [hora]. A equipe do Amazon Redshift está trabalhando em uma solução. |
| Monitoramento | REDSHIFT-EVENT-3533 | ERRO | O redimensionamento de cluster em '[nome do cluster]' foi cancelado às [hora]. A operação foi cancelada porque [motivo]. [ação necessária]. |
| Monitoramento | REDSHIFT-EVENT-3534 | INFO | O redimensionamento elástico para o cluster do Amazon Redshift “[nome do cluster]” concluído às [hora]. O cluster está agora disponível para operações de leitura e gravação enquanto transferimos dados. Algumas consultas podem levar mais tempo para finalização até que a transferência de dados seja concluída. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Monitoramento | REDSHIFT-EVENT-3537 | INFO | A transferência de dados do cluster “[nome do cluster]” concluída às [hora em UTC]. |
| Monitoramento | REDSHIFT-EVENT-3600 | INFO | A operação de redimensionamento solicitada para o cluster do Amazon Redshift '[nome do cluster]' foi cancelada no passado. A reversão foi concluída às [hora]. |
| Pendente | REDSHIFT-EVENT-3601 | INFO | Um nó em seu cluster <nome do cluster> será substituído entre <hora inicial> e <hora final>. Não é possível adiar essa manutenção. Planeje adequadamente. |
| Pendente | REDSHIFT-EVENT-3602 | INFO | Um nó em seu cluster <nome do cluster> está agendado para ser substituído entre <hora inicial> e <hora final>. Seu cluster não estará acessível. Planeje adequadamente. |
| Gerenciamento | REDSHIFT-EVENT-3603 | INFO | Falha na operação de restauração para criação de um cluster [nome do cluster] do snapshot [nome do snapshot] devido a um erro interno. O cluster está sendo colocado no status de restauração incompatível e pode ser excluído. Tente restaurar o snapshot em um cluster com uma configuração diferente. |
| Gerenciamento | REDSHIFT-EVENT-3614 | INFO | A ação agendada [nome da ação agendada] foi criada às [hora em UTC]. A primeira chamada está agendada para as [hora em UTC]. |
| Gerenciamento | REDSHIFT-EVENT-3615 | INFO | A ação agendada [nome da ação agendada] foi agendada para as [hora em UTC]. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Monitoramento | REDSHIFT-EVENT-3616 | INFO | A ação agendada [nome da ação agendada] às [hora em UTC] foi encerrada com o status 'SUCCEEDED'. |
| Monitoramento | REDSHIFT-EVENT-3617 | ERRO | A ação agendada [nome da ação agendada] não ocorreu às [hora em UTC] devido ao atraso. |
| Monitoramento | REDSHIFT-EVENT-3618 | INFO | A operação de pausa do cluster do [nome do cluster] começou às [hora em UTC]. Pausa iniciada |
| Monitoramento | REDSHIFT-EVENT-3619 | INFO | O cluster do Amazon Redshift [nome do cluster] foi pausado com êxito às [hora UTC]. |
| Gerenciamento | REDSHIFT-EVENT-3626 | INFO | A ação agendada [nome da ação agendada] foi modificada às [hora em UTC]. A primeira chamada está agendada para as [hora em UTC]. |
| Gerenciamento | REDSHIFT-EVENT-3627 | INFO | A ação agendada [nome da ação agendada] foi excluída às [hora em UTC]. |
| Monitoramento | REDSHIFT-EVENT-3628 | ERRO | A ação agendada [nome da ação agendada] às [hora em UTC] foi encerrada com o status 'FAILED'. |
| Gerenciamento | REDSHIFT-EVENT-3629 | INFO | O Amazon Redshift [nome do cluster] recebeu sua solicitação de realocação. Quando a realocação da zona de disponibilidade é concluída, o Amazon Redshift envia uma notificação de evento. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Gerenciamento | REDSHIFT-EVENT-3630 | INFO | O cluster [nome do cluster] do Amazon Redshift foi realocado com êxito de [zona de disponibilidade] para [zona de disponibilidade]. Você pode usar o cluster agora. |
| Gerenciamento | REDSHIFT-EVENT-3631 | INFO | O Amazon Redshift realocou com sucesso seu cluster [nome do cluster] do Amazon Redshift de [zona de disponibilidade] para [zona de disponibilidade] para recuperação. |
| Gerenciamento | REDSHIFT-EVENT-3632 | INFO | O Amazon Redshift desativou temporariamente a realocação de cluster para seu cluster [nome do cluster] do Amazon Redshift devido a alterações de configuração. Tente realocar o cluster novamente mais tarde. |
| Monitoramento | REDSHIFT-EVENT-3658 | ERRO | Não foi possível migrar EC2-Classic para EC2-VPC no cluster do Redshift [id do cluster]. |
| Monitoramento | REDSHIFT-EVENT-3659 | INFO | A migração EC2-Classic para EC2-VPC no cluster do Redshift [id do cluster] foi concluída. |
| Monitoramento | REDSHIFT-EVENT-3660 | INFO | O cluster está sendo colocado no status de falha de hardware. Exclua o cluster EC2-Classic e restaure para um cluster EC2-VPC a partir do último snapshot [nome do snapshot] criado às [hora em UTC]. |
| Gerenciamento | REDSHIFT-EVENT-3666 | INFO | O cluster multi-AZ [nome do cluster] do Amazon Redshift detectou uma falha às [hora em UTC] e acionou uma recuperação automática. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Gerenciamento | REDSHIFT-EVENT-3667 | INFO | O cluster multi-AZ [nome do cluster] do Amazon Redshift foi recuperado com sucesso às [hora em UTC] e está disponível para uso na [primeira zona de disponibilidade]. A computação secundária em outra AZ estará disponível em breve. |
| Monitoramento | REDSHIFT-EVENT-3668 | ERRO | A recuperação do cluster multi-AZ [nome do cluster] do Amazon Redshift apresentou falha às [hora em UTC]. |
| Gerenciamento | REDSHIFT-EVENT-3669 | INFO | O cluster multi-AZ [nome do cluster] do Amazon Redshift foi recuperado com sucesso às [hora em UTC] e está disponível para uso com recursos computacionais da [primeira zona de disponibilidade] e da [segunda zona de disponibilidade]. |
| Gerenciamento | REDSHIFT-EVENT-3670 | INFO | A manutenção do cluster [nome do cluster] do Amazon Redshift foi concluída às [hora em UTC] e está disponível para uso com recursos computacionais na [primeira zona de disponibilidade]. A computação secundária em outra AZ estará disponível em breve. |
| Gerenciamento | REDSHIFT-EVENT-3671 | INFO | O redimensionamento do cluster [nome do cluster] do Amazon Redshift foi concluído às [hora em UTC] e está disponível para uso na [primeira zona de disponibilidade]. A computação secundária em outra AZ estará disponível em breve. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Gerenciamento | REDSHIFT-EVENT-3672 | INFO | O cluster multi-AZ do Amazon Redshift [nome do cluster] detectou uma falha na [segunda zona de disponibilidade] às [hora em UTC] e acionou uma recuperação automática. |
| Gerenciamento | REDSHIFT-EVENT-3673 | INFO | A operação de habilitação de multi-AZ para o cluster [nome do cluster] do Amazon Redshift foi iniciada às [hora em UTC]. |
| Gerenciamento | REDSHIFT-EVENT-3674 | INFO | A operação de habilitação de multi-AZ para o cluster [nome do cluster] do Amazon Redshift foi concluída com êxito às [hora em UTC]. |
| Monitoramento | REDSHIFT-EVENT-3675 | ERRO | A operação de habilitação de multi-AZ para o cluster [nome do cluster] do Amazon Redshift apresentou falha às [hora em UTC]. |
| Gerenciamento | REDSHIFT-EVENT-3676 | INFO | A operação de desabilitação de multi-AZ para o cluster multi-AZ [nome do cluster] do Amazon Redshift foi iniciada às [hora em UTC]. |
| Gerenciamento | REDSHIFT-EVENT-3677 | INFO | A operação de desabilitação de multi-AZ para o cluster [nome do cluster] do Amazon Redshift foi concluída com êxito às [hora em UTC]. |
| Monitoramento | REDSHIFT-EVENT-3678 | ERRO | A operação de desabilitação de multi-AZ para o cluster [nome do cluster] do Amazon Redshift apresentou falha às [hora em UTC]. |
| Configuração | REDSHIFT-EVENT-3679 | INFO | A porta do cluster [nome do cluster] do Amazon Redshift foi modificada com êxito. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Configuração | REDSHIFT-EVENT-3680 | ERRO | O Amazon Redshift não conseguiu criar o cluster [nome do cluster] porque o perfil vinculado ao serviço (SLR) necessário para essa operação está inacessível. Tente criá-lo novamente pelo console do Amazon Redshift. O Amazon Redshift criará o SLR automaticamente. |
| Monitoramento | REDSHIFT-EVENT-3684 | ERRO | O bucket do Amazon S3 [nome do bucket] foi criptografado com uma chave do AWS KMS desconhecida ou inacessível. Modifique a criptografia do bucket do Amazon S3. |
| Gerenciamento | REDSHIFT-EVENT-3685 | ERRO | A operação de restauração no cluster [nome do cluster] falhou porque o espaço disponível em disco não é suficiente. A operação está sendo revertida. Tente restaurar em um cluster com outra configuração. |
| Gerenciamento | REDSHIFT-EVENT-3686 | ERRO | A operação de restauração no cluster [nome do cluster] falhou porque o espaço disponível em disco não é suficiente. A operação está sendo revertida. Tente restaurar em um cluster com outra configuração. |
| Segurança | REDSHIFT-EVENT-4000 | INFO | Suas credenciais de administrador para o cluster do Amazon Redshift: [nome do cluster] foram atualizadas às [hora]. |
| Segurança | REDSHIFT-EVENT-4001 | INFO | O security group [nome do security group] foi modificado às [hora]. As alterações ocorrerão automaticamente para todos os clusters associados. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Segurança | REDSHIFT-EVENT-4500 | ERRO | O security group [nome do security group] que você forneceu é inválido. Suas alteraçõe s de configuração para o cluster [nome do cluster] não foram aplicadas. Visite o AWS Management Console para corrigir o problema. |
| Segurança | REDSHIFT-EVENT-4501 | ERRO | O security group [nome do security group] especificado no security group de cluster [nome do security group de cluster] não pôde ser encontrado. A autorização não pode ser concluída. |
| Segurança | REDSHIFT-EVENT-4502 | ERRO | As credenciais de administrador do cluster [nome do cluster] do Amazon Redshift não foram atualizadas às [hora] devido a atividade simultânea. Permitir que o workload atual conclua ou reduza o workload ativo e tente novamente a operação. |
| Segurança | REDSHIFT-EVENT-4503 | ERRO | O Amazon Redshift não consegue acessar o segredo do cluster [cluster name]. |
| Segurança | REDSHIFT-EVENT-4504 | ERRO | O Amazon Redshift não consegue acessar a chave KMS [KMS key] que foi usada para criptografar o segredo das credenciais de administrador do cluster [cluster name]. |
| Segurança | REDSHIFT-EVENT-4505 | ERRO | O Amazon Redshift não consegue alternar o segredo do cluster [cluster name] porque há uma operação em andamento no cluster. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Segurança | REDSHIFT-EVENT-4506 | ERRO | O cluster do Amazon Redshift [cluster name] está pausado. O Amazon Redshift não consegue alternar os segredos de clusters pausados. |

A tabela a seguir mostra a categoria de evento e uma lista de eventos quando um parameter group é o tipo de origem.

Categorias e eventos para o tipo de origem do grupo de parâmetros

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Configuração | REDSHIFT-EVENT-1002 | INFO | O parâmetro [nome do parâmetro] foi atualizado de [valor] para [valor] às [hora]. |
| Configuração | REDSHIFT-EVENT-1003 | INFO | O parameter group de cluster [nome do grupo] foi criado. |
| Configuração | REDSHIFT-EVENT-1004 | INFO | O parameter group de cluster [nome do grupo] foi excluído. |
| Configuração | REDSHIFT-EVENT-1005 | INFO | O parameter group de cluster [nome ] foi atualizado às [hora]. Se você alterou apenas os parâmetros dinâmicos, os clusters associados estão sendo modificados agora. Se você alterou os parâmetros estáticos, todas as atualizaç ões, incluindo parâmetros dinâmicos, serão aplicadas quando você reinicializar os clusters associados. |

As tabelas a seguir mostram a categoria de evento e uma lista de eventos quando um security group é o tipo de origem.

Categorias e eventos o tipo de origem do grupo de segurança

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Segurança | REDSHIFT-EVENT-4002 | INFO | O security group de cluster [nome do grupo] foi criado. |
| Segurança | REDSHIFT-EVENT-4003 | INFO | O security group de cluster [nome do grupo] foi excluído. |
| Segurança | REDSHIFT-EVENT-4004 | INFO | O security group de cluster [nome do grupo] foi alterado às [hora]. As alteraçõe s serão automaticamente aplicadas para todos os clusters associados. |

As tabelas a seguir mostram a categoria de evento e uma lista de eventos quando um snapshot é o tipo de origem.

Categorias e eventos para o tipo de origem do snapshot

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| Gerenciam ento | REDSHIFT-EVENT-2009 | INFO | Um snapshot do usuário [nome do snapshot] para o cluster do Amazon Redshift [nome do cluster] iniciado às [hora]. Para monitorar o progresso do snapshot, acesse o AWS Management Console. |
| Gerenciam ento | REDSHIFT-EVENT-2010 | INFO | O snapshot de usuário [nome do snapshot] para seu cluster do Amazon |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
|---|---|---|---|
| | | | Redshift [nome do cluster] foi cancelado às [hora]. |
| Gerenciamento | REDSHIFT-EVENT-2011 | INFO | O snapshot de usuário [nome do snapshot] do cluster do Amazon Redshift [nome do cluster] foi excluído às [hora]. |
| Gerenciamento | REDSHIFT-EVENT-2012 | INFO | O snapshot final [nome do snapshot] do cluster do Amazon Redshift [nome do cluster] foi iniciado às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3004 | INFO | O snapshot de usuário [nome do snapshot] para seu cluster do Amazon Redshift [nome do cluster] foi concluído com êxito às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3005 | INFO | O snapshot final [nome do snapshot] para o cluster do Amazon Redshift [nome] foi concluído com êxito às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3006 | INFO | O snapshot final [nome do snapshot] para o cluster do Amazon Redshift [nome do cluster] foi cancelado às [hora]. |
| Monitoramento | REDSHIFT-EVENT-3502 | ERRO | O snapshot final [nome do snapshot] para o cluster do Amazon Redshift [nome do cluster] falhou às [hora]. A equipe está investigando o problema. Visite o AWS Management Console para tentar a operação novamente. |

| Categoria do Amazon Redshift | ID do evento | Gravidade do evento | Descrição |
| --- | --- | --- | --- |
| Monitoramento | REDSHIFT-EVENT-3503 | ERRO | O snapshot de usuário [nome do snapshot] para o cluster do Amazon Redshift [nome do cluster] falhou às [hora]. A equipe está investigando o problema. Visite o AWS Management Console para tentar a operação novamente. |

# Notificações de eventos do Amazon Redshift sem servidor com o Amazon EventBridge

O Amazon Redshift Serverless usa o Amazon EventBridge para gerenciar notificações de eventos a fim de manter você atualizado em relação às alterações no data warehouse. O Amazon EventBridge é uma tecnologia sem servidor de barramento de eventos que você pode usar para facilitar a conexão de aplicações a dados de diversas origens. Nesse caso, a fonte do evento é o Amazon Redshift. Os eventos, que são alterações monitoradas em um ambiente, são enviados automaticamente para o EventBridge pelo data warehouse do Amazon Redshift. Os eventos são entregues quase em tempo real.

Os recursos do EventBridge incluem o fornecimento de um ambiente para você escrever regras de eventos, que podem especificar ações a serem realizadas para eventos específicos. Você também pode configurar destinos, que são recursos para os quais o EventBridge pode enviar um evento. Um destino pode incluir um destino de API, um grupo de logs do Amazon CloudWatch, entre outros. Para obter mais informações sobre regras, consulte Regras do Amazon EventBridge. Para obter mais informações sobre destinos, consulte Destinos do Amazon EventBridge.

Os eventos podem ser classificados em gravidades e categorias. Os seguintes filtros estão disponíveis:

- Filtragem de recursos: receba mensagens com base no recurso ao qual os eventos estão associados. Os recursos incluem um grupo de trabalho, um snapshot e assim por diante.
- Filtro de janela de tempo: eventos do escopo em um período específico.

- Filtragem de categorias - é possível receber notificações de eventos para todos os eventos nas categorias especificadas.

A tabela a seguir inclui eventos do Amazon Redshift Serverless, com metadados adicionais:

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| RateChange | REDSHIFT-SERVERLESS-EVENT-1001 | INFO | Alteração da RPU base do grupo de trabalho concluída com êxito às <time in UTC>. |
| RateChange | REDSHIFT-SERVERLESS-EVENT-1002 | ERRO | Falha na alteração da RPU base do grupo de trabalho às <time in UTC>. |
| Monitoramento | REDSHIFT-SERVERLESS-EVENT-1003 | INFO | O software foi atualizado no seu Data Warehouse do Amazon Redshift <endpoint name> às <time in UTC>. |
| Configuração | REDSHIFT-SERVERLESS-EVENT-1011 | ERRO | O Amazon Redshift sem servidor não conseguiu criar o grupo de trabalho [nome do grupo de trabalho] porque o perfil vinculado ao serviço (SLR) |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
| --- | --- | --- | --- |
| | | | necessário para essa operação está inacessível. Tente criá-lo novamente no console do Amazon Redshift. O Amazon Redshift criará o SLR automaticamente. |
| Monitoramento | REDSHIFT-SERVERLESS-EVENT-1500 | ERRO | Não foi possível criar ou atualizar o grupo de trabalho <workgroup name> porque você excedeu o limite de endereços IP elásticos da sua conta. Exclua os endereços IP elásticos não utilizados ou solicite um aumento de limite do Amazon EC2. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
| --- | --- | --- | --- |
| Monitoramento | REDSHIFT-SERVERLESS-EVENT-1501 | ERRO | A sub-rede <subnet id> não tem endereços IP disponíveis. Isso impedirá que os seguintes tipos de consulta sejam executados com êxito no grupo de trabalho <workgroup name>: EMR, consultas federadas, COPY/UNLOAD do Amazon EC2. Para corrigir o problema, libere IPs em sua sub-rede excluindo ENIs. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Monitoramento | REDSHIFT-SERVERLESS-EVENT-1502 | ERRO | A sub-rede <subnet id> não tem endereços IP disponíveis. Isso impedirá que os tipos de consulta Amazon EMR, consultas federadas do Redshift, COPY/UNLOAD do Redshift e Redshift ML sejam executados com êxito no grupo de trabalho <workgroup name>. Para corrigir o problema, libere IPs em sua sub-rede excluindo interfaces de rede elástica (ENIs). |
| Gerenciamento | REDSHIFT-SERVERLESS-EVENT-1008 | INFO | Seu grupo de trabalho do Amazon Redshift <workgroup name> foi criado e está pronto para uso. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Gerenciamento | REDSHIFT-SERVERLESS-EVENT-1009 | INFO | Seu grupo de trabalho do Amazon Redshift <workgroup name> foi excluído às <time in UTC>. |
| Monitoramento | REDSHIFT-SERVERLESS-EVENT-1000 | INFO | Snapshot <snapshot name> realizado com êxito às <time in UTC>. |
| Gerenciamento | REDSHIFT-SERVERLESS-EVENT-1004 | INFO | Restauração do snapshot no namespace <namespace name> concluída com êxito às <time in UTC>. |
| Gerenciamento | REDSHIFT-SERVERLESS-EVENT-1005 | ERRO | Falha na restauração do snapshot no namespace <namespace name> às <time in UTC>. |
| Gerenciamento | REDSHIFT-SERVERLESS-EVENT-1006 | INFO | Restauração do ponto de recuperação no namespace <namespace name> concluída com êxito às <time in UTC>. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Gerenciamento | REDSHIFT-SERVERLESS-EVENT-1007 | INFO | Falha na restauração do ponto de recuperação no namespace <namespace name> às <time in UTC>. |
| Segurança | REDSHIFT-SERVERLESS-EVENT-1012 | ERRO | O Amazon Redshift não consegue acessar o segredo do namespace <namespace name>. |
| Segurança | REDSHIFT-SERVERLESS-EVENT-1013 | ERRO | O Amazon Redshift não consegue acessar a chave KMS que foi usada para criptografar o segredo das credenciais de administrador do namespace <namespace name>. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Segurança | REDSHIFT-SERVERLESS-EVENT-1014 | ERRO | O Amazon Redshift não consegue alternar o segredo do namespace <namespace name> porque há uma operação em andamento no grupo de trabalho. |
| Segurança | REDSHIFT-SERVERLESS-EVENT-1015 | ERRO | O namespace <namespace name> não tem um grupo de trabalho anexado. O Amazon Redshift só pode alternar segredos para namespaces com grupos de trabalho anexados. |
| Segurança | REDSHIFT-SERVERLESS-EVENT-1016 | INFO | As credenciais de administrador do namespace <namespace name> foram atualizadas às <time in UTC>. |

# Notificações de evento da integração ETL zero com o Amazon EventBridge

A integração ETL zero usa o Amazon EventBridge para gerenciar notificações de eventos a fim de manter você por dentro das alterações feitas nas integrações. O Amazon EventBridge é uma tecnologia sem servidor de barramento de eventos que você pode usar para facilitar a conexão de aplicações a dados de diversas origens. Nesse caso, a fonte do evento é o Amazon Redshift. Os eventos, que são alterações monitoradas em um ambiente, são enviados automaticamente para o EventBridge pelo data warehouse do Amazon Redshift. Os eventos são entregues quase em tempo real.

O EventBridge oferece um ambiente para você gravar regras de evento, capazes de especificar medidas a serem tomadas para eventos específicos. Você também pode configurar destinos, que são recursos para os quais o EventBridge pode enviar um evento. Um destino pode incluir um destino de API, um grupo de logs do Amazon CloudWatch, entre outros. Para obter mais informações sobre regras, consulte Regras do Amazon EventBridge. Para obter mais informações sobre destinos, consulte Destinos do Amazon EventBridge.

Os eventos podem ser classificados em gravidades e categorias. Os seguintes filtros estão disponíveis:

- Filtragem de recursos: receba mensagens com base no recurso ao qual os eventos estão associados. Entre os recursos está um grupo de trabalho ou um snapshot.
- Filtro de janela de tempo: eventos do escopo em um período específico.
- Filtragem de categorias - é possível receber notificações de eventos para todos os eventos nas categorias especificadas.

Esta tabela inclui eventos de integração ETL zero, com metadados adicionais:

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0000 | INFO | A integração ETL zero <integration |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| | | | name> foi criada e já está ATIVA. |
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0001 | INFO | A integração ETL zero <integration name> foi excluída às <time in UTC>. |
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0002 | INFO | Exclusão da integração ETL zero <integration name> iniciada às <time in UTC>. |
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0003 | INFO | A integração ETL zero <integration name> está sincronizando dados transacionais com o data warehouse de destino. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0004 | WARNING | Uma ou mais tabelas não têm uma chave primária e não podem ser sincronizadas. Faça um backup no Amazon RDS, descarte essas tabelas e as recrie seguindo as melhores práticas do Amazon Redshift para projetar tabelas. |
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0005 | WARNING | Uma ou mais tabelas não podem ser sincronizadas porque contêm tipos ou tamanhos de dados não compatíveis. Corrija as tabelas e tente novamente. Para obter tipos de dados não compatíveis, consulte Unsupported data types. |
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0006 | ERRO | Não foi possível criar a integração. Exclua e recrie a integração. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0007 | ERRO | Não foi possível carregar dados por causa de uma falha interna. Exclua e recrie a integração. |
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0008 | ERRO | Falha na autorização porque as permissões foram revogadas no cluster do banco de dados do Aurora de origem. Exclua e recrie a integração. |
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0009 | ERRO | Não foi possível enviar dados para o Amazon Redshift porque o número de tabelas e esquemas excede o limite do Amazon Redshift. Exclua e recrie a integração. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0012 | ERRO | Uma restauração do ponto de recuperação foi invocada no namespace de tecnologia sem servidor de destino. Exclua e recrie a integração. |
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0013 | INFO | A integração ETL zero <integration name> já está ATIVA. |
| Monitoramento | REDSHIFT-INTEGRATION-EVENT-0014 | ERRO | Falha na integração <integration name> porque não foi possível modificá-la por causa de um erro interno. Exclua e recrie a integração. Se o erro persistir, entre em contato com o suporte da AWS. |
| Operation | REDSHIFT-INTEGRATION-EVENT-0015 | INFO | Uma alteração DDL <DDL Change> foi aplicada à tabela <schema.name>. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Operation | REDSHIFT-INTEGRATION-EVENT-0016 | INFO | A integração ETL zero <integration name> está processando uma solicitação de modificação com os seguintes argumentos: <copy of request arguments>. |
| Operation | REDSHIFT-INTEGRATION-EVENT-0017 | INFO | A modificação feita na integração ETL zero <integration name> foi aplicada. |
| Operation | REDSHIFT-INTEGRATION-EVENT-0018 | WARNING | O cluster do Amazon Redshift de destino está sendo pausado. Aguarde o cluster ser pausado e, em seguida, retome-o para continuar transmitindo dados. |
| Operation | REDSHIFT-INTEGRATION-EVENT-0019 | WARNING | O cluster do Amazon Redshift de destino está sendo pausado. Retome o cluster para continuar transmitindo dados. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Operation | REDSHIFT-INTEGRATION-EVENT-0020 | WARNING | O cluster do Amazon Redshift de destino está sendo retomado. Aguarde o cluster estar ativo para continuar transmitindo dados. |
| Configuração | REDSHIFT-INTEGRATION-EVENT-1000 | ERRO | Um ou mais parâmetros no cluster do banco de dados do Aurora de origem estão configurados incorretamente. Corrija o grupo de parâmetros e reinicialize o cluster para aplicar as alterações e, em seguida, recrie a integração. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Configuração | REDSHIFT-INTEGRATION-EVENT-1001 | ERRO | Falha na integração porque o valor do parâmetro enable_case_sensitive_identifier está incorreto. Defina o valor como verdadeiro para o cluster do banco de dados do Aurora de origem e, em seguida, exclua e recrie a integração. |
| Configuração | REDSHIFT-INTEGRATION-EVENT-1002 | ERRO | Falha na integração porque o valor do parâmetro cdc_insert_enabled está incorreto. Defina o valor como verdadeiro para o cluster do banco de dados do Aurora de origem e, em seguida, exclua e recrie a integração. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Configuração | REDSHIFT-INTEGRATION-EVENT-1003 | ERRO | O parâmetro binlog_format no grupo de parâmetros do cluster do banco de dados de origem deve ser definido como ROW. Corrija o grupo de parâmetros e reinicialize o cluster para aplicar a alteração e, em seguida, recrie a integração. |
| Configuração | REDSHIFT-INTEGRATION-EVENT-1004 | ERRO | Não foi possível carregar dados porque o parâmetro do cluster binlog_transaction_compression está habilitado. Defina o valor do parâmetro como OFF e reinicialize a instância do gravador para aplicar a alteração e, em seguida, recrie a integração. |

| Categoria do Amazon Redshift | ID do evento externo | Problemas de segurança do evento | Descrição da mensagem |
|---|---|---|---|
| Configuração | REDSHIFT-INTEGRATION-EVENT-1005 | ERRO | Não foi possível carregar dados porque o parâmetro do cluster binlog_row_value_options está definido como PARTIAL_JSON, que não é compatível. Corrija o grupo de parâmetros e reinicialize a instância do gravador para aplicar a alteração e, em seguida, recrie a integração. |
| Configuração | REDSHIFT-INTEGRATION-EVENT-1006 | WARNING | Não foi possível analisar o filtro de integração. Corrija a sintaxe do filtro. |

# Cotas e limites no Amazon Redshift

O Amazon Redshift possui cotas que limitam o uso de vários recursos em sua conta da AWS por região da AWS. Há um valor padrão para cada cota, e algumas cotas são ajustáveis. Para cotas ajustáveis, você pode solicitar um aumento para sua conta da AWS em uma região da AWS enviando um Formulário de aumento de limite do Amazon Redshift.

## Cotas para objetos do Amazon Redshift

O Amazon Redshift tem cotas que limitam o uso de vários tipos de objeto. Há um valor padrão para cada um.

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Contas da AWS que você pode autorizar para restaurar um snapshot por snapshot | 20 | Não | O número máximo de contas da AWS que você pode autorizar para restaurar um snapshot, por snapshot. |
| Contas da AWS que você pode autorizar para restaurar um snapshot | 100 | Não | O número máximo de contas da AWS que você pode autorizar para restaurar um snapshot, por chave do KMS. Ou seja, se você tiver 10 snapshots criptografados com uma única chave KMS, poderá autorizar 10 contas da AWS para restaurar cada snapshot ou outras combinações que adicionem até 100 contas e não excedam 20 contas para cada snapshot. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| por AWS KMS key | | | |
| Funções do IAM de cluster para o Amazon Redshift acessar outros serviços da AWS | 50[1] | Não | O número máximo de funções do IAM que podem ser associadas a um cluster para autorizar o Amazon Redshift a acessar outros serviços da AWS para o usuário proprietário do cluster e das funções do IAM.<br>[1]O limite é 10 nas seguintes Regiões da AWS: us-iso-east-1, us-iso-west-1, us-isob-east-1. |
| Nível de simultaneidade (slots de consulta) para todas as filas manuais do WLM definidas pelo usuário | 50 | Não | O máximo de slots de consulta para todas as filas definidas pelo usuário definidas pelo gerenciamento manual do workload. |
| Clusters de escalabilidade de simultaneidade | 10 | Sim | O número máximo de clusters de escalabilidade de simultaneidade. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Nós DC2 em um cluster | 128 | Sim | O número máximo de nós DC2 que você pode alocar a um cluster. Para obter mais informações sobre os limites de nó para cada tipo de nó, consulte Clusters e nós no Amazon Redshift. |
| Nós DS2 em um cluster | 128 | Sim | O número máximo de nós DS2 que você pode alocar para um cluster. Para obter mais informações sobre os limites de nó para cada tipo de nó, consulte Clusters e nós no Amazon Redshift. |
| Assinaturas de eventos | 20 | Sim | O número máximo de assinaturas de eventos para esta conta na região atual da AWS. |
| Nodes | 200 | Sim | O número máximo de nós em todas as instâncias de banco de dados para esta conta na região atual da AWS. |
| Grupos de parâmetros | 20 | Não | O número máximo de grupos de parâmetros para esta conta na região atual da AWS. |
| Nós RA3 em um cluster | 128 | Sim | O número máximo de nós RA3 que você pode alocar para um cluster. Para obter mais informações sobre os limites de nó para cada tipo de nó, consulte Clusters e nós no Amazon Redshift. |
| Endpoints da VPC gerenciados por Redshift e conectados a um cluster | 30 | Sim | O número máximo de endpoints da VPC gerenciados por Redshift que podem ser conectados a um cluster. Para obter mais informações sobre endpoints da VPC gerenciados por Redshift, consulte Trabalhando com endpoints da VPC gerenciados por Redshift. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Favorecidos para cluster acessado por meio de um endpoint da VPC gerenciado por RedShift | 5 | Sim | O número máximo de favorecidos que um proprietário de cluster pode autorizar a criar um endpoint da VPC gerenciado por RedShift para um cluster. Para obter mais informações sobre endpoints da VPC gerenciados por Redshift, consulte Trabalhando com endpoints da VPC gerenciados por Redshift. |
| Endpoints da VPC gerenciados por Redshift por autorização | 5 | Sim | O número máximo de endpoints da VPC gerenciados por Redshiftque podem ser criados por autorização. Para obter mais informações sobre endpoints da VPC gerenciados por Redshift, consulte Trabalhando com endpoints da VPC gerenciados por Redshift. |
| Nós reservados | 200 | Sim | O número máximo de nós reservados para esta conta na região atual da AWS. |
| Esquemas em cada banco de dados por cluster | 9.900 | Não | O número máximo de esquemas que você pode criar em cada banco de dados, por cluster. No entanto, os esquemas `pg_temp_*` não entram nessa cota. |
| Grupos de segurança | 20 | Sim | O número máximo de grupos de segurança para esta conta na região atual da AWS. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Tamanho de linha única ao carregar por COPY | 4 | Não | O tamanho máximo (em MB) de uma única linha ao carregar usando o comando COPY. |
| Snapshots | 20 | Sim | O número máximo de snapshots de usuário para esta conta na região atual da AWS. |
| Grupos de sub-rede | 20 | Sim | O número máximo de grupos de sub-redes para esta conta na região atual da AWS. |
| Sub-redes em um grupo de sub-redes | 20 | Sim | O número máximo de sub-redes para um grupo de sub-redes. |
| Tabelas para o tipo de nó de cluster `large` | 9.900 | Não | O número máximo de tabelas para o tipo de nó de cluster grande. Esse limite inclui tabelas permanentes, tabelas temporárias, tabelas de unidade de compartilhamento de dados e visualizações materializadas. Tabelas externas são contabilizadas como tabelas temporárias. As tabelas temporárias incluem tabelas temporárias definidas pelo usuário e tabelas temporárias criadas pelo Amazon Redshift durante o processamento de consultas ou manutenção do sistema. As visualizações e tabelas de sistemas não estão incluídas nesse limite. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
| --- | --- | --- | --- |
| Tabelas para o tipo de nó de cluster `xlarge` | 9.900 | Não | O número máximo de tabelas para o tipo de nó de cluster `xlarge`. Esse limite inclui tabelas permanentes, tabelas temporárias, tabelas de unidade de compartilhamento de dados e visualizações materializadas. Tabelas externas são contabilizadas como tabelas temporárias. As tabelas temporárias incluem tabelas temporárias definidas pelo usuário e tabelas temporárias criadas pelo Amazon Redshift durante o processamento de consultas ou manutenção do sistema. As visualizações e tabelas de sistemas não estão incluídas nesse limite. |
| Tabelas para tipo de nó de cluster `xlplus` com um cluster de nó único. | 9.900 | Não | O número máximo de tabelas para o tipo de nó de cluster `xlplus` com um cluster de nó único. Esse limite inclui tabelas permanentes, tabelas temporárias, tabelas de unidade de compartilhamento de dados e visualizações materializadas. Tabelas externas são contabilizadas como tabelas temporárias. As tabelas temporárias incluem tabelas temporárias definidas pelo usuário e tabelas temporárias criadas pelo Amazon Redshift durante o processamento de consultas ou manutenção do sistema. As visualizações e tabelas de sistemas não estão incluídas nesse limite. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
| --- | --- | --- | --- |
| Tabelas para tipo de nó de cluster `xlplus` com um cluster de vários nós. | 20.000 | Não | O número máximo de tabelas para o tipo de nó de cluster `xlplus` com um cluster de vários nós. Esse limite inclui tabelas permanentes, tabelas temporárias, tabelas de unidade de compartilhamento de dados e visualizações materializadas. Tabelas externas são contabilizadas como tabelas temporárias. As tabelas temporárias incluem tabelas temporárias definidas pelo usuário e tabelas temporárias criadas pelo Amazon Redshift durante o processamento de consultas ou manutenção do sistema. As visualizações e tabelas de sistemas não estão incluídas nesse limite. |
| Tabelas para o tipo de nó de cluster `4xlarge` | 200.000 | Não | O número máximo de tabelas para o tipo de nó de cluster `4xlarge`. Esse limite inclui tabelas permanentes, tabelas temporárias, tabelas de unidade de compartilhamento de dados e visualizações materializadas. Tabelas externas são contabilizadas como tabelas temporárias. As tabelas temporárias incluem tabelas temporárias definidas pelo usuário e tabelas temporárias criadas pelo Amazon Redshift durante o processamento de consultas ou manutenção do sistema. As visualizações e tabelas de sistemas não estão incluídas nesse limite. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Tabelas para o tipo de nó de cluster `8xlarge` | 200.000 | Não | O número máximo de tabelas para o tipo de nó de cluster `8xlarge`. Esse limite inclui tabelas permanentes, tabelas temporárias, tabelas de unidade de compartilhamento de dados e visualizações materializadas. Tabelas externas são contabilizadas como tabelas temporárias. As tabelas temporárias incluem tabelas temporárias definidas pelo usuário e tabelas temporárias criadas pelo Amazon Redshift durante o processamento de consultas ou manutenção do sistema. As visualizações e tabelas de sistemas não estão incluídas nesse limite. |
| Tabelas para o tipo de nó de cluster `16xlarge` | 200.000 | Não | O número máximo de tabelas para o tipo de nó de cluster `16xlarge`. Esse limite inclui tabelas permanentes, tabelas temporárias, tabelas de unidade de compartilhamento de dados e visualizações materializadas. Tabelas externas são contabilizadas como tabelas temporárias. As tabelas temporárias incluem tabelas temporárias definidas pelo usuário e tabelas temporárias criadas pelo Amazon Redshift durante o processamento de consultas ou manutenção do sistema. As visualizações e tabelas de sistemas não estão incluídas nesse limite. |
| Número de bancos de dados | 60 | Não | A contagem máxima permitida de bancos de dados em um cluster do Amazon Redshift. Isso exclui bancos de dados criados de unidades de compartilhamento de dados. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Tempo limite para sessões ociosas ou inativas | 4 horas | Não | Esta configuração se aplica ao cluster. Para obter informações sobre como definir o valor de tempo limite de sessão ociosa para um usuário, consulte ALTER US no Guia do desenvolvedor de banco de dados do Amazon Redshift. A configuração do usuário tem precedência sobre a configuração do cluster. |
| Tempo limite para transações ociosas | 6 horas | Não | O período máximo de inatividade para uma transação aberta antes que o Amazon Redshift encerre a sessão associada à transação. Essa configuração tem precedência sobre outras configurações de tempo limite ocioso definido pelo usuário. Ela se aplica ao cluster. |
| Procedimentos armazenados em um banco de dados | 10.000 | Não | O número máximo de procedimentos armazenados. Consulte Limites e diferenças para o suporte a procedimento armazenado para mais limites. |
| Número máximo de conexões para nós RA3 | 2.000 | Não | O número máximo de conexões com um cluster RA3. (Isso se aplica especificamente aos tipos de nó ra3.xlplus, ra3.4xlarge e ra3.16xlarge.) O máximo de conexões permitidas varia de acordo com o tipo de nó. |
| Número máximo de conexões para nós DC2 e DS2 | Varia | Não | O número máximo de conexões com um cluster dc2.large ou um cluster ds2.large é 500. O número máximo de coleções para um cluster dc2.8xlarge ou ds2.8xlarge é 2.000. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Número de funções do Amazon Redshift em um cluster | 1.000 | Sim | O número máximo de funções do Amazon Redshift que é possível criar por cluster. Para obter mais informações sobre funções do controle de acesso baseado em perfil (RBAC), consulte Role-based access control (RBAC) no Guia de desenvolvedor do banco de dados do Amazon Redshift |

## Cotas para objetos do Amazon Redshift Serverless

O Amazon Redshift tem cotas que limitam o uso de vários tipos de objeto na instância do Amazon Redshift Serverless. Há um valor padrão para cada um.

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Número de bancos de dados | 100 | Não | A contagem máxima permitida de bancos de dados em um namespace do Amazon Redshift sem servidor. Isso exclui bancos de dados criados de unidades de compartilhamento de dados. |
| Número de esquemas | 9.900 | Não | A contagem máxima permitida de esquemas em uma instância do Amazon Redshift Serverless. |
| Número de tabelas | 200.000 | Não | A contagem máxima permitida de tabelas em uma instância do Amazon Redshift Serverless. |
| Tempo limite para sessões ociosas ou inativas | 1 hora | Não | Para obter informações sobre como definir o valor de tempo limite de sessão ociosa para um usuário, consulte ALTER US no Guia do desenvolvedor de banco de dados do Amazon Redshift. A configuração do usuário tem precedência. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Tempo limite de uma consulta em execução | 86.399 segundos (24 horas) | Não | O tempo máximo que uma consulta pode ficar em execução antes que o Amazon Redshift a encerre. |
| Tempo limite para transações ociosas | 6 horas | Não | O período máximo de inatividade para uma transação aberta antes que o Amazon Redshift Serverles s encerre a sessão associada à transação. Essa configuração tem precedência sobre outras configura ções de tempo limite ocioso definido pelo usuário. |
| Número máximo de conexões | 2000 | Não | O número máximo de conexões permitido para se conectar a um grupo de trabalho. |
| Número de grupos de trabalho | 25 | Sim | O número de grupos de trabalho compatíveis. |
| Número de namespace s | 25 | Sim | O número de namespaces compatíveis. |
| Número de funções do Amazon Redshift em um grupo de trabalho | 1.000 | Sim | O número máximo de funções do Amazon Redshift que é possível criar por grupo de trabalho. Para obter mais informações sobre funções do controle de acesso baseado em perfil (RBAC), consulte Role-base d access control (RBAC) no Guia de desenvolvedor do banco de dados do Amazon Redshift |

Para obter mais informações sobre como o faturamento do Amazon Redshift Serverless é afetado pela configuração de tempo limite, consulte Faturamento do Amazon Redshift Serverless.

# Cotas da API de dados do Amazon Redshift

O Amazon Redshift tem cotas que limitam o uso da API de dados do Redshift. Há um valor padrão para cada um. Para obter mais informações sobre a API de dados do Amazon Redshift, consulte Usar a API de dados Amazon Redshift.

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Transações por segundo (TPS) para a API `BatchExecuteStatement` | 20 | Não | O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. |
| Transações por segundo (TPS) para a API `CancelStatement` | 3 | Não | O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. |
| Transações por segundo (TPS) para a API `DescribeStatement` | 100 | Não | O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
| --- | --- | --- | --- |
| Transações por segundo (TPS) para a API `DescribeTable` | 3 | Não | O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. |
| Transações por segundo (TPS) para a API `ExecuteStatement` | 30 | Não | O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. |
| Transações por segundo (TPS) para a API `GetStatementResult` | 20 | Não | O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. |
| Transações por segundo (TPS) para a API `ListDatabases` | 3 | Não | O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
| --- | --- | --- | --- |
| Transações por segundo (TPS) para a API `ListSchemas` | 3 | Não | O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. |
| Transações por segundo (TPS) para a API `ListStatements` | 3 | Não | O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. |
| Transações por segundo (TPS) para a API `ListTables` | 3 | Não | O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. |

# Cotas para objetos do editor de consultas v2

O Amazon Redshift tem cotas que limitam o uso de vários tipos de objeto no editor de consultas v2 do Amazon Redshift. Há um valor padrão para cada um.

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| Conexões | 500 | Sim | Número máximo de conexões que você pode criar usando o editor de consultas v2 nesta conta na região atual. |
| Entidades principais ativas por conta | 50 | Sim | Número máximo de entidades principais simultâneas que podem usar o editor de consultas v2 nessa conta na região atual. |
| Consultas salvas | 2.500 | Sim | Número máximo de consultas salvas que você pode criar usando o editor de consultas v2 nesta conta na região atual. |
| Versões de consulta | 20 | Sim | Número máximo de versões por consulta que você pode criar usando o editor de consultas v2 nesta conta na região atual. |
| Gráficos salvos | 500 | Sim | Número máximo de gráficos salvos que você pode criar usando o editor de consultas v2 nesta conta na região atual. |
| Linhas obtidas por consulta | 100.000 | Não | Número máximo de linhas obtidas por consulta pelo editor de consultas v2 nesta conta na região atual. |
| Tamanho dos dados obtidos por consulta | 5 | Não | Tamanho máximo, em megabytes, de dados obtidos por consulta pelo editor de consultas v2 nesta conta na região atual. |
| Conexões de soquete simultâne as por | 10 | Sim | Número máximo de conexões de soquete simultâneas para o editor de consultas v2 que uma única entidade principal pode estabelecer na região atual. Avalie se deve aumentar essa cota se você receber erros |

| Nome da cota | Valor padrão da AWS | Ajustável | Descrição |
|---|---|---|---|
| entidade principal | | | indicando que suas conexões de soquete estão acima do limite. |
| Conexões de soquete simultâneas por conta | 250 | Sim | Número máximo de conexões de soquete simultâneas para o editor de consultas v2 que todas as entidades principais podem estabelecer na região atual. Avalie se deve aumentar essa cota se você receber erros indicando que suas conexões de soquete estão acima do limite. |
| Máximo de conexões simultâneas | 3 | Não | Máximo de conexões de banco de dados por usuário (inclui sessões isoladas). Esse valor pode ser definido de 1 a 10 pelo administrador do editor de consultas v2 em Account settings (Configurações da conta). Se você atingir o limite definido pelo administrador, considere usar sessões compartilhadas em vez de sessões isoladas ao executar seu SQL. Para obter mais informações sobre conexões, consulte Abrir o editor de consultas v2. Para obter mais informações sobre o limite, consulte Alterar as configurações da conta. |

# Cotas e limites para objetos do Amazon Redshift Spectrum

O Amazon Redshift Spectrum tem as seguintes cotas e limites:

- O número máximo de bancos de dados por conta da AWS ao usar um AWS Glue Data Catalog. Para obter esse valor, consulte Cotas do serviço AWS Glue no Referência geral da Amazon Web Services.
- O número máximo de tabelas por banco de dados ao usar um AWS Glue Data Catalog. Para obter esse valor, consulte Cotas do serviço AWS Glue no Referência geral da Amazon Web Services.
- O número máximo de partições por tabela ao usar um AWS Glue Data Catalog. Para obter esse valor, consulte Cotas do serviço AWS Glue no Referência geral da Amazon Web Services.

- O número máximo de partições por conta da AWS ao usar um AWS Glue Data Catalog. Para obter esse valor, consulte Cotas do serviço AWS Glue no Referência geral da Amazon Web Services.
- O número máximo de colunas para tabelas externas ao usar um AWS Glue Data Catalog, 1.597 quando pseudocolunas estão habilitadas e 1.600 quando pseudocolunas não estão habilitadas.
- O tamanho máximo de um valor de string em um arquivo ION ou JSON ao usar um AWS Glue Data Catalog é de 16 KB. A string poderá ser truncada se você atingir esse limite.
- É possível adicionar no máximo 100 partições usando uma única instrução ALTER TABLE.
- Todos os dados do S3 devem estar localizados na mesma região da AWS que o cluster do Amazon Redshift.
- Os timestamps em Ion e JSON precisam ter formato ISO8601.
- Não há suporte para a compactação externa de arquivos ORC.
- Texto, OpenCSV e Regex SERDEs não são compatíveis com delimitadores octais maiores que '\177'.
- Você deve especificar um predicado na coluna de partição para evitar leituras de todas as partições.

  Por exemplo, o seguinte predicado filtra a coluna `ship_dtm`, mas não aplica o filtro à coluna de partição `ship_yyyymm`:

  ```
  WHERE ship_dtm > '2018-04-01'.
  ```

  Para ignorar partições desnecessárias, você precisa adicionar um predicado `WHERE ship_yyyymm = '201804'`. Esse predicado limitará as operações de leitura à partição `\ship_yyyymm=201804\`.

Esses limites não se aplicam a uma metastore do Apache Hive.

# Restrições de nomenclatura

A tabela a seguir descreve as restrições de nomenclatura no Amazon Redshift.

| | |
|---|---|
| Identificador de Cluster | • Um identificador de cluster deve conter somente caracteres em minúsculas.<br>• |

| | |
|---|---|
| | Deve conter de 1 a 63 caracteres alfanuméricos ou hifens.<br>• O primeiro caractere deve ser uma letra.<br>• Não pode terminar com um hífen ou conter dois hifens consecutivos.<br>• Ele deve ser exclusivo para todos os clusters dentro de uma conta da AWS. |
| Database name | • Um nome de banco de dados deve conter de 1 a 64 caracteres alfanuméricos.<br>• Ele deve conter somente letras minúsculas.<br>• Ele não pode ser uma palavra reservada. Para obter uma lista de palavras reservadas, consulte Palavras reservadas no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Nome do endpoint de um endpoint da VPC gerenciado por RedShift | • O nome do endpoint deve conter de 1 a 30 caracteres.<br>• Os caracteres válidos são A-Z, a-z, 0-9 e hífen (-).<br>• O primeiro caractere deve ser uma letra.<br>• O nome não pode conter dois hifens consecutivos ou terminar com um hífen. |

| | |
|---|---|
| Nome de usuário administrador | • Um nome de usuário administrador deve conter somente caracteres em minúsculas.<br>• Deve conter de 1 a 128 caracteres alfanuméricos.<br>• O primeiro caractere deve ser uma letra.<br>• Ele não pode ser uma palavra reservada. Para obter uma lista de palavras reservadas, consulte Palavras reservadas no Guia do desenvolvedor de banco de dados do Amazon Redshift. |
| Senha do Admin | • Uma senha de administrador deve conter de 8 a 64 caracteres.<br>• Ela deve conter pelo menos uma letra maiúscula.<br>• Ela deve conter pelo menos uma letra minúscula.<br>• Ela deve conter um número.<br>• Ele pode usar qualquer caractere ASCII com os códigos ASCII 33–126, exceto ' (aspas simples), " (aspas duplas), \, / ou @. |
| Nome do parameter group | • Um nome de grupo de parâmetros deve conter de 1 a 255 caracteres alfanuméricos ou hifens.<br>• Ele deve conter somente caracteres minúsculos.<br>• O primeiro caractere deve ser uma letra.<br>• Não pode terminar com um hífen ou conter dois hífens consecutivos. |

| | |
|---|---|
| Nome do grupo de segurança do cluster | • Um nome de grupo de segurança do cluster não deve conter mais de 255 caracteres alfanuméricos ou hifens.<br>• Ele deve conter somente caracteres minúsculos.<br>• Ele não deve ser **`Default`**.<br>• Ele deve ser exclusivo para todos os grupos de segurança criados pela conta da AWS. |
| Nome do grupo de sub-redes | • Um nome do grupo de sub-redes não deve conter mais de 255 caracteres alfanuméricos ou hifens.<br>• Ele deve conter somente caracteres minúsculos.<br>• Ele não deve ser **`Default`**.<br>• Ele deve ser exclusivo para todos os grupos de sub-rede criados pela conta da AWS. |
| Identificador de snapshot do cluster | • Um identificador de snapshot do cluster não deve conter mais de 255 caracteres alfanuméricos ou hifens.<br>• Ele deve conter somente caracteres minúsculos.<br>• Ele não deve ser **`Default`**.<br>• Ele deve ser exclusivo para todos os identificadores de snapshot criados pela conta da AWS. |

# Marcação de recursos no Amazon Redshift

Tópicos


- Visão geral da marcação
- Gerenciamento de tags de recursos usando o console
- Gerenciar etiquetas usando a API do Amazon Redshift


## Visão geral da marcação

Na AWS, as etiquetas são rótulos definidos pelo usuário que consistem em pares de chave-valor. O Amazon Redshift oferece suporte para marcações para fornecer metadados sobre recursos rapidamente e para categorizar seus relatórios de faturamento com base na alocação de custos. Para usar tags para alocação de custo, você deve primeiro ativar essas tags no serviço do AWS Billing and Cost Management. Para obter mais informações sobre a configuração e o uso de tags para fins de faturamento, consulte Usar tags de alocação de custos para relatórios de faturamento personalizados e Configuração do relatório de alocação de custo mensal.

As marcações não são necessárias para recursos no Amazon Redshift, mas ajudam a fornecer contexto. Talvez você queira marcar recursos com tags com metadados sobre centros de custo, nomes de projeto e outras informações pertinentes relacionadas ao recurso. Por exemplo, suponha que você queira rastrear quais recursos pertencem a um ambiente de teste e a um ambiente de produção. Você poderia criar uma chave chamada `environment` e fornecer o valor `test` ou `production` para identificar os recursos usados em cada ambiente. Se você usa marcação em outros serviços da AWS ou tem categorias padrão para o seu negócio, recomendamos que você crie os mesmos pares de chave-valor para recursos no Amazon Redshift para consistência.

As tags são retidas para recursos quando você redimensiona um cluster e quando restaura um snapshot de um cluster dentro da mesma região. No entanto, as tags não são retidas se você copiar um snapshot para outra região, portanto você deve recriar as tags na nova região. Se você excluir um recurso, todas as tags associadas serão excluídas.

Cada recurso tem um conjunto de tags, que é uma coleção de uma ou mais tags atribuídas ao recurso. Cada recurso pode ter até 50 tags por conjunto de tags. Você pode adicionar tags ao criar um recurso e após a criação de um recurso. Você pode adicionar etiquetas aos seguintes tipos de recurso no Amazon Redshift:

- CIDR/IP
- Cluster
- Security group de cluster
- Regra de entrada do security group de cluster
- Grupo de segurança do Amazon EC2
- Conexão do Hardware Security Module (HSM)
- Certificado do cliente HSM
- Grupo de parâmetros
- Snapshot
- Grupo de sub-redes

Para usar a marcação no console do Amazon Redshift, o usuário do IAM pode anexar a política gerenciada pela AWS `AmazonRedshiftFullAccess`. Para obter um exemplo de política do IAM com permissões de marcação limitadas que você pode anexar a um usuário do console do Amazon Redshift, consulte Exemplo 7: permitir que um usuário marque recursos com o console do Amazon Redshift. Para obter mais informações sobre marcação, consulte O que é o AWS Resource Groups?.

## Requisitos de marcação

As tags têm os seguintes requisitos:

- As chaves não podem ser prefixadas com `aws:`.
- As chaves devem ser exclusivas por conjunto de tags.
- Uma chave deve ter entre 1 e 128 caracteres permitidos.
- Um valor deve ter entre 0 e 256 caracteres permitidos.
- Os valores não precisam ser exclusivos por conjunto de tags.
- Os caracteres permitidos para chaves e valores são letras Unicode, dígitos, espaço em branco e qualquer um dos seguintes símbolos: _ . : / = + - @.
- As chaves e os valores diferenciam letras maiúsculas de minúsculas.

# Gerenciamento de tags de recursos usando o console

Para gerenciar etiquetas em seus recursos do Amazon Redshift

1. Faça login no AWS Management Console e abra o console do Amazon Redshift em https://console.aws.amazon.com/redshiftv2/.
2. No menu de navegação, escolha Configurations (Configurações), depois selecione Manage tags (Gerenciar etiquetas).
3. Insira suas opções para os recursos e escolha quais tags adicionar, modificar ou excluir. Depois, escolha Manage tags of the resources that you chose (Gerenciar tags dos recursos escolhidos).

   Os recursos que podem ser marcados incluem clusters, grupos de parâmetros, grupos de sub-redes, certificados de clientes HSM, conexões HSM e snapshots.
4. Na página de navegação Gerenciar tags, escolha Revisar e aplicar alterações de tags e escolha Aplicar para salvar suas alterações.

# Gerenciar etiquetas usando a API do Amazon Redshift

Você pode usar as operações da AWS CLI a seguir para gerenciar eitquetas no Amazon Redshift.

- create-tags
- delete-tags
- describe-tags

Você pode usar as seguintes operações da API do Amazon Redshift para gerenciar tags:

- CreateTags
- DeleteTags
- DescribeTags
- Tag
- TaggedResource

Além disso, você pode usar as seguintes operações da API do Amazon Redshift para gerenciar e visualizar etiquetas de um recurso específico:

- CreateCluster
- CreateClusterParameterGroup
- CreateClusterSecurityGroup
- CreateClusterSnapshot
- CreateClusterSubnetGroup
- CreateHsmClientCertificate
- CreateHsmConfiguration
- DescribeClusters
- DescribeClusterParameterGroups
- DescribeClusterSecurityGroups
- DescribeClusterSnapshots
- DescribeClusterSubnetGroups
- DescribeHsmClientCertificates
- DescribeHsmConfigurations

# Versões de cluster para o Amazon Redshift

O Amazon Redshift lança versões de cluster regularmente. Seus clusters do Amazon Redshift são corrigidos durante a janela de manutenção do sistema. O momento do patch depende de sua Região da AWS e das configurações da janela de manutenção. É possível exibir ou alterar as configurações da janela de manutenção no console do Amazon Redshift. Para obter mais informações sobre manutenção, consulte Manutenção do cluster.

Você pode visualizar a versão de seu cluster no console do Amazon Redshift na guia Maintenance (Manutenção) dos detalhes do cluster. Ou você pode ver a versão do cluster na saída do comando SQL:

```
SELECT version();
```

Tópicos


- Patch 180 do Amazon Redshift
- Patch 179 do Amazon Redshift
- Patch 178 do Amazon Redshift
- Patch 177 do Amazon Redshift
- Patch 176 do Amazon Redshift
- Patch 175 do Amazon Redshift
- Patch 174 do Amazon Redshift
- Patch 173 do Amazon Redshift
- Patch 172 do Amazon Redshift
- Patch 171 do Amazon Redshift
- Patch 170 do Amazon Redshift
- Patch 169 do Amazon Redshift
- Patch 168 do Amazon Redshift


# Patch 180 do Amazon Redshift

Versões de cluster neste patch:

- 1.0.63590: versão atual da faixa: lançada em 19 de fevereiro de 2024
- 1.0.63567: versão do Amazon Redshift sem servidor: lançada em 16 de fevereiro de 2024
- 1.0.63282: versão do Amazon Redshift sem servidor: lançada em 13 de fevereiro de 2024
- 1.0.63269: versão atual da faixa: lançada em 13 de fevereiro de 2024
- 1.0.63215: versão do Amazon Redshift sem servidor: lançada em 12 de fevereiro de 2024
- 1.0.63205: versão atual da faixa: lançada em 12 de fevereiro de 2024
- 1.0.63030: versão do Amazon Redshift sem servidor: lançada em 7 de fevereiro de 2024
- 1.0.62913: versão atual da faixa: lançada em 7 de fevereiro de 2024
- 1.0.62922: versão do Amazon Redshift sem servidor: lançada em 5 de fevereiro de 2024
- 1.0.62878: versão atual da faixa: lançada em 5 de fevereiro de 2024
- 1.0.62698: versão do Amazon Redshift sem servidor: lançada em 31 de janeiro de 2024.
- 1.0.62614: versão atual da faixa: lançada em 31 de janeiro de 2024.
- 1.0.61687: versão do Amazon Redshift sem servidor: lançada em 5 de janeiro de 2024
- 1.0.61678 – Versão atual da faixa – Lançada em 5 de janeiro de 2024
- 1.0.61567 – Versão do Amazon Redshift sem servidor – Lançada em 31 de dezembro de 2023
- 1.0.61559 – Versão da faixa atual – Lançada em 31 de dezembro de 2023
- 1.0.61567 – Versão do Amazon Redshift sem servidor – Lançada em 29 de dezembro de 2023
- 1.0.61395 – Versão da faixa atual – Lançada em 29 de dezembro de 2023

## Novos recursos e melhorias nesse patch

- Altera CURRENT_USER para deixar de truncar o nome de usuário retornado para 64 caracteres.
- Adiciona a capacidade de aplicar políticas de mascaramento de dados em exibições padrão e exbições de vinculação tardia.
- Adiciona a capacidade de aplicar o mascaramento dinâmico de dados (DDM) a atributos escalares em colunas do tipo de dados SUPER.
- Adiciona a função SQL OBJECT_TRANSFORM. Para obter mais informações, consulte OBJECT_TRANSFORM function no Guia de desenvolvedor do banco de dados do Amazon Redshift.
- Adiciona a capacidade de aplicar controle de acesso refinado do AWS Lake Formation aos dados aninhados e consultar usando a análise de data lake do Amazon Redshift.

- Adiciona o tipo de dados INTERVAL.
- Adiciona CONTINUE_HANDLER, que é um tipo de manipulador de exceções que controla o fluxo de um procedimento armazenado. Ao usá-lo, você pode capturar e processar exceções sem encerrar o bloco de instruções existente.
- Adiciona a capacidade de definir permissões em um escopo (esquema ou banco de dados), além de objetos individuais. Isso permite que usuários e funções recebam uma permissão em todos os objetos atuais e futuros dentro do escopo.
- Adiciona a capacidade de criar um banco de dados a partir de uma unidade de compartilhamento de dados com permissões que permitem a administradores no lado do consumidor conceder permissões individuais em objetos de banco de dados compartilhados para usuários e funções no lado do consumidor.
- Adiciona suporte para o tipo de dados de retorno SUPER de modelos BYOM remotos. Isso expande a variedade de modelos do SageMaker aceitos para incluir aqueles com formatos de retorno mais complexos.
- Altera funções externas para agora converter implicitamente números com ou sem partes fracionárias no tipo de dados numéricos da coluna. Para colunas int2, int4 e int8, números com dígitos fracionários são aceitos por truncamento, a menos que o número esteja fora do intervalo. Para colunas float4 e float8, números são aceitos sem dígitos fracionários.
- Adiciona três funções espaciais que funcionam com o sistema da grade de indexação geoespacial hierárquica H3: H3_FromLonglat, H3_FromPoint e H3_Polyfill.

# Patch 179 do Amazon Redshift

Versões de cluster neste patch:

- 1.0.62317: versão do Amazon Redshift sem servidor: lançada em 29 de janeiro de 2024
- 1.0.62312: versão atual da faixa: lançada em 29 de janeiro de 2024.
- 1.0.61631: versão do Amazon Redshift sem servidor: lançada em 5 de janeiro de 2024
- 1.0.61626 – Versão atual da faixa – Lançada em 5 de janeiro de 2024
- 1.0.61191 – Versão da faixa atual – Lançada em 16 de dezembro de 2023
- 1.0.61150 – Versão do Amazon Redshift sem servidor – Lançada em 16 de dezembro de 2023
- 1.0.60982 – Versão do Amazon Redshift sem servidor – Lançada em 13 de dezembro de 2023
- 1.0.60854 – Versão da faixa atual – Lançada em 10 de dezembro de 2023
- 1.0.60354 – Versão do Amazon Redshift sem servidor – Lançada em 22 de novembro de 2023

- 1.0.60353 – Versão da faixa atual – Lançada em 21 de novembro de 2023
- 1.0.60293 – Versão do Amazon Redshift sem servidor – Lançada em 21 de novembro de 2023
- 1.0.60292 – Versão da faixa atual – Lançada em 22 de novembro de 2023
- 1.0.60161 – Versão do Amazon Redshift sem servidor – Lançada em 18 de novembro de 2023
- 1.0.60140 – Versão da faixa atual – Lançada em 18 de novembro de 2023
- 1.0.60139 – Versão do Amazon Redshift sem servidor – Lançada em 18 de novembro de 2023
- 1.0.59947 – Versão do Amazon Redshift sem servidor – Lançada em 16 de novembro de 2023
- 1.0.59945 – Versão da faixa atual – Lançada em 16 de novembro de 2023
- 1.0.59118 – Versão do Amazon Redshift sem servidor – Lançada em 9 de novembro de 2023
- 1.0.59117 – Versão da faixa atual – Lançada em 9 de novembro de 2023

## Novos recursos e melhorias nesse patch

- Adiciona suporte para que usuários federados com permissões indicadas possam exibir a segurança no nível da linha e as exibições de sistema do mascaramento de dados dinâmicas, inclusive:
  - SVV_ATTACHED_MASKING_POLICY
  - SVV_MASKING_POLICY
  - SVV_RLS_ATTACHED_POLICY
  - SVV_RLS_POLICY
  - SVV_RLS_RELATION
- Adiciona funcionalidade para que uma consulta que contenha apenas funções escalares na cláusula FROM agora resulte em um erro.
- Adiciona instruções CREATE TABLE AS (CTAS) com a funcionalidade de tabelas de destino permanentes a clusters de escalabilidade de simultaneidade. Os clusters de escalabilidade de simultaneidade agora dão suporte a mais consultas.
- Adiciona as seguintes tabelas de sistema para rastrear o status de redistribuição da tabela depois da execução do redimensionamento clássico em clusters RA3:
  - A tabela de sistema SYS_RESTORE_STATE mostra o progresso da redistribuição no nível da tabela.
  - A tabela de sistema SYS_RESTORE_LOG mostra o throughput histórico da redistribuição de dados.

- Melhora a distorção de fatias, minimizando tabelas EVEN após a execução do redimensionamento clássico em tipos de nó RA3. Isso também se aplica a clusters do patch 178 que executavam o redimensionamento clássico.
- Adiciona suporte para UNLOAD com EXTENSION em clusters de escalabilidade de simultaneidade.
- Melhora o desempenho para consultas que contenham UDFs Λ em junções HashJoins e NestLoop.
- Melhora o desempenho do redimensionamento elástico em tipos de nó RA3.
- Melhora o desempenho de consultas do compartilhamento de dados.
- Melhora o desempenho de consultas de análise iniciadas manualmente em clusters provisionados com redimensionamento elástico e grupos de trabalho de tecnologia sem servidor.
- Melhora o desempenho da consulta automática WLM com melhor previsão de recursos no gerenciamento do workload.
- Remove a funcionalidade do lançamento de clusters em VPCs de locação dedicadas. Essa alteração não afeta a locação de nenhuma instância EC2 na VPC. Você pode modificar a locação da VPC para o padrão usando o comando `modify-vpc-tenancy` da AWS CLI.
- A atualização manual da visão materializada agora é compatível em clusters provisionados de escalabilidade de simultaneidade e computação de escalonamento automático de tecnologia sem servidor.
- Adiciona suporte para literais INTERVAL à função EXTRACT. Por exemplo, `EXTRACT('hours' from Interval '50 hours')` retorna 2 porque 50 horas são interpretadas como 2 dias e 2 horas, e o componente de hora de 2 é extraído.

# Patch 178 do Amazon Redshift

Versões de cluster neste patch:

- 1.0.63327: versão atual da faixa: lançada em 9 de fevereiro de 2024
- 1.0.63313: versão atual da faixa: lançada em 9 de fevereiro de 2024
- 1.0.60977 – Versão da faixa anterior – Lançada em 15 de dezembro de 2023
- 1.0.59596 – Versão da faixa atual – Lançada em 9 de novembro de 2023
- 1.0.58593 - Versão do Amazon Redshift sem servidor – Lançada em 23 de outubro de 2023
- 1.0.58558 - Versão da faixa atual – Lançada em 23 de outubro de 2023

- 1.0.57864 - Versão da faixa atual – Lançada em 12 de outubro de 2023
- 1.0.57850 - Versão do Amazon Redshift sem servidor – Lançada em 12 de outubro de 2023
- Versão de trilha atual: 1.0.56952 (lançada em 25 de setembro de 2023)
- Versão do Amazon Redshift sem servidor: 1.0.56970 (lançada em 25 de setembro de 2023)

## Novos recursos e melhorias nesse patch

- Agora o Amazon Redshift melhorou a performance das consultas de compartilhamento de dados ao acelerar a atualização de metadados nas instâncias de consumidor, enquanto mudanças simultâneas de dados estão ocorrendo na instância de produtor.
- Adiciona compatibilidade para atualização automática e incremental de visões materializadas em instâncias de consumidor de compartilhamento de dados do Amazon Redshift quando as tabelas base da visão materializada se referem aos dados compartilhados.
- Adiciona compatibilidade para armazenar objetos grandes de até 16 MB no tipo de dados SUPER. Ao ingerir arquivos de origem JSON, PARQUET, TEXT e CSV, você pode carregar até 16 MB de dados ou documentos semiestruturados como valores no tipo de dados SUPER.
- Adiciona compatibilidade para redimensionamento elástico e escalabilidade de e para um cluster RA3 de nó único do Amazon Redshift.
- Os clusters RA3 de nó único do Amazon Redshift agora podem se beneficiar dos aprimoramentos de criptografia, reduzindo o tempo geral de criptografia e melhorando a disponibilidade do data warehouse durante o processo de criptografia.
- Melhora a compatibilidade para consultas ao desaninhar e transformar os dados armazenados no tipo de dados SUPER de colunas para linhas.
- Melhora a performance da atualização de visões materializadas com tipos de dados SUPER.
- Adiciona compatibilidade para agregar literais INTERVAL à função ANY_VALUE.
- A ingestão de streaming agora comporta este novo comando SQL para limpar dados de streaming: `DELETE FROM streaming_materialized_views WHERE <where filter clause>`
- A função DECODE substitui um valor específico por outro valor específico ou por valor padrão, dependendo do resultado de uma condição de igualdade. O DECODE agora requer os três seguintes parâmetros:
  - expressão
  - pesquisa
  - resultado

- Adiciona funcionalidade aos procedimentos armazenados para permitir a identificação de erros de conversão do tipo de dados de transbordamento e o tratamento dentro de um bloco de tratamento de exceções.
- Agora você receberá um erro ao consultar relações protegidas por segurança em nível de linha ou por mascaramento de dados dinâmico se alterar enable_case_sensitive_identifier para ser diferente da configuração padrão da sessão. Além disso, a configuração a seguir é bloqueada quando políticas de segurança em nível de linha ou de política de mascaramento de dados dinâmico são aplicadas ao cluster provisionado ou namespace sem servidor:

  ```
  ALTER USER <current_user> SET case-sensitive identifier.
  ```
- O comando MERGE agora comporta uma sintaxe simplificada que requer apenas a tabela de destino e de origem. Para obter mais informações, consulte MERGE no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- Adiciona compatibilidade para anexar políticas de mascaramento de dados dinâmico idênticas a vários usuários ou funções com a mesma prioridade ou sem especificar a prioridade.
- Agora você pode especificar um AGRUPAMENTO ao adicionar uma nova coluna por meio de ALTER TABLE ADD COLUMN.
- Corrige um problema que atrasa a aplicação das regras de monitoramento de consultas (QMR) em clusters de escalabilidade simultânea e no Amazon Redshift sem servidor.
- A consulta federada do Amazon Redshift ampliou o suporte à aplicação de predicados para fuso horário com registro de data e hora no Amazon RDS para PostgreSQL e no Amazon Aurora PostgreSQL.
- Você já pode usar o Amazon RDS para MySQL e os nomes de banco de dados do Aurora MySQL começando com dígitos com consultas federadas.
- Adiciona a visão SYS_ANALYZE_HISTORY, que contém detalhes de registro para operações ANALYZE.
- Adiciona a visão SYS_ANALYZE_COMPRESSION_HISTORY, que contém detalhes do registro das operações de análise de compressão durante os comandos COPY ou ANALYZE COMPRESSION.
- Adiciona a visão SYS_SESSION_HISTORY, que contém detalhes de registro relacionados a sessões ativas, históricas e reiniciadas.
- Adiciona a visão SYS_TRANSACTION_HISTORY, que contém detalhes de registro relacionados a análise em nível de transação, que fornece o tempo gasto na confirmação, o número de blocos confirmados e o nível de isolamento.

- Adiciona a visão SVV_REDSHIFT_SCHEMA_QUOTA, que contém registros relacionados às cotas e ao uso atual do disco para cada esquema em um banco de dados.
- Adiciona a visão SYS_PROCEDURE_CALL, que contém registros relacionados a chamadas de procedimentos armazenados, incluindo hora de início, hora de término, status da chamada de procedimento armazenado e hierarquia de chamadas de procedimentos armazenados aninhados.
- Adiciona a visão SYS_CROSS_REGION_DATASHARING_USAGE, que contém registros relacionados a rastreamento do uso do compartilhamento de dados entre regiões.
- Adiciona a visão SYS_PROCEDURE_MESSAGES, que contém registros relacionados a informações de rastreamento sobre mensagens registradas do procedimento armazenado.
- Adiciona a visão SYS_UDF_LOG, que contém registros relacionados a rastreamento de mensagens de log do sistema com base em chamadas de função, erros, avisos ou rastreamentos definidos pelo usuário, quando aplicável.
- Adiciona as novas colunas IS_RECURSIVE, IS_NESTED, S3LIST_TIME e GET_PARTITION_TIME a SYS_EXTERNAL_QUERY_DETAIL.
- Adiciona MaxRPU, uma nova configuração de controle de custos de computação para o Redshift Serverless. Com MaxRPU, você também pode especificar um limite de computação máximo para controlar custos de data warehouse em momentos diferentes selecionando o nível de computação máximo que o Redshift Serverless pode escalar por grupo de trabalho.
- Corrige a saída do literal INTERVAL com strings de intervalos numéricos. Por exemplo, um intervalo especificado como `INTERVAL '1' YEAR` agora retorna `1 YEAR`, em vez de `"00:00:00`. Além disso, a saída do literal INTERVAL é truncada no menor componente INTERVAL especificado. Por exemplo, `INTERVAL '1 day 1 hour 1 minute 1.123 seconds' HOUR TO MINUTE` é truncado em `1 day 01:01:00`.

# Patch 177 do Amazon Redshift

Versões de cluster neste patch:

- 1.0.57922 - Versão da faixa anterior – Lançada em 12 de outubro de 2023
- 1.0.57799 - Versão do Amazon Redshift sem servidor – Lançada em 10 de outubro de 2023
- 1.0.57798 - Versão da faixa atual – Lançada em 10 de outubro de 2023
- Versão de trilha atual: 1.0.57085 (lançada em 26 de setembro de 2023)
- Versão do Amazon Redshift sem servidor: 1.0.56899 (lançada em 21 de setembro de 2023)
- Versão de trilha atual: 1.0.56754 (lançada em 21 de setembro de 2023)

- Versão de trilha atual: 1.0.56242 (lançada em 11 de setembro de 2023)
- Versão do Amazon Redshift sem servidor: 1.0.55539 (lançada em 28 de agosto de 2023)
- Versão de trilha atual: 1.0.55524 (lançada em 28 de agosto de 2023)
- Versão de trilha atual: 1.0.54899 (lançada em 15 de agosto de 2023)
- Versão de trilha atual: 1.0.54899 (lançada em 14 de agosto de 2023)
- Versão de trilha atual: 1.0.54899 (lançada em 15 de agosto de 2023)
- Versão de trilha atual: 1.0.54239 (lançada em 3 de agosto de 2023)
- Versão do Amazon Redshift sem servidor: 1.0.54321 (lançada em 3 de agosto de 2023)

## Novos recursos e melhorias nesse patch

- Adiciona a visualização SYS_MV_STATE, que contém uma linha para cada transição de estado de uma visão materializada. SYS_MV_STATE pode ser usado para monitoramento de atualização de MV para instâncias provisionadas do Amazon Redshift sem servidor e do Amazon Redshift.
- Adiciona a visualização SYS_USERLOG, que registra detalhes das alterações em um usuário do banco de dados em “Criar usuário”, “Descartar usuário”, “Alterar usuário (renomear)”, “Alterar usuário (alterar propriedades)”.
- Adiciona a visualização SYS_COPY_REPLACEMENTS, a qual exibe um log que registra quando caracteres UTF-8 inválidos são substituídos pelo comando COPY com a opção ACCEPTINVCHARS.
- Adiciona a visualização SYS_SPATIAL_SIMPLIFY, que contém informações sobre objetos de geometria espacial simplificada usando o comando COPY.
- Adiciona a visualização SYS_VACUUM_HISTORY, que você pode usar para ver os detalhes e os resultados das operações VACUUM.
- Adiciona a visualização SYS_SCHEMA_QUOTA_VIOLATIONS para registrar a ocorrência, o carimbo de data/hora, XID e outras informações úteis quando uma cota de esquema é excedida.
- Adiciona a visualização SYS_RESTORE_STATE, que você pode usar para monitorar o progresso da redistribuição de cada tabela no cluster durante o redimensionamento clássico assíncrono.
- Adiciona a visualização SYS_EXTERNAL_QUERY_ERROR, que retorna informações sobre erros de verificação do Redshift Spectrum.
- Adiciona o parâmetro tag ao comando CREATE MODEL, para que agora você possa monitorar os custos de treinamento com os trabalhos de treinamento do piloto automático.
- Adiciona nomes de domínio personalizados (CNAME) para clusters do Amazon Redshift.

- Adiciona suporte de pré-visualização para o Apache Iceberg, permitindo que os clientes executem consultas analíticas nas tabelas do Apache Iceberg no Amazon Redshift.
- Adiciona suporte ao uso de perfis de usuário com grupos de parâmetros no gerenciamento da workload (WLM).
- Adiciona suporte para montagem automática de AWS Glue Data Catalog, possibilitando que os clientes executem consultas mais facilmente nos data lakes.
- Adiciona funcionalidade de forma que o uso de funções de agrupamento sem uma cláusula GROUP BY ou o uso de operações de agrupamento em uma cláusula WHERE resulte em um erro.
- Adiciona funcionalidade aos procedimentos armazenados para permitir a identificação de erros de divisão por zero e o tratamento dentro de um bloco de tratamento de exceções.
- Corrige um bug que impedia que as consultas usassem a escalabilidade simultânea para gravar dados em tabelas quando a tabela de origem era de compartilhamento de dados.
- Corrige o identificador que diferencia letras maiúsculas de minúsculas documentado em enable_case_sensitive_identifier para que agora funcione com instruções MERGE.
- Corrige o bug em que uma consulta na função pg_get_late_binding_view_cols () pode ser ignorada ocasionalmente. Agora você sempre pode cancelar essas consultas.
- Melhora a performance das consultas de compartilhamento de dados realizadas em consumidores quando são executados trabalhos de vacuum no produtor.
- Melhora a performance das consultas de compartilhamento de dados e escalabilidade simultânea, especialmente com alterações simultâneas de dados no produtor ou ao transferir para uma instância de escalabilidade simultânea conectada ao consumidor.

# Patch 176 do Amazon Redshift

Versões de cluster neste patch:

- Versão de trilha atual: 1.0.56738 (lançada em 21 de setembro de 2023)
- Versão de trilha atual: 1.0.55837 (lançada em 11 de setembro de 2023)
- Versão de trilha atual: 1.0.54776 (lançada em 15 de agosto de 2023)
- Versão de trilha atual: 1.0.54052 (lançada em 26 de julho de 2023)
- Versão do Amazon Redshift sem servidor: 1.0.53642 (lançada em 20 de julho de 2023)
- Versão de trilha atual: 1.0.53301 (lançada em 20 de julho de 2023)

- Versão do Amazon Redshift sem servidor: 1.0.52943 (lançada em 7 de julho de 2023)
- Versão de trilha atual: 1.0.52931 (lançada em 7 de julho de 2023)
- Versão do Amazon Redshift sem servidor: 1.0.52194 (lançada em 21 de junho de 2023)
- Versão de trilha atual: 1.0.51986 (lançada em 16 de junho de 2023)
- Versão de trilha atual: 1.0.51594 (lançada em 9 de junho de 2023)

## Novos recursos e melhorias nesse patch

- Tratamento aprimorado de erros ao escrever GROUP BY () para um conjunto de agrupamento vazio. Isso era ignorado anteriormente, mas agora retorna um erro do analisador.
- Melhorias de performance para atualização incremental das visões materializadas com colunas SUPER.
- ALTER TABLE <target_tbl> APPEND FROM <streaming_mv>: o comando SQL (ATA) agora comporta a transferência de todos os registros de uma visão materializada (MV) de streaming como origem, além das tabelas como origem, para uma tabela de destino. O suporte a ATA em MVs de streaming permite que os usuários eliminem rapidamente todos os registros em uma MV de streaming ao movê-los para outra tabela a fim de gerenciar o crescimento dos dados.
- TRUNCATE <streaming_mv>: o comando SQL agora comporta o truncamento de todos os registros em uma visão materializada (MV) de streaming, além das tabelas. TRUNCATE exclui todos os registros da MV de streaming, mantendo sua estrutura intacta. A execução de TRUNCATE em MVs de streaming permite que os clientes eliminem rapidamente todos os registros em uma MV de streaming para gerenciar o crescimento dos dados.
- Adicionada a funcionalidade da cláusula QUALIFY ao comando SELECT.
- Suporte a machine learning do Redshift para previsão de séries temporais por meio da integração com o Amazon Forecast.
- Suporte à montagem automática do AWS Glue Data Catalog para simplificar a consulta de um data lake sem etapas adicionais e criar referências a esquema externos.
- Agora é possível alterar políticas de RLS. Consulte a documentação para obter mais detalhes em ALTER RLS POLICY.
- As UDFs do Lambda agora são compatíveis com o parâmetro STABLE de volatilidade de funções na instrução CREATE FUNCTION. Quando o parâmetro STABLE é usado na instrução CREATE FUNCTION e a UDF do Lambda é chamada várias vezes e com os mesmos argumentos, o número esperado de invocações da função UDF do Lambda diminui. A categoria STABLE de volatilidade de funções está explicada em mais detalhes em Parâmetros de CREATE FUNCTION.

- Várias melhorias na performance de UDFs do Lambda. Especificamente, melhoria do suporte ao agrupamento de registros ao consultar uma tabela protegida por uma política de segurança por linha (RLS).
- Redução no tempo geral de criptografia dos clusters RA3 do Amazon Redshift e melhoria na disponibilidade do data warehouse durante a criptografia. Para obter mais informações, consulte Criptografia de bancos de dados no Amazon Redshift.
- Adição da nova visão do sistema SYS_MV_REFRESH_HISTORY ao Redshift. A visão SYS_MV_REFRESH_HISTORY contém uma linha para a atividade de atualização de visões materializadas. Usando SYS_MV_REFRESH_HISTORY, você pode verificar o histórico de atualização das visões materializadas. SYS_MV_REFRESH_HISTORY é visível para todos os usuários. Os superusuários podem ver todas as linhas; usuários regulares podem ver somente seus próprios dados.

  Uma nova coluna SPILLED_BLOCK_LOCAL_DISK foi adicionada à visão do sistema SYS_QUERY_DETAIL. A nova coluna SPILLED_BLOCK_LOCAL_DISK ajuda os clientes a determinar os blocos excedentes que são enviados ao disco local. Você pode usar SYS_QUERY_DETAIL para visualizar detalhes de consultas por etapa. SYS_QUERY_HISTORY é visível a todos os usuários. Os superusuários podem ver todas as linhas e os usuários comuns podem ver somente os metadados aos quais eles têm acesso.
- A nova visão do sistema SYS_QUERY_TEXT foi adicionada ao Amazon Redshift sem servidor e ao Amazon Redshift provisionado. A visão SYS_QUERY_TEXT é semelhante à SVL_STATEMENTTEXT para clusters provisionados. Use a coluna `sequence` na visão SYS_QUERY_TEXT para obter o texto completo da instrução SQL.

# Patch 175 do Amazon Redshift

Versões de cluster neste patch:

- Versão de trilha atual: 1.0.53064 (lançada em 7 de julho de 2023)
- Versão de trilha atual: 1.0.51973 (lançada em 16 de junho de 2023)
- Versão de trilha atual: 1.0.51781 (lançada em 10 de junho de 2023)
- Versão do Amazon Redshift sem servidor: 1.0.51314 (lançada em 3 de junho de 2023)
- Versão de trilha atual: 1.0.51304 (lançada em 2 de junho de 2023)
- Versão de trilha atual: 1.0.50708 (lançada em 19 de maio de 2023)
- Versão de trilha atual: 1.0.50300 (lançada em 8 de maio de 2023)

- Versão do Amazon Redshift sem servidor: 1.0.49710 (lançada em 28 de abril de 2023)
- Versão de trilha atual: 1.0.49676 (lançada em 28 de abril de 2023)

### Novos recursos e melhorias nesse patch

- Correções de erros secundárias.
- A ingestão de streaming do Amazon Redshift agora é compatível com a ingestão de streaming entre regiões, caso em que o tópico de origem do Amazon Kinesis Data Streams (KDS) ou Amazon Managed Streaming para Apache Kafka (MSK) pode estar localizado em uma região da AWS diferente da região em que o data warehouse do AWS Amazon Redshift está localizado. A documentação em Conceitos básicos da ingestão de streaming do Amazon Kinesis Data Streams foi revisada e explica como a palavra-chave REGION é usada.
- Ajuste do horário de verão do Egito.
- Tempos gerais aprimorados para criptografia de clusters RA3.

## Patch 174 do Amazon Redshift

### 1.0.51296 (lançada em 2 de junho de 2023)

Versão para a trilha anterior. Sem notas de release.

### 1.0.50468: lançamento em 12 de maio de 2023

Versão de manutenção. Sem notas de release.

### 1.0.49780, 1.0.49868 e 1.0.49997: lançamento em 28 de abril de 2023

Notas de release desta versão:

- Suporte em lote aprimorado para UDF do Lambda.
- Processamento em lote incremental para UDF do Lambda.
- Novo comando MERGE SQL para aplicar alterações nos dados de origem às tabelas do Amazon Redshift.
- Novo recurso dinâmico de mascaramento de dados para simplificar o processo de proteção de dados confidenciais em um data warehouse do Amazon Redshift.

- Novo controle de acesso centralizado para compartilhamento de dados com o Lake Formation que permite gerenciar concessões de permissões, visualizar controles de acesso e auditar permissões nas tabelas e visualizações nas unidades de compartilhamento de dados do Amazon Redshift usando as APIs do Lake Formation e o console da AWS.
- Ajuste do horário de verão do Egito.

## 1.0.49087: lançamento em 12 de abril de 2023

Versão de manutenção. Sem notas de release.

## 1.0.48805: lançamento em 5 de abril de 2023

Notas de release desta versão:

- O Amazon Redshift adicionou novos aprimoramentos de performance para consultas com muitas strings usando BYTEDICT, uma nova codificação de compactação no Amazon Redshift que acelera o processamento de dados baseado em strings de 5 a 63 vezes em comparação com codificações de compactação alternativas, como LZO ou ZSTD. Para obter mais informações sobre esse recurso, consulte Codificação do dicionário de bytes no Guia do desenvolvedor de banco de dados do Amazon Redshift.

## 1.0.48004: lançamento em 17 de março de 2023

Versão de manutenção. Sem notas de release.

## 1.0.47470: lançamento em 11 de março de 2023

Notas de release desta versão:

- Melhora a performance de consultas em `pg_catalog.svv_table_info`. Também adiciona a nova coluna `create_time`. Ao criar uma tabela, essa coluna armazena o carimbo de data/hora em UTC.
- Adiciona suporte à especificação de tempo limite por sessão na consulta federada.

# Patch 173 do Amazon Redshift

## 1.0.49788: lançamento em 28 de abril de 2023

Notas de release desta versão:

- Ajuste do horário de verão do Egito.

## 1.0.49074: lançamento em 12 de abril de 2023

Notas de release desta versão:

- Atualização da configuração de fuso horário para a versão 2022g da biblioteca IANA.

## 1.0.48766: lançamento em 5 de abril de 2023

Versão de manutenção. Sem notas de release.

## 1.0.48714: lançamento em 5 de abril de 2023

Versão de manutenção. Sem notas de release.

## 1.0.48022: lançamento em 17 de março de 2023

Versão de manutenção. Sem notas de release.

## 1.0.47357: lançamento em 7 de março de 2023

Versão de manutenção. Sem notas de release.

## 1.0.46987: lançado em 24 de fevereiro de 2023

Versão de manutenção. Sem notas de release.

## 1.0.46806: lançado em 18 de fevereiro de 2023

Versão de manutenção. Sem notas de release.

## 1.0.46607: lançado em 13 de fevereiro de 2023

Notas de release desta versão:

- agora, convertemos automaticamente tabelas com chaves de classificação intercaladas definidas manualmente em chaves de classificação compostas se o seu estilo de distribuição tiver sido definido como DISTSTYLE KEY, para melhorar o desempenho dessas tabelas. Isso é feito no momento da restauração de um snapshot no Amazon Redshift sem servidor.

## 1.0.45698: lançamento em 20 de janeiro de 2023

Notas de release desta versão:

- Adiciona um parâmetro de extensão de arquivo ao comando UNLOAD, para que extensões de arquivo sejam adicionadas automaticamente aos nomes dos arquivos.
- É compatível com a proteção de objetos protegidos por RLS por padrão ao adicioná-los a uma unidade de compartilhamento de dados ou se eles já fizerem parte de uma unidade de compartilhamento de dados. Agora, os administradores podem desativar o RLS para unidades de compartilhamento de dados para permitir que os consumidores acessem o objeto protegido.
- Adiciona novas tabelas de sistema para monitoramento: `SVV_ML_MODEL_INFO`, `SVV_MV_DEPENDENCY` e `SYS_LOAD_DETAIL`. Também adiciona as colunas `data_skewness` e `time_skewness` à tabela do sistema `SYS_QUERY_DETAIL`.

# Patch 172 do Amazon Redshift

Versões de cluster neste patch:

- 1.0.46534: lançado em 18 de fevereiro de 2023
- 1.0.46523: lançado em 13 de fevereiro de 2023
- 1.0.46206: lançado em 1º de fevereiro de 2023
- 1.0.45603: lançamento em 20 de janeiro de 2023
- 1.0.44924: lançado em 19 de dezembro de 2022
- 1.0.44903: lançado em 18 de dezembro de 2022
- 1.0.44540: lançado em 13 de dezembro de 2022
- 1.0.44126: lançado em 23 de novembro de 2022

- 1.0.43980: lançado em 17 de novembro de 2022

## Novos recursos e melhorias nesse patch

- As tabelas criadas por CTAS são AUTO por padrão.
- Adiciona suporte para segurança por linha (RLS) em visões materializadas.
- Aumenta o tempo limite do S3 para melhorar o compartilhamento de dados entre regiões.
- Adiciona a nova função espacial `ST_GeomFromGeohash`.
- Melhora a seleção automática da chave de distribuição a partir de chaves primárias compostas para melhorar a performance imediata.
- Adiciona uma chave primária automática à chave de distribuição para tabelas com chaves primárias compostas, melhorando a performance imediata.
- Melhora a escalabilidade da simultaneidade para permitir que mais consultas sejam escaladas mesmo quando os dados mudam.
- Melhora a performance de consultas de compartilhamento de dados.
- Adiciona métricas de probabilidade de Machine Learning para modelos de classificação.
- Adiciona novas tabelas de sistema para monitoramento: `SVV_USER_INFO`, `SVV_MV_INFO`, `SYS_CONNECTION_LOG`, `SYS_DATASHARE_USAGE_PRODUCER`, `SYS_DATASHARE_USAGE_CONSUMER` e `SYS_DATASHARE_CHANGE_LOG`.
- Adiciona compatibilidade para consultar colunas VARBYTE em tabelas externas para tipos de arquivo Parquet e ORC.

# Patch 171 do Amazon Redshift

Versões de cluster neste patch:

- 1.0.43931: lançado em 16 de novembro de 2022
- 1.0.43551: lançado em 5 de novembro de 2022
- 1.0.43331: lançado em 29 de setembro de 2022
- 1.0.43029: lançado em 26 de setembro de 2022

## Novos recursos e melhorias nesse patch

- Suporte a CONNECT BY: adiciona suporte à estrutura CONNECT BY SQL, permitindo que você consulte recursivamente os dados hierárquicos em seu data warehouse com base na relação pai-filho dentro desse conjunto de dados.

# Patch 170 do Amazon Redshift

Versões de cluster neste patch:

- 1.0.43922: lançado em 21 de novembro de 2022
- 1.0.43573: lançado em 7 de novembro de 2022
- 1.0.41881: lançado em 20 de setembro de 2022
- 1.0.41465: lançamento em 7 de setembro de 2022
- 1.0.40325: lançamento em 27 de julho de 2022

## Novos recursos e melhorias nesse patch

- ST_GeomfromGeoJSON: constrói um objeto de geometria espacial do Amazon Redshift com base em VARCHAR na representação GeoJSON.

# Patch 169 do Amazon Redshift

Versões de cluster neste patch:

- 1.0.41050: lançado em 7 de setembro de 2022
- 1.0.40083 - lançamento em 16 de julho de 2022
- 1.0.39734 - lançamento em 7 de julho de 2022
- 1.0.39380 - lançamento em 23 de junho de 2022
- 1.0.39251 - lançamento em 15 de junho de 2022
- 1.0.39009 - lançamento em 8 de junho de 2022

## Novos recursos e melhorias nesse patch

- Adiciona função como um parâmetro para o comando Alter Default Privileges para oferecer suporte ao Controle de Acesso Baseado em Função.
- Adiciona o parâmetro ACCEPTINVCHARS para oferecer suporte à substituição de caracteres UTF-8 inválidos ao copiar de arquivos Parquet e ORC.
- Adiciona a função OBJECT(k,v) para construir objetos SUPER a partir de pares de chave e valor.

# Patch 168 do Amazon Redshift

Versões de cluster neste patch:

- 1.0.38698: lançamento em 25 de maio de 2022
- 1.0.38551: lançamento em 20 de maio de 2022
- 1.0.38463: lançamento em 18 de maio de 2022
- 1.0.38361: lançamento em 13 de maio de 2022
- 1.0.38199 - lançamento em 9 de maio de 2022
- 1.0.38112: lançamento em 6 de maio de 2022
- 1.0.37684: lançamento em 20 de abril de 2022

## Novos recursos e melhorias nesse patch

- Compatibilidade adicionada para o tipo de modelo Linear Learner no ML do Amazon Redshift.
- Adição da opção SNAPSHOT para o nível de isolamento de transações SQL.
- Adição de `farmhashFingerprint64` como novo algoritmo de hash para dados `VARBYTE` e `VARCHAR`.
- Suporte para a função AVG na atualização incremental de visualizações materializadas.
- Suporte para subconsultas correlacionadas em tabelas externas no Redshift Spectrum.
- Para melhorar a performance da consulta pronta para uso, o Amazon Redshift escolhe automaticamente uma chave primária de coluna única para tabelas específicas como uma chave de distribuição.

# Exemplos de código para o Amazon Redshift usando SDKs da AWS

Os exemplos de código a seguir mostram como usar o Amazon Redshift com um kit de desenvolvimento de software (SDK) da AWS.

Ações são trechos de código de programas maiores e devem ser executadas em contexto. Embora as ações mostrem como chamar funções de serviço específicas, é possível ver as ações contextualizadas em seus devidos cenários e exemplos entre serviços.

Cenários são exemplos de código que mostram como realizar uma tarefa específica chamando várias funções dentro do mesmo serviço.

Exemplos entre serviços são amostras de aplicações que funcionam em vários Serviços da AWS.

Para obter uma lista completa dos Guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Conceitos básicos

## Olá, Amazon Redshift

O exemplo de código a seguir mostra como começar a usar o Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

```
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()));
    }
}
```

- Para obter detalhes da API, consulte describeClusters na Referência da API do AWS SDK for Java 2.x.

Exemplos de código

- Ações do Amazon Redshift usando AWS SDKs
  - Crie um cluster do Amazon Redshift usando um SDK da AWS
  - Criar um cluster do Amazon Redshift usando um SDK da AWS
  - Exclua um cluster do Amazon Redshift usando um SDK da AWS

- Descrever uma instrução de consulta do Amazon Redshift usando um SDK da AWS
- Descrever clusters usando um SDK da AWS
- Obter o resultado da instrução do Amazon Redshift usando um SDK da AWS
- Inserir dados em uma tabela do Amazon Redshift usando um SDK da AWS
- Modifique um cluster do Amazon Redshift usando um SDK da AWS
- Consultar uma tabela do Amazon Redshift usando um SDK da AWS

- Cenários do Amazon S3 usando SDKs da AWS
  - Conceitos básicos de tabelas, itens e consultas do Amazon Redshift
- Exemplos entre serviços do Amazon RDS usando SDKs da AWS
  - Criar um rastreador de itens do Amazon Redshift

# Ações do Amazon Redshift usando AWS SDKs

Os exemplos de código a seguir demonstram como realizar ações específicas do Amazon Redshift com SDKs da AWS. Esses trechos chamam a API do Amazon Redshift e são trechos de código de programas maiores que devem ser executados no contexto. Cada exemplo inclui um link para o GitHub, em que é possível encontrar instruções para configurar e executar o código.

Os exemplos a seguir incluem apenas as ações mais utilizadas. Para obter uma lista completa, consulte a Referência da API do Amazon Redshift.

Exemplos

- Crie um cluster do Amazon Redshift usando um SDK da AWS
- Criar um cluster do Amazon Redshift usando um SDK da AWS
- Exclua um cluster do Amazon Redshift usando um SDK da AWS
- Descrever uma instrução de consulta do Amazon Redshift usando um SDK da AWS
- Descrever clusters usando um SDK da AWS
- Obter o resultado da instrução do Amazon Redshift usando um SDK da AWS
- Inserir dados em uma tabela do Amazon Redshift usando um SDK da AWS
- Modifique um cluster do Amazon Redshift usando um SDK da AWS
- Consultar uma tabela do Amazon Redshift usando um SDK da AWS

# Crie um cluster do Amazon Redshift usando um SDK da AWS

O exemplo de código a seguir mostra como criar um cluster do Amazon Redshift.

CLI

AWS CLI

Criar um cluster com parâmetros mínimos Este exemplo cria um cluster com o conjunto mínimo de parâmetros. Por padrão, o formato da saída é JSON. Comando:

```
aws redshift create-cluster --node-type dw.hs1.xlarge --number-of-nodes 2 --
master-username adminuser --master-user-password TopSecret1 --cluster-identifier
 mycluster
```

Resultado:

```
{
   "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"
   }
}
```

- Para obter detalhes da API, consulte CreateCluster na Referência de comandos da AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

Crie o 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);
        }
    }
```

- Para obter detalhes da API, consulte CreateCluster na Referência da API do AWS SDK for Java 2.x.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e veja como configurar e executar no Repositório de exemplos de código da AWS.

Crie o cliente.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Crie o 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();
```

- Para obter detalhes da API, consulte CreateCluster na Referência da API do AWS SDK for JavaScript.

Kotlin

SDK for Kotlin

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

Crie o 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}")
    }
}
```

- Para obter detalhes da API, consulte CriarCluster na AWS Referência de API SDK para Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

## Criar um cluster do Amazon Redshift usando um SDK da AWS

O exemplo de código a seguir mostra como criar uma tabela do Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

```
    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);
        }
    }
```

- Para obter detalhes da API, consulte CreateTable na Referência da API do AWS SDK for Java 2.x.

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

## Exclua um cluster do Amazon Redshift usando um SDK da AWS

O exemplo de código a seguir mostra como excluir um cluster do Amazon Redshift.

CLI

AWS CLI

Excluir um cluster sem um snapshot final do cluster Este exemplo exclui um cluster, forçando a exclusão de dados, para que nenhum snapshot final do cluster seja criado. Comando:

```
aws redshift delete-cluster --cluster-identifier mycluster --skip-final-cluster-
snapshot
```

Excluir um cluster, permitindo a criação de um snapshot final do cluster Este exemplo exclui um cluster, mas especifica o snapshot final do cluster. Comando:

```
aws redshift delete-cluster --cluster-identifier mycluster --final-cluster-
snapshot-identifier myfinalsnapshot
```

- Para obter detalhes da API, consulte DeleteCluster na Referência de comandos da AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

Excluir o cluster.

```
   public static void deleteRedshiftCluster(RedshiftClient redshiftClient,
String clusterId) {
       try {
           DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
                   .clusterIdentifier(clusterId)
                   .skipFinalClusterSnapshot(true)
                   .build();

           DeleteClusterResponse response =
redshiftClient.deleteCluster(deleteClusterRequest);
           System.out.println("The status is " +
response.cluster().clusterStatus());

       } catch (RedshiftException e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Para obter detalhes da API, consulte DeleteCluster na Referência da API do AWS SDK for Java 2.x.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e veja como configurar e executar no Repositório de exemplos de código da AWS.

Crie o cliente.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Crie o 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();
```

- Para obter detalhes da API, consulte DeleteCluster na Referência da API do AWS SDK for JavaScript.

Kotlin

SDK for Kotlin

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

Excluir o cluster.

```
suspend fun deleteRedshiftCluster(clusterId: String?) {

    val request = DeleteClusterRequest {
        clusterIdentifier = clusterId
        skipFinalClusterSnapshot = true
    }

    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val response = redshiftClient.deleteCluster(request)
        println("The status is ${response.cluster?.clusterStatus}")
    }
}
```

- Para obter detalhes da API, consulte ExcluirCluster na AWS Referência da API SDK para Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

## Descrever uma instrução de consulta do Amazon Redshift usando um SDK da AWS

O exemplo de código a seguir mostra como descrever uma instrução de consulta do Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

```
   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);
        }
    }
```

- Para obter detalhes da API, consulte DescribeStatement na Referência da API do AWS SDK for Java 2.x.

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

## Descrever clusters usando um SDK da AWS

Os exemplos de código a seguir mostram como descrever clusters do Amazon Redshift.

CLI

AWS CLI

Obter uma descrição de todos os clusters Este exemplo retorna uma descrição de todos os clusters da conta. Por padrão, o formato da saída é JSON. Comando:

```
aws redshift describe-clusters
```

Resultado:

```
{
   "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"
   }
}
```

Você pode obter as mesmas informações em formato de texto com a opção `--output text`. Comando:

opção `--output text`. Comando:

opção. Comando:

```
aws redshift describe-clusters --output text
```

Resultado:

```
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
```

- Para obter detalhes da API, consulte DescribeClusters na Referência de comandos da AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

Descrever o 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);
        }
    }
```

- Para obter detalhes da API, consulte DescribeClusters na Referência da API do AWS SDK for Java 2.x.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e veja como configurar e executar no Repositório de exemplos de código da AWS.

Crie o cliente.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Descreva seus clusters.

```
// Import required AWS SDK clients and commands for Node.js
import { DescribeClustersCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "./libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new DescribeClustersCommand(params));
    console.log("Success", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Para obter detalhes da API, consulte DescribeClusters na Referência da API do AWS SDK for JavaScript.

Kotlin

SDK for Kotlin

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

Descrever o 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}")
            }
        }
    }
}
```

- Para obter detalhes da API, consulte DescreverClusters na AWS Referência da API SDK para Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

# Obter o resultado da instrução do Amazon Redshift usando um SDK da AWS

O exemplo de código a seguir mostra como obter o resultado da instrução.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

Verifique o resultado da instrução

```
   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);
       }
   }
```

- Para obter detalhes da API, consulte GetStatementResult na Referência da API do AWS SDK for Java 2.x.

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

## Inserir dados em uma tabela do Amazon Redshift usando um SDK da AWS

O exemplo de código a seguir mostra como inserir dados em uma tabela do Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

```
   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. ");
    }
```

- Para obter detalhes da API, consulte Insert, na Referência da API do AWS SDK for Java 2.x.

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

## Modifique um cluster do Amazon Redshift usando um SDK da AWS

Os exemplos de código a seguir mostram como modificar um cluster do Amazon Redshift.

CLI

AWS CLI

Associar um grupo de segurança a um cluster Este exemplo mostra como associar um grupo de segurança de cluster ao cluster especificado. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --cluster-security-
groups mysecuritygroup
```

Modificar a janela de manutenção de um cluster Este exemplo mostra como alterar a janela de manutenção semanal preferencial de um cluster para a janela de intervalo mínimo de quatro horas, começando aos domingos às 23h15 e terminando às segundas-feiras às 3h15. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --preferred-
maintenance-window Sun:23:15-Mon:03:15
```

Alterar a senha mestre do cluster Este exemplo mostra como alterar a senha mestre de um cluster. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --master-user-password
 A1b2c3d4
```

- Para obter detalhes da API, consulte ModifyCluster na Referência de comandos da AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

Modifique um 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);
       }
   }
```

- Para obter detalhes da API, consulte ModifyCluster na Referência da API do AWS SDK for Java 2.x.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e veja como configurar e executar no Repositório de exemplos de código da AWS.

Crie o cliente.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Modifique um 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();
```

- Para obter detalhes da API, consulte ModifyCluster na Referência da API do AWS SDK for JavaScript.

Kotlin

SDK for Kotlin

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

Modificar um 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")
    }
}
```

- Para obter detalhes da API, consulte ModificarCluster na AWS Referência da API SDK for Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

# Consultar uma tabela do Amazon Redshift usando um SDK da AWS

O exemplo de código a seguir mostra como consultar uma tabela do Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

Consulte uma tabela.

```
    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 "";
    }
```

- Para obter detalhes da API, consulte Query na Referência da API do AWS SDK for Java 2.x.

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

# Cenários do Amazon S3 usando SDKs da AWS

Os exemplos de código a seguir mostram como implementar cenários comuns no Amazon Redshift com SDKs da AWS. Esses cenários mostram como realizar tarefas específicas chamando várias funções no Amazon Redshift. Cada exemplo inclui um link para o GitHub, em que é possível encontrar instruções sobre como configurar e executar o código.

Exemplos

- Conceitos básicos de tabelas, itens e consultas do Amazon Redshift

## Conceitos básicos de tabelas, itens e consultas do Amazon Redshift

O exemplo de código a seguir mostra como trabalhar com tabelas, itens e consultas do Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

```
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);
        }
    }
}
```

- Para obter detalhes da API, consulte os tópicos a seguir na Referência da API do AWS SDK for Java 2.x.
  - createCluster
  - describeClusters
  - describeStatement
  - executeStatement
  - getStatementResult
  - listDatabasesPaginator
  - modifyCluster

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

# Exemplos entre serviços do Amazon RDS usando SDKs da AWS

Os exemplos de aplicações a seguir usam SDKs da AWS para associar o Amazon Redshift a outros Serviços da AWS. Cada exemplo inclui um link para o GitHub, em que é possível encontrar instruções sobre como configurar e executar a aplicação.

Exemplos

- Criar um rastreador de itens do Amazon Redshift

## Criar um rastreador de itens do Amazon Redshift

Os exemplos de código a seguir mostram como criar uma aplicação Web que rastreia e gera relatórios sobre itens de trabalho usando um banco de dados do Amazon Redshift.

Java

SDK para Java 2.x

Mostra como criar uma aplicação Web que rastreia e gera relatórios sobre itens de trabalho armazenados em um banco de dados do Amazon Redshift.

Para obter o código-fonte completo e instruções sobre como configurar a API Spring REST que consulta os dados do Amazon Redshift e para uso por uma aplicação React, consulte o exemplo completo no GitHub.

Serviços utilizados neste exemplo

- Amazon Redshift
- Amazon SES

Kotlin

SDK for Kotlin

Mostra como criar uma aplicação Web que rastreia e gera relatórios sobre itens de trabalho armazenados em um banco de dados do Amazon Redshift.

Para obter o código-fonte completo e instruções sobre como configurar a API Spring REST que consulta os dados do Amazon Redshift e para uso por uma aplicação React, consulte o exemplo completo no GitHub.

Serviços utilizados neste exemplo

- Amazon Redshift
- Amazon SES

Para obter uma lista completa dos Guias do desenvolvedor do AWS SDK e exemplos de código, consulte Usar este serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

# Histórico do documento

> **Note**
>
> Para ver uma descrição dos novos recursos no Amazon Redshift, consulte What's new.

A tabela a seguir descreve as alterações importantes do Guia de gerenciamento do Amazon Redshift após junho de 2018. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

Versão da API: 01/12/2012

Para obter uma lista das alterações feitas no Guia do desenvolvedor do banco de dados do Amazon Redshift, consulte Histórico do documento do guia do desenvolvedor do banco de dados do Amazon Redshift.

Para obter mais informações sobre os novos recursos, incluindo uma lista de correções e os números de versão do cluster associados a cada versão, consulte Histórico das versões de cluster.

| Alteração | Descrição | Data |
| --- | --- | --- |
| Atualizar as políticas gerenciadas do editor de consultas v2 | Atualizações das políticas gerenciadas `AmazonRedshiftQueryEditorV2FullAccess`, `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` e `AmazonRedshiftQueryEditorV2ReadWriteSharing` com as permissões `redshift-serverless:ListNamespaces` e `redshift-serverless:ListWorkgroups`. | 21 de fevereiro de 2024 |

| | | |
|---|---|---|
| Atualizar a política gerenciada de acesso somente leitura do Amazon Redshift | Atualizações na política gerenciada `AmazonRedshiftReadOnlyAccess` com permissão `redshift:ListRecommendations` para listar as recomendações do Amazon Redshift Advisor. | 7 de fevereiro de 2024 |
| Patch 180 do Amazon Redshift lançado. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre a versão, consulte Patch 180 do Amazon Redshift. | 29 de dezembro de 2023 |
| Patch 179 do Amazon Redshift lançado. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 179 do Amazon Redshift. | 9 de novembro de 2023 |

| | | |
|---|---|---|
| Atualizar políticas gerenciadas pelo Amazon Redshift | Atualizações feitas na política gerenciada por `AmazonRedshiftServiceLinkedRolePolicy` com permissões `ec2:AssignIpv6Addresses` e `ec2:UnassignIpv6Addresses` . | 31 de outubro de 2023 |
| Lançamento do patch 178 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 178. do Amazon Redshift. | 25 de setembro de 2023 |
| Atualizar as políticas gerenciadas do editor de consultas v2 | Atualizações das políticas gerenciadas `AmazonRedshiftQueryEditorV2NoSharing` , `AmazonRedshiftQueryEditorV2ReadSharing` e `AmazonRedshiftQueryEditorV2ReadWriteSharing` com as permissões `sqlworkbench:GetAutocompletionMetadata` e `sqlworkbench:GetAutocompletionResource` . | 16 de agosto de 2023 |

| | | |
|---|---|---|
| Atualizar a política gerenciada do Amazon Redshift | Atualizações feitas na política gerenciada por `AmazonRedshiftServiceLinkedRolePolicy` para conceder permissões em AWS Secrets Manager a fim de criar e gerenciar segredos de credencial do administrador. | 14 de agosto de 2023 |
| Lançamento do patch 177 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 177 do Amazon Redshift. | 3 de agosto de 2023 |
| Lançamento do patch 176 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 176 do Amazon Redshift. | 8 de junho de 2023 |

| | | |
|---|---|---|
| Lançamento do patch 175 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 175 do Amazon Redshift. | 28 de abril de 2023 |
| Atualizar a política gerenciada do Amazon Redshift | Atualizações na política gerenciada `AmazonRedshiftServiceLinkedRolePolicy` para remover permissões para ações relacionadas à rede ec2. Elas foram especificamente associadas à tag de recurso Purpose:RedshiftMigrateToVpc. | 27 de abril de 2023 |
| Atualizar a política gerenciada da API de dados do Amazon Redshift | Atualizações da política gerenciada `AmazonRedshiftDataFullAccess` com a permissão `redshift:GetClusterCredentialsWithIAM` . | 7 de abril de 2023 |

| | | |
|---|---|---|
| Atualizar as políticas gerenciadas do editor de consultas v2 | Atualizações das políticas gerenciadas `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` e `AmazonRedshiftQueryEditorV2ReadWriteSharing` com permissão `sqlworkbench:GetSchemaInference`. | 21 de março de 2023 |
| Lançamento do patch 174 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 174 do Amazon Redshift. | 11 de março de 2023 |
| Atualizar as políticas gerenciadas do editor de consultas v2 | Atualizações das políticas gerenciadas `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` e `AmazonRedshiftQueryEditorV2ReadWriteSharing` com permissão `sqlworkbench:AssociateNotebookWithTab`. | 2 de fevereiro de 2023 |

| | | |
|---|---|---|
| Lançamento do patch 173 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 173 do Amazon Redshift. | 20 de janeiro de 2023 |
| Lançamento do patch 172 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 172 do Amazon Redshift. | 17 de novembro de 2022 |
| Lançamento do patch 171 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 171 do Amazon Redshift. | 9 de novembro de 2022 |

| | | |
|---|---|---|
| Lançamento do patch 170 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 170 do Amazon Redshift. | 20 de julho de 2022 |
| Lançamento do patch 169 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 169 do Amazon Redshift. | 8 de junho de 2022 |
| Lançamento do patch 168 do Amazon Redshift. | Um novo patch do Amazon Redshift está sendo implantado. Demora várias semanas para uma nova versão se tornar disponível em todas as Regiões da AWS compatíveis com o Amazon Redshift. Para obter mais informações sobre essa versão, consulte Patch 168 do Amazon Redshift. | 19 de abril de 2022 |
| Compatibilidade de perfis de autenticação com drivers do Amazon Redshift | Agora é possível se conectar ao Amazon Redshift usando um perfil de autenticação. | 2 de agosto de 2021 |

| | | |
|---|---|---|
| Oferece suporte para endpoints entre VPCs para o Amazon Redshift com tecnologia AWS PrivateLink | Agora você pode usar endpoints da VPC gerenciados pelo Redshift no Amazon Redshift. | 1º de abril de 2021 |
| Oferece suporte para aprimoramentos do editor de consultas do Amazon Redshift | Agora você pode usar o editor de consultas com o roteamento aprimorado da VPC, tempos de execução de consultas mais longos e mais tipos de nós de cluster. | 17 de fevereiro de 2021 |
| Compatibilidade para a integração de console com parceiros | É possível integrar com parceiros usando o console do Amazon Redshift. | 9 de dezembro de 2020 |
| Compatibilidade para movimentação de clusters entre zonas de disponibilidade | Agora é possível mover clusters RA3 entre zonas de disponibilidade. | 9 de dezembro de 2020 |
| Compatibilidade com tipos de nó ra3.xlplus | Agora é possível criar tipos de nó ra3.xlplus. | 9 de dezembro de 2020 |
| Compatibilidade com driver JDBC versão 2.0 | Agora é possível configurar o driver JDBC versão 2.0. | 5 de novembro de 2020 |
| Compatibilidade com UDFs do Lambda e tokenização | Agora é possível gravar UDFs do Lambda para habilitar a tokenização externa de dados. | 26 de outubro de 2020 |
| Compatibilidade para programar a execução de uma instrução SQL | Agora é possível programar uma consulta no console do Amazon Redshift. | 22 de outubro de 2020 |

| | | |
|---|---|---|
| Compatibilidade com a API de dados do Amazon Redshift | Agora o Amazon Redshift pode ser acessado usando a API de dados integrada . Atualizações feitas na documentação incluem uma Referência da API de dados do Amazon Redshift. | 10 de setembro de 2020 |
| Compatibilidade com monitoramento de consultas do console do Amazon Redshift | O guia foi atualizado para descrever novos gráficos de monitoramento de consultas. | 7 de maio de 2020 |
| Suporte para limites de uso | Guia atualizado com a descrição dos limites de uso. | 23 de abril de 2020 |
| Autenticação multifator | O guia foi atualizado com a descrição da compatibilidade com a autenticação multifator. | 20 de abril de 2020 |
| O redimensionamento elástico agora aceita alterações no tipo de nó | Descrição atualizada do redimensionamento elástico. | 6 de abril de 2020 |
| Compatibilidade com tipos de nó ra3.4xlarge com armazenamento gerenciado | Guia atualizado para incluir tipos de nó ra3.4xlarge. | 2 de abril de 2020 |
| Compatibilidade para pausa e retomada | Atualização do guia de descrição das operações de pausa e retomada de clusters. | 11 de março de 2020 |
| Compatibilidade com o Microsoft Azure AD como provedor de identidades | Atualização do guia para descrever as etapas para usar o Microsoft Azure AD como um provedor de identidades. | 10 de fevereiro de 2020 |

| | | |
|---|---|---|
| Compatibilidade com o tipo de nó RA3 | O guia foi atualizado para descrever o novo tipo de nó RA3. | 3 de dezembro de 2019 |
| Compatibilidade com o novo console | Guia atualizado para descrever o novo console do Amazon Redshift. | 11 de novembro de 2019 |
| Atualizações nas informações de segurança | Atualizações na documentação das informações de segurança. | 24 de junho de 2019 |
| Aprimoramentos nos snapshots | O Amazon Redshift agora é compatível com vários aprimoramentos para gerenciar e programar snapshots. | 4 de abril de 2019 |
| Escalabilidade da simultaneidade | É possível configurar o gerenciamento do workload (WLM) para habilitar o modo de escalabilidade da simultaneidade. Para obter mais informações, consulte Configurar o gerenciamento do workload. | 21 de março de 2019 |
| Drivers JDBC e ODBC atualizados | O Amazon Redshift agora é compatível com novas versões dos drivers JDBC e ODBC. Para obter mais informações, consulte Configurar uma conexão JDBC e Configurar uma conexão ODBC. | 4 de fevereiro de 2019 |

| | | |
|---|---|---|
| Manutenção adiada | Se precisar reprogramar a janela de manutenção do cluster, você terá a opção de adiar a manutenção em até 14 dias. Se precisarmos atualizar o hardware ou fazer outras atualizações obrigatórias durante o período de adiamento, notificaremos você e faremos as alterações necessárias. O cluster não ficará disponível durante essas atualizações. Para obter mais informações, consulte Adiamento da manutenção. | 20 de novembro de 2018 |
| Notificação prévia | O Amazon Redshift fornece notificação antecipadamente para alguns eventos. Esses eventos têm uma categoria de evento de `pending`. Por exemplo, enviamos uma notificação prévia se uma atualização de hardware for necessária para um dos nós no cluster. Você pode assinar eventos pendentes da mesma forma que outros eventos do Amazon Redshift. Para obter mais informações, consulte Assinatura de notificações de eventos do Amazon Redshift. | 20 de novembro de 2018 |

| | | |
|---|---|---|
| Elastic resize (Redimensionamento elástico) | O redimensionamento elástico é o método mais rápido para redimensionar um cluster. O redimensionamento elástico adiciona ou remove nós em um cluster existente e depois redistribui automaticamente os dados para os novos nós. Como não cria um cluster, a operação de redimensionamento elástico é concluída de forma rápida, geralmente em alguns minutos. Para obter mais informações, consulte Redimensionar clusters. | 15 de novembro de 2018 |
| Novos drivers ODBC | Os drivers ODBC do Amazon Redshift foram atualizados para a versão 1.4.3.1000. Para obter mais informações, consulte Configuração de uma conexão ODBC. | 8 de novembro de 2018 |
| Cancelar operação de redimensionamento | Agora é possível cancelar uma operação de redimensionamento em andamento. Para obter mais informações, consulte Visão geral da operação de redimensionamento. | 2 de novembro de 2018 |

| | | |
|---|---|---|
| Modificar o cluster para alterar a criptografia | É possível modificar um cluster não criptografado para usar a criptografia do AWS Key Management Service (AWS KMS) usando uma chave gerenciada pela AWS ou uma chave gerenciada pelo cliente. Ao modificar o cluster para habilitar a criptografia KMS, o Amazon Redshift migra automaticamente os dados para um novo cluster criptografado. Você também pode migrar um cluster não criptografado para um cluster criptografado, modificando o cluster. | 16 de outubro de 2018 |
| O Amazon Redshift Spectrum é compatível com o roteamento aprimorado de VPC | Agora é possível usar o Redshift Spectrum com o roteamento aprimorado de VPC habilitado para o cluster. Pode ser necessário executar etapas de configuração adicionais. Para obter mais informações, consulte Usar o Amazon Redshift Spectrum com o roteamento avançado de VPC. | 10 de outubro de 2018 |
| Editor de consultas | Agora é possível executar consultas SQL no Console de Gerenciamento do Amazon Redshift. | 4 de outubro de 2018 |

| | | |
|---|---|---|
| Gráfico de análise de execução de workload | Agora, você pode obter uma visualização detalhada da performance de seu workload observando o gráfico de análise de execução do workload no console. Para obter mais informações, consulte Analisar a performance do workload. | 30 de julho de 2018 |
| Acompanhamentos de manutenção | Agora é possível determinar se o cluster será sempre atualizado para a versão mais recente do Amazon Redshift ou para uma versão anterior selecionando um acompanhamento de manutenção. Para obter mais informações, consulte Selecionar acompanhamentos de manutenção do cluster. | 26 de julho de 2018 |

A tabela a seguir descreve as alterações importantes no Guia de gerenciamento de clusters do Amazon Redshift antes de julho de 2018.

| Alteração | Descrição | Data de lançamento |
|---|---|---|
| Novas métricas do CloudWatch | Novas métricas de CloudWatch adicionadas para monitoramento de performance de consulta. Para obter mais informações, consulte Monitorar o Amazon Redshift usando métricas do CloudWatch | 17 de maio de 2018 |
| Criptografia de HSM | O Amazon Redshift é compatível apenas com o AWS CloudHSM para o gerenciamento de chave do módulo de segurança de hardware (HSM). Para obter mais | 6 de março de 2018 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| | informações, consulte Criptografia de banco de dados do Amazon Redshift. | |
| Encadeamento de funções do IAM | Se uma função do IAM anexada ao cluster não tiver acesso aos recursos necessários, você poderá encadear outra função, possivelmente pertencente a outra conta. O cluster assumirá a função encadeada temporariamente para acessar os dados. Você também pode conceder acesso entre contas com o encadeamento de funções. Cada função em cadeia assume a próxima função na cadeia, até que o cluster assuma a função no final da cadeia. Você pode encadear um máximo de 10 funções. Para obter mais informações, consulte Encadeando funções do IAM no Amazon Redshift. | 23 de fevereiro de 2018 |
| Novos tipos de nó DC2 | A nova geração de tipos de nó de computação densa (dense compute, DC) oferece performance muito melhor pelo mesmo preço do DC1. Para aproveitar as melhorias de performance, você pode migrar seu cluster DC1 para os tipos de nó DC2 mais novos. Para obter mais informações, consulte Clusters e nós no Amazon Redshift. | 17 de outubro de 2017 |
| Certificados ACM | O Amazon Redshift está substituindo os certificados SSL nos clusters pelos certificados emitidos pelo AWS Certificate Manager (ACM). O ACM é uma autoridad e de certificação pública confiável pela maioria dos sistemas atuais. Talvez seja necessário atualizar os certificados CA raiz confiáveis atuais para continuar se conectando aos clusters por meio de SSL. Para obter mais informações, consulte Transição para certifica dos ACM das conexões SSL. | 18 de setembro de 2017 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Perfis vinculados ao serviço | A função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao Amazon Redshift. As funções vinculadas ao serviço são predefinidas pelo Amazon Redshift e incluem todas as permissões exigidas pelo serviço para chamar os serviços da AWS em nome do cluster do Amazon Redshift. Para obter mais informações, consulte Uso de funções vinculadas ao serviço para o Amazon Redshift. | 18 de setembro de 2017 |
| Autenticação do usuário do banco de dados do IAM | Você pode configurar o sistema para permitir que os usuários criem credenciais de usuário e façam logon no banco de dados com base em suas credencia is do IAM. Você também pode configurar o sistema para permitir que os usuários façam logon usando autenticação única federada por meio de um provedor de identidades compatível com o SAML 2.0. Para obter mais informações, consulte Usar a autenticação do IAM para gerar credenciais do usuário do banco de dados. | 11 de agosto de 2017 |
| Restauração no nível da tabela oferece suporte ao roteamento aprimorado de VPC | Agora a restauração no nível da tabela é compatíve l em clusters que usem Enhanced VPC routing. Para obter mais informações, consulte Restaurar uma tabela de um snapshot. | 19 de julho de 2017 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Regras de monitoramento de consulta | Usando as regras de monitoramento de consulta do WLM, você pode definir limites de performance baseados em métricas para filas do WLM e especificar a ação a ser tomada quando uma consulta ultrapass ar esses limites — registrar, saltar ou anular. Você define regras de monitoramento de consultas como parte da configuração do Workload Management (WLM – Gerenciamento do workload). Para obter mais informações, consulte Configurar o gerenciamento do workload. | 21 de abril de 2017 |
| Enhanced VPC routing | Ao usar o roteamento aprimorado de VPC do Amazon Redshift, o Amazon Redshift força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados por meio da Amazon VPC. Para obter mais informações, consulte Roteamento aprimorado da VPC no Amazon Redshift. | 15 de setembro de 2016 |
| Novos campos de log de conexão | O log de auditoria Log de conexão tem dois campos novos para acompanhar conexões SSL. Se sempre carregar logs de auditoria em uma tabela do Amazon Redshift, você precisará adicionar as novas colunas a seguir à tabela de destino: sslcompression e sslexpansion. | 5 de maio de 2016 |
| Novos drivers ODBC | Os drivers ODBC do Amazon Redshift foram atualizad os para a versão 1.2.7.1007. Para obter mais informações, consulte Configurar uma conexão ODBC. | 30 de março de 2016 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Funções do IAM para COPY e UNLOAD | Agora é possível especificar uma ou mais funções do AWS Identity and Access Management (IAM) que o cluster pode usar na autenticação para acessar outros serviços da AWS. As funções do IAM oferecem uma alternativa mais segura para fornecer autentica ção com os comandos COPY, UNLOAD ou CREATE LIBRARY. Para obter mais informações, consulte Autorizar o Amazon Redshift a acessar outros serviços da AWS em seu nome e Autorizar operações COPY, UNLOAD, CREATE EXTERNAL FUNCTION e CREATE EXTERNAL SCHEMA usando funções do IAM. | 29 de março de 2016 |
| Restaurar da tabela | Você pode restaurar uma tabela de um snapshot de cluster para uma nova tabela em um cluster ativo. Para obter mais informações, consulte Restaurar uma tabela de um snapshot. | 10 de março de 2016 |
| Usar condição do IAM em políticas | Você pode restringir ainda mais o acesso a recursos usando o elemento Condition em políticas do IAM. Para obter mais informações, consulte Uso de condições de política do IAM para controle de acesso refinado. | 10 de dezembro de 2015 |
| Modificar acessível publicamente | Você pode modificar um cluster existente em uma VPC para alterar se isso é acessível publicamente. Para obter mais informações, consulte Modificar um cluster. | 20 de novembro de 2015 |
| Correções na documentação | Diversas correções na documentação publicadas. | 28 de agosto de 2015 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Atualização da documentação | Atualizada a orientação para solução de problemas sobre como definir configurações de rede para garantir que hosts com tamanhos de Maximum Transmiss ion Unit (MTU – Unidade de transmissão máxima) diferentes possam determinar o tamanho do pacote para uma conexão. Para obter mais informações, consulte As consultas parecem travar e, às vezes, não se comunicam com o cluster. | 25 de agosto de 2015 |
| Atualização da documentação | Revisada toda a seção sobre grupos de parâmetro s tendo em vista uma melhor organização e mais clareza. Para obter mais informações, consulte Grupos de parâmetros do Amazon Redshift. | 17 de agosto de 2015 |
| Propriedades dinâmicas do WLM | O parâmetro de configuração do WLM agora dá suporte à aplicação de algumas propriedades dinamicamente. Outras propriedades permanecem alterações estáticas e exigem que clusters associados sejam reiniciados, de maneira que as alterações feitas na configuração possam ser aplicadas. Para obter mais informações, consulte Propriedades dinâmicas e estáticas do WLM e Grupos de parâmetros do Amazon Redshift. | 3 de agosto de 2015 |
| Copiar clusters KMS criptogra fados para outra região da AWS | Adição de conteúdo sobre como configurar concessõe s de cópia do snapshot a fim de habilitar a cópia de clusters criptografados do AWS KMS para outra região da AWS. Para obter mais informações, consulte Copiar snapshots criptografados pelo AWS KMS para outra região da AWS. | 28 de julho de 2015 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Atualização da documentação | Atualização da seção de criptografia do banco de dados para explicar melhor como o Amazon Redshift usa o AWS KMS ou HSMs para gerenciar chaves e como o processo de criptografia funciona com cada uma dessas opções. Para obter mais informações, consulte Criptografia de banco de dados do Amazon Redshift. | 28 de julho de 2015 |
| Novo tipo de nó | O Amazon Redshift agora oferece um novo tipo de nó, DS2. Atualizadas referências de documentação para tipos de nó existentes a fim de usar novos nomes introduzidos nesta versão. Também revisada a seção para explicar melhor as combinações do tipo de nó e esclarecer limites de cota padrão. Para obter mais informações, consulte Clusters e nós no Amazon Redshift. | 9 de junho de 2015 |
| Ofertas de nó reservado | Adicionado conteúdo sobre novas ofertas de nó reservado. Também revisada a seção para explicar e comparar melhor as opções disponíveis e fornecidos exemplos para demonstrar como a definição de preço do nó reservado e sob demanda afeta a cobrança. Para obter mais informações, consulte Visão geral. | 9 de junho de 2015 |
| Novos drivers ODBC | O driver ODBC do Amazon Redshift foi atualizado. Adicionados uma seção para versões anteriores desses drivers e um link para notas de release dos drivers. Para obter mais informações, consulte Configurar uma conexão ODBC. | 5 de junho de 2015 |
| Correções na documentação | Diversas correções na documentação publicadas. | 30 de abril de 2015 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Novo recurso | Esta versão do Amazon Redshift apresenta novos drivers ODBC e JDBC otimizados para serem usados com o Amazon Redshift. Para obter mais informaçõ es, consulte Conectar-se a um data warehouse do Amazon Redshift usando ferramentas de cliente SQL. | 26 de fevereiro de 2015 |
| Novo recurso | Esta versão do Amazon Redshift apresenta métricas de performance do cluster que permitem exibir e analisar detalhes de execução da consulta. Para obter mais informações, consulte Visualizar consultas e cargas. | 26 de fevereiro de 2015 |
| Atualização da documentação | Adição de uma nova política de exemplo que demonstra como conceder permissão para ações de serviço da AWS comuns e recursos nos quais o Amazon Redshift confia. Para obter mais informações, consulte Exemplos de política gerenciada pelo cliente. | 16 de janeiro de 2015 |
| Atualização da documentação | Atualizada orientação sobre como definir a MTU para desativar quadros jumbo TCP/IP. Para obter mais informações, consulte Uso do EC2-VPC ao criar o cluster e As consultas parecem travar e, às vezes, não se comunicam com o cluster. | 16 de janeiro de 2015 |
| Atualização da documentação | Revisado o conteúdo sobre o parâmetro `wlm_json_configuration` e fornecida uma sintaxe de exemplo para configurar esse parâmetro usando a AWS CLI nos sistemas operacionais Linux, Mac OS X e Microsoft Windows. Para obter mais informações, consulte Configurar o gerenciamento do workload. | 13 de janeiro de 2015 |
| Atualização da documentação | Adicionadas notificações e descrições de evento não encontradas. Para obter mais informações, consulte Categorias de eventos e mensagens de eventos do Amazon Redshift. | 8 de janeiro de 2015 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Atualização da documentação | Atualização da orientação sobre políticas do IAM para ações e recursos do Amazon Redshift. Revisão da seção para melhorar a organização e a clareza. Para obter mais informações, consulte Segurança no Amazon Redshift. | 21 de novembro de 2014 |
| Novo recurso | Esta versão do Amazon Redshift introduz a capacidade de criptografar clusters usando chaves de criptografia do AWS Key Management Service (AWS KMS). O AWS KMS combina hardware e software seguros e altamente disponíveis para fornecer um sistema de gerenciamento de chaves escalado para a nuvem. Para obter mais informações sobre AWS KMS e opções de criptografia para o Amazon Redshift, consulte Criptografia de banco de dados do Amazon Redshift e Gerenciamento de clusters usando o console. | 12 de novembro de 2014 |
| Novo recurso | Esta versão do Amazon Redshift apresenta a capacidade de etiquetar recursos, como clusters e snapshots. As tags permitem fornecer metadados definidos pelo usuário para categorizar os relatórios de cobrança com base na alocação de custo, além de ajudar a identificar melhor recursos rapidamente. Para obter mais informações, consulte Marcação de recursos no Amazon Redshift. | 4 de novembro de 2014 |
| Novo recurso | Aumentado o limite máximo de nó para 128 nós de tamanhos de nó dw1.8xlarge e dw2.8xlarge. Para obter mais informações, consulte Clusters e nós no Amazon Redshift. | 30 de outubro de 2014 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Atualização da documentação | Adicionados links aos pacotes redistribuíveis do Microsoft Visual C++ 2010 necessários para o Amazon Redshift usar drivers ODBC do PostgreSQL. Para obter mais informações, consulte Instalar e configurar o driver ODBC do Amazon Redshift no Microsoft Windows. | 30 de outubro de 2014 |
| Novo recurso | Adição da capacidade de terminar consultas e cargas no console do Amazon Redshift. Para obter mais informações, consulte Visualizar consultas e cargas e Visualizar métricas do cluster durante as operações de carga. | 28 de outubro de 2014 |
| Correções na documentação | Diversas correções na documentação publicadas. | 17 de outubro de 2014 |
| Novo conteúdo | Adicionado conteúdo sobre como encerrar e excluir clusters. Para obter mais informações, consulte Desativação e exclusão de clusters e Excluir um cluster. | 14 de agosto de 2014 |
| Atualização da documentação | Esclarecido o comportamento da configuração Allow Version Upgrade para clusters. Para obter mais informações, consulte Visão geral do do Amazon Redshift. | 14 de agosto de 2014 |
| Atualização da documentação | Revisão dos procedimentos, capturas de tela e organização do tópico sobre como trabalhar com clusters no console do Amazon Redshift. Para obter mais informações, consulte Gerenciamento de clusters usando o console. | 11 de julho de 2014 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Novo conteúdo | Adição de um novo tutorial sobre como redimensionar clusters do Amazon Redshift, inclusive como redimensionar um cluster enquanto minimiza o valor de tempo em que o cluster permanece em modo somente leitura. Para obter mais informações, consulte Redimensionar clusters. | 27 de junho de 2014 |
| Novo recurso | Adicionada a possibilidade de renomear clusters. Para obter mais informações, consulte Renomeação de clusters e Modificar um cluster. | 2 de junho de 2014 |
| Atualização da documentação | Atualizado o exemplo de código do .NET para usar o provedor de dados ODBC durante a conexão com um cluster de maneira programática usando o .NET. Para ter mais informações, consulte Conectar-se ao data warehouse de forma programática. | 15 de maio de 2014 |
| Novo recurso | Foram adicionadas opções para selecionar um parameter group e um security group diferentes quando você restaurar um cluster de um snapshot. Para obter mais informações, consulte Restauração de um cluster usando um snapshot. | 12 de maio de 2014 |
| Novo recurso | Adição da nova seção para descrever como configurar um alarme do Amazon CloudWatch padrão para monitorar a porcentagem de espaço em disco usado em um cluster do Amazon Redshift. Esse alarme é uma nova opção no processo de criação do cluster. Para obter mais informações, consulte Alarme padrão de espaço em disco. | 28 de abril de 2014 |
| Atualização da documentação | Esclarecimento das informações sobre compatibilidade com o Elliptic curve Diffie—Hellman Exchange (ECDHE) no Amazon Redshift. Para obter mais informações, consulte Conexão usando SSL. | 22 de abril de 2014 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Novo recurso | Adição da afirmação sobre suporte do Amazon Redshift para o protocolo de acordo de chaves do Elliptic curve Diffie—Hellman (ECDH). Para obter mais informações, consulte Conexão usando SSL. | 18 de abril de 2014 |
| Atualização da documentação | Revisados e reorganizados os tópicos na seção Conectar-se a um data warehouse do Amazon Redshift usando ferramentas de cliente SQL. Adicionadas mais informações sobre conexões JDBC e ODBC, e uma nova seção para solução de problemas de conexão. | 15 de abril de 2014 |
| Atualização da documentação | Adicionada versão em exemplos de política do IAM em todo o guia. | 3 de abril de 2014 |
| Atualização da documentação | Adicionadas informações sobre como a definição de preço funciona quando você redimensiona um cluster. Para obter mais informações, consulte Comprar nós reservados do Amazon Redshift. | 2 de abril de 2014 |
| Novo recurso | Adicionada uma seção sobre um novo parâmetro , `max_cursor_result_set_size` , que define o tamanho máximo do conjunto de resultados, em megabytes, que pode ser armazenado por cursor individual. Esse valor de parâmetro também afeta o número de cursores ativos simultaneamente para o cluster. Para obter mais informações, consulte Grupos de parâmetros do Amazon Redshift. | 28 de março de 2014 |
| Novo recurso | Adicionada explicação sobre o campo Cluster Version agora incluindo a versão do mecanismo do cluster e o número de revisão do banco de dados. Para obter mais informações, consulte Clusters provisionados do Amazon Redshift. | 21 de março de 2014 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Novo recurso | Atualizado o procedimento de redimensionamento para mostrar as novas informações de andamento do redimensionamento na guia Status do cluster. Para obter mais informações, consulte Redimensionamento de um cluster. | 21 de março de 2014 |
| Atualização da documentação | Reorganizado e atualizado O que é o Amazon Redshift? e revisado Visão geral dos clusters provisionados do Amazon Redshift. Diversas correções na documentação publicadas. | 21 de fevereiro de 2014 |
| Novo recurso | Adição dos novos tipos de nó e tamanhos de clusters do Amazon Redshift, além de nova redação do respectivo tópico de visão geral do cluster, tendo em vista uma melhor organização e mais clareza nos comentários. Para obter mais informações, consulte Clusters provisionados do Amazon Redshift. | 23 de janeiro de 2014 |
| Novo recurso | Adição de informações sobre endereços IP elásticos (EIP) de clusters do Amazon Redshift acessíveis publicamente em nuvens privadas virtuais. Para obter mais informações sobre EIP no Amazon Redshift, consulte Gerenciamento de clusters em uma VPC e Criar um cluster em uma VPC. | 20 de dezembro de 2013 |
| Novo recurso | Adição de informações sobre os registros do AWS CloudTrail do Amazon Redshift. Para obter mais informações a compatibilidade do Amazon Redshift com o CloudTrail, consulte Registrar em log com o CloudTrail. | 13 de dezembro de 2013 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Novo recurso | Adição de informações sobre o novo registro de atividade do usuário e o parâmetro do banco de dados do `enable_user_activity_logging` para o recurso de registro em log de auditoria do banco de dados no Amazon Redshift. Para obter mais informaçõ es sobre o registro em log de auditoria do banco de dados, consulte Registro em log da auditoria de banco de dados. Para obter mais informações sobre parâmetros de banco de dados, consulte Grupos de parâmetros do Amazon Redshift. | 6 de dezembro de 2013 |
| Novo recurso | Atualização para descrever como configurar o Amazon Redshift para copiar automaticamente snapshots automatizados e manuais para uma região secundári a da AWS. Para obter mais informações sobre como configurar uma cópia do snapshot em várias regiões, consulte Copiar snapshots para outra região da AWS. | 14 de novembro de 2013 |
| Novo recurso | Adição de seção para descrever o registro em log de auditoria do Amazon Redshift para conexão e atividade do usuário e armazenar esses logs no Amazon S3. Para obter mais informações sobre o registro em log de auditoria do banco de dados, consulte Registro em log da auditoria de banco de dados. | 11 de novembro de 2013 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Novo recurso | Adição de seção para descrever a criptografia do Amazon Redshift com novos recursos para gerenciar chaves de criptografia em um módulo de segurança de hardware (HSM) e em chaves de criptografia alternáveis. Para obter mais informações sobre criptografia, HSM e rodízio de chaves, consulte Criptografia de banco de dados do Amazon Redshift, Criptografia para Amazon Redshift usando módulos de segurança de hardware e Alternância de chave de criptografia no Amazon Redshift. | 11 de novembro de 2013 |
| Novo recurso | Atualização para descrever como publicar notificações de eventos do Amazon Redshift usando o Amazon SNS. Para obter mais informações sobre notificações de evento do Amazon Redshift, consulte Notificações de eventos do Amazon Redshift. | 11 de novembro de 2013 |
| Novo recurso | Atualização para descrever permissões no nível de recurso do IAM. Para obter mais informações sobre as permissões IAM do Amazon Redshift, consulte Segurança no Amazon Redshift. | 9 de agosto de 2013 |
| Novo recurso | Atualizado para descrever métricas de progresso da restauração. Para obter mais informações, consulte Restauração de um cluster usando um snapshot. | 9 de agosto de 2013 |
| Novo recurso | Atualizado para descrever as métricas de compartil hamento de snapshot do cluster e criar métricas de andamento do snapshot. Para obter mais informações, consulte Compartilhar snapshots. | 17 de julho de 2013 |
| Correções na documentação | Diversas correções na documentação publicadas. | 8 de julho de 2013 |

| Alteração | Descrição | Data de lançamento |
| --- | --- | --- |
| Novas telas de console | Atualização do Guia de gerenciamento de clusters do Amazon Redshift para comparar alterações no console do Amazon Redshift. | 22 de abril de 2013 |
| Novo guia | Esta é a primeira versão do Guia de gerenciamento do Amazon Redshift. | 14 de fevereiro de 2013 |