Amazon Redshift

集群管理指南

Amazon Redshift: 集群管理指南

Copyright © 2022 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其它商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅中国的 Amazon Web Services 服务入门。

Table of Contents

什么是 Amazon Redshift？ 1
Amazon Redshift Serverless 1
您是首次接触 Amazon Redshift 用户吗？ 1
Amazon Redshift 管理概览 1
集群管理 2
集群访问和安全性 2
监控集群 3
数据库 3
Amazon Redshift Serverless 功能概览 4
将 Amazon Redshift Serverless 与 Amazon Redshift 预调配数据仓库进行比较 5
Amazon Redshift Serverless 15
什么是 Amazon Redshift Serverless？ 15
Amazon Redshift Serverless 控制台 16
Amazon Redshift Serverless 的计算容量 17
了解 Amazon Redshift Serverless 容量 17
Amazon Redshift Serverless 的计费 18
了解 Amazon Redshift Serverless 计费 18
连接到 Amazon Redshift Serverless 20
连接到 Amazon Redshift Serverless 20
通过 JDBC 驱动程序连接到 Amazon Redshift Serverless 21
使用数据 API 连接到 Amazon Redshift Serverless 21
使用 SSL 连接到 Amazon Redshift Serverless 22
从 Amazon Redshift 托管式 VPC 端点连接到 Amazon Redshift Serverless 22
创建可公开访问的 Amazon Redshift Serverless 实例并连接到该实例 23
Amazon Redshift Serverless 中的安全性和连接 23
Amazon Redshift Serverless 中的 Identity and Access Management 24
将预置集群迁移到 Amazon Redshift Serverless 25
创建预置集群的快照 25
使用驱动程序端点 26
使用 Amazon Redshift Serverless SDK 27
Amazon Redshift Serverless 工作组和命名空间概览 27
Amazon Redshift Serverless 工作组和命名空间概览 27
通过控制台开始使用 Amazon Redshift Serverless 29
首次设置 Amazon Redshift Serverless 29
配置 Amazon Redshift Serverless 29
使用控制面板检查 Amazon Redshift Serverless 29
搜索工作组 30
创建带有伴随命名空间的工作组 30
使用控制台配置工作组 31
管理使用限制 31
管理查询限制 32
使用控制台删除工作组 32
搜索命名空间 33
配置命名空间 33
编辑安全性和加密 33
删除命名空间 34
更改命名空间的 Amazon KMS 密钥 34
使用 Amazon Redshift Serverless 监控查询和工作负载 35
使用 Amazon Redshift Serverless 监控查询和工作负载 35
Amazon Redshift Serverless 事件通知 38
使用 Amazon EventBridge 发送事件通知 38
管理 Amazon Redshift Serverless 告警 40
Amazon Redshift Serverless 的审计日志记录 40
导出日志 40

使用快照和恢复点 44
使用快照和恢复点 44
Amazon Redshift Serverless 中的数据共享 47
Amazon Redshift Serverless 中的数据共享 47
为资源添加标签 48
为资源添加标签概览 48
使用 Amazon Redshift Serverless 时的注意事项 49
集群 50
Amazon Redshift 集群概览 50
集群和节点 50
在创建集群时使用 EC2-VPC 54
EC2-VPC 54
EC2-Classic 54
启动集群 54
RA3 节点类型概述 55
使用 Amazon Redshift 托管存储 55
管理 RA3 节点类型 56
Amazon 区域中的 RA3 节点类型可用性 56
升级到 RA3 节点类型 57
在弹性调整大小或快照恢复期间将 DS2 保留节点升级为 RA3 保留节点 58
从 DC1 节点类型升级到 DC2 节点类型 59
将 EC2-Classic 上的 DS2 集群升级为 EC2-VPC 60
区域和可用区注意事项 60
集群维护 60
维护时段 61
推迟维护 62
选择集群维护跟踪 62
管理集群版本 63
回滚集群版本 63
确定集群维护版本 63
默认磁盘空间警报 64
集群状态 64
管理集群的概述 65
调整集群大小 65
暂停和恢复集群 73
重命名集群 74
关闭和删除集群 74
使用 AQUA 74
什么时候使用 AQUA？ 75
管理使用限制 77
管理集群重新定位 78
启用集群重新定位 79
限制 79
使用控制台管理重新定位 79
使用 Amazon Redshift CLI 管理重新定位 80
使用 Redshift 托管的 VPC 终端节点 81
注意事项 81
使用 Redshift 控制台进行管理 82
使用 Amazon CLI 进行管理 83
使用 Amazon Redshift API 操作进行管理 83
使用控制台管理集群 83
创建集群 84
修改集群 86
删除集群 86
重新引导集群 87
调整集群大小 87
升级集群的发行版本 88

获取有关集群配置的信息 88
获取集群状态概述 88
创建集群快照 88
创建或编辑磁盘空间警报 89
使用集群性能数据 89
使用 Amazon CLI 和 Amazon Redshift API 管理集群 89
使用 Amazon SDK for Java 管理集群 90
在 VPC 中管理集群 92
概览 92
在 VPC 中创建集群 93
管理集群的 VPC 安全组 94
集群子网组 95
集群版本历史记录 98
查询数据库 100
使用 Amazon Redshift 查询编辑器 v2 查询数据库 100
配置您的 Amazon Web Services 账户 101
使用查询编辑器 v2 106
编写和运行查询 115
查询数据湖 118
使用数据共享 121
可视化结果 123
以团队形式协作和共享 127
使用查询编辑器查询数据库 128
注意事项 129
启用访问 129
使用查询编辑器进行连接 130
使用查询编辑器 131
计划查询 132
使用 SQL 客户端工具连接到集群 135
在 Amazon Redshift 中配置连接 136
配置连接的安全选项 217
通过客户端工具和代码连接到集群 221
解决 Amazon Redshift 中的连接问题 263
使用 Data API 267
使用数据 API 268
调用数据 API 时的注意事项 268
授予访问权限 270
调用 Data API 273
解决 Data API 问题 289
使用 Amazon EventBridge 计划数据 API 操作 290
监控数据 API 290
增强型 VPC 路由 293
使用 VPC 终端节点 294
启用增强型 VPC 路由 294
将 Amazon Redshift Spectrum 与增强型 VPC 路由一起使用 295
在 Redshift Spectrum 中使用增强型 VPC 路由的注意事项 295
参数组 299
概览 299
关于参数组 299
默认参数值 299
使用 Amazon CLI 配置参数值 300
配置工作负载管理 301
WLM 动态和静态属性 301
wlm_json_configuration 参数的属性 302
使用 Amazon CLI 配置 wlm_json_configuration 参数 305
使用控制台管理参数组 310
创建参数组 310

修改参数组 ... 310
使用控制台创建或修改查询监控规则 ... 312
删除参数组 ... 313
将参数组与集群相关联 ... 313
使用 Amazon SDK for Java 管理参数组 ... 313
使用 Amazon CLI 和 Amazon Redshift API 管理参数组 ... 317
快照 ... 318
概览 ... 318
自动快照 ... 318
自动快照计划 ... 319
快照计划格式 ... 319
手动快照 ... 320
管理快照存储 ... 321
从快照中排除表 ... 321
将快照复制到另一个 Amazon 区域 ... 321
从快照还原集群 ... 322
从快照中还原表 ... 324
共享快照 ... 325
使用控制台管理快照 ... 326
创建快照计划 ... 327
创建手动快照 ... 327
更改手动快照保留期 ... 327
删除手动快照 ... 327
复制自动快照 ... 328
从快照还原集群 ... 328
从快照还原无服务器命名空间 ... 328
共享集群快照 ... 329
为未加密的集群配置跨区域快照复制 ... 330
为 Amazon KMS 加密的集群配置跨区域快照复制 ... 330
修改跨区域快照复制的保留期 ... 331
使用 Amazon SDK for Java 管理快照 ... 331
使用 Amazon CLI 和 Amazon Redshift API 管理快照 ... 334
将 Amazon 合作伙伴集成 ... 335
使用 Amazon Redshift 控制台与 Amazon 合作伙伴集成 ... 335
购买预留节点 ... 337
概览 ... 337
关于预留节点产品 ... 337
比较不同预留节点产品的定价 ... 337
预留节点的工作方式 ... 338
预留节点和整合账单 ... 338
预留节点示例 ... 339
使用控制台购买预留节点产品 ... 340
使用 Amazon CLI 升级预留节点 ... 340
使用 Java 购买预留节点产品 ... 341
使用 Amazon CLI 和 Amazon Redshift API 购买预留节点产品 ... 344
安全性 ... 345
数据保护 ... 346
数据加密 ... 346
数据令牌化 ... 355
互联网络流量隐私 ... 355
身份和访问管理 ... 356
使用身份进行身份验证 ... 356
访问控制 ... 358
有关管理访问的概述 ... 358
使用基于身份的策略（IAM policy） ... 363
Amazon Redshift 的原生身份提供者 (IdP) 联合身份验证 ... 386
Amazon Redshift API 权限参考 ... 389

使用服务相关角色 389
使用 IAM 身份验证生成数据库用户凭证 393
授权 Amazon Redshift 访问 Amazon 服务 425
日志记录和监控 443
数据库审计日志记录 443
使用 Cloudtrail 进行日志记录 450
合规性验证 456
故障恢复能力 457
基础设施安全性 457
网络隔离 355
安全组 458
使用接口 VPC 终端节点连接 458
配置和漏洞分析 461
使用 Amazon Redshift 管理界面 463
使用 Amazon SDK for Java 463
使用 Eclipse 运行 Java 示例 464
从命令行中运行 Java 示例 464
设置终端节点 465
对 HTTP 请求进行签名 465
示例签名计算 466
设置 Amazon Redshift CLI 467
安装说明 467
Amazon Command Line Interface入门 468
监控 集群性能 472
概览 472
性能数据 472
Amazon Redshift 指标 473
Amazon Redshift 指标的维度 478
Amazon Redshift 查询和加载性能数据 479
使用性能数据 480
查看集群性能数据 480
查看查询历史记录 486
查看数据库性能数据 489
查看工作负载并发和并发扩展数据 492
查看查询和加载 494
在加载操作期间查看集群指标 498
分析工作负载性能 498
管理警报 499
在 CloudWatch 控制台中使用性能指标 500
事件 501
Overview 501
使用控制台查看事件 501
使用 Amazon SDK for Java 查看事件 501
使用 Amazon CLI 和 Amazon Redshift API 查看事件 503
事件通知 503
概览 503
Amazon Redshift 事件类别和事件消息 505
使用 Amazon Redshift 控制台管理事件通知 512
使用 Amazon CLI 和 Amazon Redshift API 管理事件通知 513
配额和限制 514
Amazon Redshift 对象的配额 514
Amazon Redshift Serverless 对象的配额 517
查询编辑器 v2 对象的配额 517
Amazon Redshift Spectrum 对象的配额和限制 518
命名约束 518
Tagging 520
标记概述 520

标记要求 520
使用控制台管理资源标签 521
使用 Amazon Redshift API 管理标签 521
集群版本 523
补丁 170 523
新功能 523
补丁 169 523
新功能 523
补丁 168 524
新功能 524
文档历史记录 525

什么是 Amazon Redshift？

欢迎使用 Amazon Redshift 集群管理指南。Amazon Redshift 是一种完全托管的 PB 级云中数据仓库服务。开始时，您可以只使用几百 GB 数据，然后扩展至 1 PB 或更多。这样，您可以使用数据获得对您的业务和客户的新洞察。

创建数据仓库的第一步是启动一组节点（称为 Amazon Redshift 集群）。预置集群后，您可以上传数据集，然后执行数据分析查询。无论数据集的大小如何，Amazon Redshift 都使用您目前所用的基于 SQL 的相同工具和业务情报应用程序，来提供快速的查询性能。

Amazon Redshift Serverless

Amazon Redshift Serverless 通过简单的配置和管理提供数据仓库容量和智能扩展。您无需设置预调配的数据仓库即可访问和分析数据。有关更多信息，请参阅什么是 Amazon Redshift Serverless？。

您是首次接触 Amazon Redshift 用户吗？

如果您是首次接触 Amazon Redshift 的用户，我们建议您先阅读以下部分：

- Amazon Redshift 管理概览 (p. 1) – 本主题简要介绍 Amazon Redshift。
- 服务亮点和定价 – 该产品详细信息页面提供 Amazon Redshift 价值主张、服务亮点和定价。
- Amazon Redshift 入门指南 – 本指南引导您完成创建集群、创建数据库表、上载数据和测试查询的过程。
- Amazon Redshift 集群管理指南（本指南）— 本指南向您展示如何创建和管理 Amazon Redshift 集群。
- Amazon Redshift 数据库开发人员指南 – 如果您是数据库开发人员，则本指南说明如何设计、构建、查询和维护构成数据仓库的数据库。

可通过多种方式管理集群。如果您首选更具交互性的方式来管理集群，则可以使用 Amazon Redshift 控制台或 Amazon Command Line Interface (Amazon CLI)。如果您是应用程序开发人员，可以使用 Amazon Redshift 查询 API 或 Amazon 软件开发工具包 (SDK) 库以编程方式管理集群。如果您使用 Amazon Redshift 查询 API，则必须通过对发送到 API 的每个 HTTP 或 HTTPS 请求进行签名来执行身份验证。有关对请求签名的更多信息，请转到对 HTTP 请求进行签名 (p. 465)。

有关 CLI、API 和 SDK 的信息，请转到以下链接：

- Amazon CLI 命令引用
- Amazon Redshift API 参考
- 适用于 Amazon Web Services 的工具中的开发工具包参考。

Amazon Redshift 管理概览

Amazon Redshift 服务管理数据仓库的所有设置、操作和扩展工作。这些任务包括：预置容量，监控和备份集群，以及向 Amazon Redshift 引擎应用修补程序和升级。

集群管理

Amazon Redshift 集群是一组节点，其中包含一个领导节点以及一个或多个计算节点。所需计算节点的类型和数量取决于数据的大小、将运行的查询数以及所需的查询执行性能。

创建和管理集群

根据数据仓库需要，开始时您可以使用一个小的单节点集群，然后随着您的需求变化轻松地扩展为更大的多节点集群。您可以在集群中添加或删除计算节点，而不会出现任何服务中断。有关更多信息，请参阅Amazon Redshift 集群 (p. 50)。

预留计算节点

如果您打算让集群保持运行一年或更长时间，则可以将计算节点保留一年或三年的时间，从而节省成本。与您按需预置计算节点时支付的小时费率相比，保留计算节点可大大地节省成本。有关更多信息，请参阅购买 Amazon Redshift 预留节点 (p. 337)。

创建集群快照

快照是集群的时间点备份。存在两种类型的快照：自动和手动。Amazon Redshift 通过使用加密的安全套接字层 (SSL) 连接，在 Amazon Simple Storage Service（Amazon S3）内部存储这些快照。如果您需要从快照还原，Amazon Redshift 会创建一个新集群并从您指定的快照导入数据。有关 快照的更多信息，请参阅 Amazon Redshift 快照 (p. 318)。

集群访问和安全性

Amazon Redshift 中有几项与集群访问和安全相关的功能。这些功能可帮助您控制对集群的访问，定义连接规则，以及对数据和连接进行加密。这些功能是除 Amazon Redshift 中与数据库访问和安全相关的功能之外的功能。有关数据库安全的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的管理数据库安全。

Amazon 账户和 IAM 凭证

预设情况下，只有创建集群的 Amazon 账户才能访问 Amazon Redshift 集群。该集群被锁定，这样其他任何人都不能访问它。在 Amazon 账户内，您可以使用 Amazon Identity and Access Management (IAM) 服务创建用户账户和管理这些账户的权限以控制集群操作。有关更多信息，请参阅Amazon Redshift 中的安全性 (p. 345)。

安全组

预设情况下，您创建的任何集群都对所有人关闭。IAM 凭证仅控制对 Amazon Redshift API 相关资源的访问：Amazon Redshift 控制台、命令行界面 (CLI)、API 和开发工具包。要能够通过 JDBC 或 ODBC 从 SQL 客户端工具访问集群，您可以使用安全组：

- 如果您使用 EC2-VPC 平台访问 Amazon Redshift 集群，则必须使用 VPC 安全组。我们建议您在 EC2-VPC 平台中启动集群。

  使用 EC2-Classic 启动集群后，无法将其移动到 VPC。不过，您可以使用 Amazon Redshift 控制台将 EC2-Classic 快照还原到 EC2-VPC 集群。有关更多信息，请参阅从快照还原集群 (p. 328)。
- 如果您使用 EC2-Classic 平台访问 Amazon Redshift 集群，则必须使用 Amazon Redshift 安全组。

在上述任一情况下，您可以向安全组中添加规则，以授予对特定 CIDR/IP 地址范围或 Amazon Elastic Compute Cloud (Amazon EC2) 安全组（如果 SQL 客户端运行在 Amazon EC2 实例上）的显式入站访问权限。有关更多信息，请参阅Amazon Redshift 集群安全组 (p. 458)。

除入站访问规则之外，您还可以创建数据库用户以提供凭证向集群自身内的数据库进行身份验证。有关更多信息，请参阅本主题中的数据库 (p. 3)。

加密

当您预置集群时，可以选择对集群进行加密以提高安全性。启用加密时，Amazon Redshift 会将所有数据以加密格式存储在用户创建的表中。使用 Amazon Key Management Service (Amazon KMS) 来管理 Amazon Redshift 的加密密钥。

加密是集群的不可变属性。从加密集群切换到非加密集群的唯一方式是：卸载数据并将其重新加载到新集群。加密会应用于集群和所有备份。从加密快照还原集群时，新集群也会加密。

有关加密、密钥和硬件安全模块的更多信息，请参阅 Amazon Redshift 数据库加密 (p. 347)。

SSL 连接

您可以使用安全套接字层 (SSL) 加密对 SQL 客户端和集群之间的连接进行加密。有关更多信息，请参阅配置连接的安全选项 (p. 217)。

监控集群

Amazon Redshift 中有几项与监控相关的功能。您可以使用数据库审计日志记录来生成活动日志，配置事件和通知订阅来跟踪感兴趣的信息。使用 Amazon Redshift 和 Amazon CloudWatch 中的指标，了解集群和数据库的运行状况及性能。

数据库审核日志记录

您可以使用数据库审计日志记录功能来跟踪有关身份验证尝试次数、连接数、断开连接数、数据库用户定义更改以及数据库中运行的查询的信息。这些信息对 Amazon Redshift 中的安全和故障排除非常有用。日志存储在 Simple Storage Service（Amazon S3）存储桶中。有关更多信息，请参阅数据库审计日志记录 (p. 443)。

事件和通知

Amazon Redshift 跟踪事件并在您的 Amazon 账户中将事件的相关信息保留几周。对于每个事件，Amazon Redshift 会报告事件发生日期、描述、事件源（例如，集群、参数组或快照）和源 ID 等信息。您可以创建 Amazon Redshift 事件通知订阅以指定一组事件筛选器。当发生与筛选条件匹配的事件时，Amazon Redshift 将使用 Amazon Simple Notification Service 主动通知您发生了该事件。有关事件和通知的更多信息，请参阅 Amazon Redshift 事件 (p. 501)。

性能

Amazon Redshift 提供性能指标和数据，以便您可以跟踪集群和数据库的运行状况及性能。Amazon Redshift 使用 Amazon CloudWatch 指标监控集群的物理方面，例如 CPU 使用率、延迟和吞吐量。Amazon Redshift 还提供查询和加载性能数据，以帮助您监控集群中的数据库活动。有关性能指标和监控的更多信息，请参阅监控 Amazon Redshift 集群性能 (p. 472)。

数据库

当您预置集群时，Amazon Redshift 会创建一个数据库。这是您用于加载数据并对数据运行查询的数据库。您可以根据需要通过运行 SQL 命令来创建其他数据库。有关创建其他数据库的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的步骤 1：创建数据库。

当您预置集群时，可以指定一个管理员用户，此管理员用户可以访问在该集群内创建的所有数据库。此管理员用户是最初唯一可以访问数据库的超级用户，此用户也可以创建其它超级用户和用户。有关更多信息，请转至 Amazon Redshift 数据库开发人员指南中的超级用户和用户。

Amazon Redshift 使用参数组定义集群中所有数据库的行为，例如，日期表示样式和浮点精度。如果您在预置集群时未指定参数组，则 Amazon Redshift 会将一个默认参数组与集群相关联。有关更多信息，请参阅Amazon Redshift 参数组 (p. 299)。

有关 Amazon Redshift 中的数据库的更多信息，请转至 Amazon Redshift 数据库开发人员指南。

Amazon Redshift Serverless 功能概览

Amazon Redshift Serverless 也支持 Amazon Redshift 预调配数据仓库所支持的大多数功能。以下是它的一些关键功能。

功能	描述
快照	您可以将 Amazon Redshift Serverless 或预调配数据仓库的快照还原到 Amazon Redshift Serverless。有关更多信息，请参阅使用快照和恢复点 (p. 44)。
恢复点	Amazon Redshift Serverless 每 30 分钟自动创建一个恢复点。这些恢复点将保留 24 个小时。在意外写入或删除之后，您可以使用它们进行还原。从恢复点还原时，Amazon Redshift Serverless 数据库中的所有数据都将还原到较早的时间点。如果需要将恢复点保留较长时间，也可以从恢复点创建快照。有关更多信息，请参阅使用快照和恢复点 (p. 44)。
基本 RPU 容量	您能够以 Redshift 处理单元（RPU）为单位设置基本容量。一个 RPU 提供 16 GB 内存。此设置使您能够控制正在使用的资源与工作负载成本之间的平衡。您可以增加此值以增加可用资源并提高查询性能，或者降低此值以限制您的支出。原定设置为 128 个 RRU。您还可以设置使用量限制（例如，每天使用的 RPU）来控制成本。有关更多信息，请参阅Amazon Redshift Serverless 的计费 (p. 18)。
数据共享的使用限制	您可以使用控制台或 API，限制从生产者区域向使用者区域传输的数据量。这些数据传输成本因 Amazon Web Services 区域而不同，以 TB 为单位测量。有关数据共享的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》https://docs.amazonaws.cn/redshift/latest/dg/getting-started-datashare-console.html中的使用控制台实现数据共享入门。
用户定义的函数（UDF）	您可以在 Amazon Redshift Serverless 中运行用户定义的函数（UDF）。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的创建用户定义的函数。
存储过程	您可以在 Amazon Redshift Serverless 中运行存储过程。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的创建存储过程。
实体化视图	您可以在 Amazon Redshift Serverless 中创建实体化视图。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的创建具体化视图。
空间函数	您可以在 Amazon Redshift Serverless 中运行空间函数。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的查询空间数据。
联合查询	您可以运行查询，以将数据与 Amazon Redshift Serverless 中的 Aurora 和 Amazon RDS 数据库连接起来。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的通过联合查询来查询数据。
数据湖查询	您可以运行查询，以将 Amazon S3 数据湖中的数据与 Amazon Redshift Serverless 连接起来。有关更多信息，请参阅《Amazon Redshift 集群管理指南》中的查询数据湖。
HyperLogLog	您可以在 Amazon Redshift Serverless 中运行 HyperLogLog 函数。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的使用 HyperlogLog 草图。
跨数据库查询数据	您可以通过 Amazon Redshift Serverless 跨数据库查询数据。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的跨数据库查询数据。
数据共享	您可以使用 Amazon Redshift Serverless 访问预调配数据仓库上的数据共享。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的跨集群共享数据。

功能	描述
半结构化数据查询	您可以通过 Amazon Redshift Serverless 上的 SUPER 数据类型来摄取和存储半结构化数据。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的摄取和查询半结构化数据。
为资源添加标签	您可以使用 Amazon CLI 或 Amazon Redshift Serverless API，通过与资源相关的元数据来给资源添加标签。有关更多信息，请参阅标记资源。
机器学习	您可以将 Amazon Redshift 机器学习与 Amazon Redshift Serverless 结合使用。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的使用机器学习。
SQL 命令和函数	除了一些例外情况（例如 REBOOT_CLUSTER），您可以将 Amazon Redshift SQL 命令和函数与 Amazon Redshift Serverless 结合使用。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 SQL 参考。
CloudFormation 资源	使用 CloudFormation 模板，您可以部署和更新 Amazon Redshift Serverless 资源。这种集成意味着您可以花更少的时间管理资源，从而将精力集中在应用程序上。有关 Amazon Redshift Serverless 中的 CloudFormation 资源的更多信息，请参阅 Amazon Redshift Serverless resource type reference（Amazon Redshift Serverless 资源类型参考）。
CloudTrail 资源	Amazon Redshift Serverless 与 Amazon CloudTrail 集成，以便提供在 Amazon Redshift Serverless 中执行的操作的记录。CloudTrail 将 Amazon Redshift Serverless 的所有 API 调用作为事件捕获。有关更多信息，请参阅 CloudTrail for Amazon Redshift Serverless。

将 Amazon Redshift Serverless 与 Amazon Redshift 预调配数据仓库进行比较

对于 Amazon Redshift Serverless 来说，一些概念和功能与 Amazon Redshift 预调配数据仓库的相应功能不同。例如，一个截然不同的比较是 Amazon Redshift Serverless 没有集群或节点的概念。下表介绍 Amazon Redshift Serverless 中的功能和行为，并解释了它们与预调配数据仓库中的等效功能有何不同。

功能	描述	Serverless (无服务器)	已预置
工作组和命名空间	要在 Amazon Redshift Serverless 中隔离工作负载并管理不同的资源，您可以创建命名空间和工作组，以便分别管理存储资源和计算资源。	命名空间是数据库对象和用户的集合。工作组是计算资源的集合。有关更多信息，请参阅 Amazon Redshift Serverless (p. 15) 以了解 Amazon Redshift Serverless 的设计。	预调配集群是计算节点和领导节点的集合，您可以直接管理这些节点。有关更多信息，请参阅Amazon Redshift 集群 (p. 50)。

功能	描述	Serverless (无服务器)	已预置
节点类型	当您使用 Amazon Redshift Serverless 时，您不会像对待预调配的 Amazon Redshift 集群那样选择节点类型或指定节点计数。	Amazon Redshift Serverless 会自动为您预置和管理容量。您可以选择指定基本数据仓库容量，以便为您的工作负载选择合适的性价比平衡。您还可以指定最大 RPU 小时数来设置成本控制，以确保成本是可预测的。有关更多信息，请参阅了解 Amazon Redshift Serverless 容量 (p. 17)。	您可以使用符合成本和性能规格的节点类型构建集群。有关更多信息，请参阅Amazon Redshift 集群 (p. 50)。
工作负载管理和并发扩展	Amazon Redshift 可以在高负载时段进行扩展。Amazon Redshift Serverless 还可以进行扩展，以应对间歇性的高负载时段。	Amazon Redshift Serverless 自动、高效地管理资源，并根据工作负载在成本控制的阈值范围内进行扩缩。有关更多信息，请参阅计算容量的计费 (p. 18)。	使用预调配数据仓库，您可以在集群上启用并发扩展以应对高负载时段。有关更多信息，请参阅并发扩展。

功能	描述	Serverless (无服务器)	已预置
端口	用于连接的端口号。	使用 Amazon Redshift Serverless，您的端口 5439 为静态的。有关更多信息，请参阅连接到 Amazon Redshift Serverless (p. 20)。	使用预调配数据仓库，您可以选择任何端口进行连接。
调整大小	添加或删除计算资源以更好地应对工作负载。	调整大小在 Amazon Redshift Serverless 中不适用。但是，您可以根据价格和性能要求更改基本数据仓库 RPU 容量。有关更多信息，请参阅了解 Amazon Redshift Serverless 容量 (p. 17)。	对于预调配集群，您可以执行集群调整大小以添加节点或删除节点。有关更多信息，请参阅在 Amazon Redshift 中管理集群的概览。
暂停和恢复	在没有工作负载要运行时，可以暂停预调配集群，以节省成本。	使用 Amazon Redshift Serverless，您只需在查询运行时付费，因此无需暂停或恢复。有关更多信息，请参阅计算容量的计费 (p. 18)。	您可以在不同时间根据对工作负载的评估，手动暂停和恢复集群。有关更多信息，请参阅在 Amazon Redshift 中管理集群的概览。

功能	描述	Serverless (无服务器)	已预置
使用 Spectrum 查询以查询外部数据	您可以在 Amazon S3 桶中查询各种格式（例如 JSON）的数据。	当计算资源处理工作负载时，账单会累积。此外，与任何其他事务一样，在查询外部 Redshift Spectrum 数据时，账单也将累积。有关更多信息，请参阅计算容量的计费 (p. 18)。	对于预调配数据仓库，Amazon Redshift Spectrum 容量存在于从 Amazon Redshift 集群查询的单独服务器上。有关更多信息，请参阅使用 Amazon Redshift Spectrum 查询外部数据。
计算资源账单	Amazon Redshift 与 Amazon Redshift Serverless 的账单是如何累积的。	使用 Amazon Redshift Serverless，您按秒支付以 RPU 小时为单位运行的工作负载，最低收费时间为 60 秒。这包括在 Amazon S3 中以开放文件格式访问数据的查询。有关更多信息，请参阅计算容量的计费 (p. 18)。	对于预调配集群，当集群未暂停时，将按秒计费。
维护时段	服务器维护的工作原理。	对于 Amazon Redshift Serverless，没有维护时段。可以无缝地处理更新。有关更多信息，请参阅什么是 Amazon Redshift Serverless？	对于预调配集群，您可以指定进行修补时的维护时段。（通常，当使用率较低时，您可以选择一个重复时间。）

功能	描述	Serverless (无服务器)	已预置
加密	您可以启用数据库加密。	Amazon Redshift Serverless 始终使用 Amazon KMS、Amazon 托管式或客户托管式密钥进行加密。	可以使用 Amazon KMS（Amazon 托管式或客户托管式密钥）对预调配数据仓库中的数据进行加密，或进行解密。请参阅Amazon Redshift 数据库加密 (p. 347)。
存储计费	存储计费的工作原理。	适用于 Amazon Redshift Serverless。费率按每月 GB 计算。请参阅计算容量的计费 (p. 18)。	对于具有 RA3 节点的预调配集群，存储与计算资源分开计费。
用户管理	如何管理用户。	对于预调配数据仓库和 Amazon Redshift Serverless 这两者，用户是 IAM 或 Redshift 用户。有关更多信息，请参阅Amazon Redshift Serverless 中的安全性和连接 (p. 23)。	

功能	描述	Serverless (无服务器)	已预置
JDBC 和 ODBC 工具和兼容性	客户端连接的工作原理。	预调配数据仓库和 Amazon Redshift Serverless 都与任何符合 JDBC 或 ODBC 标准的工具或客户端应用程序兼容。有关驱动程序的更多信息，请参阅《Amazon Redshift 集群管理指南》中的配置连接。有关连接到 Amazon Redshift Serverless 的信息，请参阅配置连接。	
登录时的凭证要求	如何处理凭证。	对于 Amazon Redshift Serverless，您不必在每个实例中输入凭证。有关更多信息，请参阅连接到 Amazon Redshift Serverless (p. 20)。	访问 Amazon Redshift 需要对预调配数据仓库具有特定权限的 IAM 用户提供的用户名和密码凭证。（您还可以将用户与 IAM 角色关联。）经过身份验证后，用户可以无缝连接到数据库、Redshift 控制台和查询编辑器 v2。

功能	描述	Serverless (无服务器)	已预置
数据 API	您可以访问来自 Web 服务和其他应用程序的数据。	Amazon Redshift Serverless 支持 Amazon Redshift 数据 API。对于 Amazon Redshift Serverless，您使用 `workgroup-name` 参数，而不是 `cluster-identity` 参数。有关调用数据 API 的更多信息，请参阅使用 Amazon Redshift 数据 API (p. 267)。	
快照	提供时间点恢复。	Amazon Redshift Serverless 支持快照和恢复点。有关命名空间的快照和恢复点的更多信息，请参阅使用快照和恢复点 (p. 44)。	预调配集群支持快照。有关更多信息，请参阅使用控制台管理快照。

功能	描述	Serverless (无服务器)	已预置
数据共享	提供在同一个账户或不同账户中的数据库之间共享数据的功能。	Amazon Redshift Serverless 支持预调配数据仓库所能实现的所有数据共享功能，还支持在 Amazon Redshift Serverless 与预调配数据仓库、工具或客户端应用程序之间共享数据。	预调配集群支持跨数据库、跨账户、跨区域和 Amazon Web Services Data Exchange 数据共享。有关更多信息，请参阅在 Amazon Redshift 中跨集群共享数据。
跟踪	提供软件更新的时间表。	Amazon Redshift Serverless 没有跟踪的概念。版本和更新由服务处理。有关 Amazon Redshift Serverless 的设计的更多信息，请参阅使用快照和恢复点 (p. 44)。	预调配集群支持在当前跟踪和尾随跟踪之间切换。
系统表和视图	提供一种监控您的资源和系统元数据的方法。	Amazon Redshift Serverless 支持新的系统表和视图。有关系统表的更多信息，请参阅监控视图 (p. 36)。	预调配数据仓库支持一组现有的系统表和视图，它们用于进行监控和其他需要系统元数据的任务。

功能	描述	Serverless (无服务器)	已预置
参数组	这是一组适用于在集群中创建的所有数据库的参数。这些参数可用于配置数据库设置，例如查询超时和日期样式。	Amazon Redshift Serverless 没有参数组的概念。	预调配数据仓库支持参数组。有关预置集群的参数组的更多信息，请参阅 Amazon Redshift 参数组 (p. 299)。
查询监控	提供基于时间的查询运行视图。	Amazon Redshift Serverless 中的查询监控要求用户连接到数据库以使用系统表。因此，查询监控和系统表是同步的。对 Amazon Redshift Serverless 中系统表的查询使用映射到 IAM 用户的数据库用户，以便使用查询监控。有关监控查询的更多信息，请参阅使用 Amazon Redshift Serverless 监控查询和工作负载。	预调配集群中的查询监控不会显示系统表中的所有数据。

功能	描述	Serverless (无服务器)	已预置
审计日志记录	提供有关数据库中的连接和用户活动的信息。	使用 Amazon Redshift Serverless，CloudWatch 是审计日志的目标。Amazon Redshift Serverless 不支持基于 Amazon S3 的审计日志交付。有关更多信息，请参阅 Amazon Redshift Serverless 的审计日志记录。	对于预调配集群，基于 Amazon S3 的审计日志交付一直是常态。现在，向 CloudWatch 交付审计日志的范围也扩展到包括预调配数据仓库。
事件通知	Amazon EventBridge 是一种无服务器事件总线服务，让您可以轻松地将应用程序与来自各种源的事件数据相连接。	Amazon Redshift Serverless 使用 Amazon EventBridge 管理事件通知，以便随时了解数据仓库中的更改。有关更多信息，请参阅 Amazon Redshift Serverless 事件通知。	对于预调配集群，可以使用 Amazon Redshift 控制台创建事件订阅来管理事件通知。有关更多信息，请参阅使用 Amazon Redshift 控制台管理事件通知。

Amazon Redshift Serverless

借助 Amazon Redshift Serverless，无需预调配和管理数据仓库，即可方便地运行和扩展分析。借助 Amazon Redshift Serverless，数据分析人员、开发人员和数据科学家现在通过将数据加载到数据仓库中并查询数据仓库中的记录，就可以使用 Amazon Redshift 在几秒钟内从数据中获取洞察。Amazon Redshift 会自动预置和扩展数据仓库容量，以便为要求苛刻且不可预测的工作负载提供快速性能。您仅需为实际使用的容量付费。您无需更改现有分析和商业智能应用程序，即可受益于这种简单性。

主题

- 什么是 Amazon Redshift Serverless？ (p. 15)
- Amazon Redshift Serverless 的计算容量 (p. 17)
- Amazon Redshift Serverless 的计费 (p. 18)
- 连接到 Amazon Redshift Serverless (p. 20)
- Amazon Redshift Serverless 中的安全性和连接 (p. 23)
- 将预置集群迁移到 Amazon Redshift Serverless (p. 25)
- Amazon Redshift Serverless 工作组和命名空间概览 (p. 27)
- 通过控制台开始使用 Amazon Redshift Serverless (p. 29)
- 使用 Amazon Redshift Serverless 监控查询和工作负载 (p. 35)
- Amazon Redshift Serverless 事件通知 (p. 38)
- 管理 Amazon Redshift Serverless 告警 (p. 40)
- Amazon Redshift Serverless 的审计日志记录 (p. 40)
- 使用快照和恢复点 (p. 44)
- Amazon Redshift Serverless 中的数据共享 (p. 47)
- 为资源添加标签 (p. 48)
- 使用 Amazon Redshift Serverless 时的注意事项 (p. 49)

什么是 Amazon Redshift Serverless？

Amazon Redshift Serverless 会自动预置数据仓库容量并智能扩展基础资源。Amazon Redshift Serverless 可在几秒钟内调整容量，以便为要求最苛刻和急剧波动的工作负载提供始终如一的高性能和简化的操作。

使用 Amazon Redshift Serverless，您可从以下功能中受益：

- 无需设置、优化和管理 Amazon Redshift 预置集群即可访问和分析数据。
- 使用卓越的 Amazon Redshift SQL 功能、行业领先的性能和数据湖集成，以跨数据仓库、数据湖和操作数据源进行无缝查询。
- 通过智能和自动扩缩，即使是最苛刻和急剧波动的工作负载，也能提供始终如一的高性能和简化操作。
- 使用工作组和命名空间，通过精细的成本控制来组织计算资源和数据。
- 仅在使用数据仓库时付费。

借助 Amazon Redshift Serverless，您可以使用控制台界面访问无服务器数据仓库或 API 以构建应用程序。通过数据仓库，您可访问 Amazon Redshift 托管存储和 Simple Storage Service（Amazon S3）数据湖。

本视频向您展示 Amazon Redshift Serverless 如何轻松运行和扩展分析，而无需管理数据仓库基础设施：

Amazon Redshift Serverless 控制台

在 Serverless dashboard（无服务器控制面板）页面中，您可查看资源摘要和使用情况图表。

- Namespace overview（命名空间概览）– 本部分显示命名空间内的快照和数据共享的数量。
- Workgroups（工作组）– 本部分显示 Amazon Redshift Serverless 中的所有工作组。
- Queries metrics（查询指标）– 本部分显示过去一小时的查询活动。
- RPU capacity used（已使用的 RPU 容量）– 本部分显示过去一小时内使用的容量。
- Free trial（免费试用）– 本部分显示您 Amazon 账户中的剩余免费试用积分。这涵盖了同一账户下所有对 Amazon Redshift Serverless 资源和操作的使用，包括快照、存储、工作组等。
- Alarms（告警）– 本节显示您在 Amazon Redshift Serverless 中配置的告警。

您可以在 Data backup（数据备份）选项卡上使用以下选项：

- Snapshots（快照）– 您可以创建、删除和管理 Amazon Redshift Serverless 数据的快照。原定设置的保留期为 `indefinitely`，但您可以将保留期配置为 1 到 3653 天之间的任意值。您可以授权 Amazon Web Services 账户从快照还原命名空间。
- Recovery points（恢复点）– 显示自动创建的恢复点，以便可以还原过去 24 小时内的意外写入或删除。要恢复数据，您可以将恢复点还原到任何可用的命名空间。如果想要将恢复点保留更长时间段，则可以从恢复点创建快照。原定设置的保留期为 `indefinitely`，但您可以将保留期配置为 1 到 3653 天之间的任意值。

您可在 Data access（数据访问）选项卡上使用以下选项：

- Network and security（网络和安全性）设置 – 您可以查看与 VPC 相关的值，Amazon KMS 加密值和审计日志记录值。您只能更新审计日志记录。有关使用控制台设置网络和安全性设置的更多信息，请参阅配置 Amazon Redshift Serverless (p. 29)。
- Amazon KMS key — 用于加密 Amazon Redshift Serverless 中资源的 Amazon KMS key。
- Permissions（权限）– 您可以管理 IAM 角色，Amazon Redshift Serverless 可担任此角色以代表您来使用资源。有关更多信息，请参阅Amazon Redshift Serverless 中的 Identity and Access Management (p. 24)。
- Redshift-managed VPC endpoints（Redshift 托管式 VPC 端点）– 您可从另一个 VPC 或子网访问 Amazon Redshift Serverless 实例。有关更多信息，请参阅从 Redshift 托管式 VPC 端点连接到 Amazon Redshift Serverless (p. 22)。

在 Limits（限制）选项卡上，您可以使用以下选项：

- Base capacity in Redshift processing units (RPUs)（以 Redshift 处理单元 (RPU) 计算的基本容量）设置 – 您可以设置用于处理工作负载的基本容量。要改善查询性能，请增加 RPU 值。
- Usage limits（使用限制）– 在启动操作之前的一段时间内，Amazon Redshift Serverless 实例可以使用的最大计算资源。您可限制 Amazon Redshift Serverless 用于运行工作负载的资源量。使用情况以 Redshift 处理单元 (RPU) 小时为单位衡量。RPU 小时是一小时内使用的 RPU 数量。您可以确定达到您设置的阈值时的操作，如下所示：
  - 发送提示。
  - 将条目记录到系统表中。
  - 禁用用户查询。
- Query limits（查询限制）–在 Amazon Redshift Serverless 停止查询之前，查询运行的最长时间。

有关更多信息，请参阅了解 Amazon Redshift Serverless 容量 (p. 17)。

在 Datashares（数据共享）选项卡上，可以使用以下选项：

- Datashares created in my namespace（在我的命名空间中创建的数据共享）设置 – 您可以创建数据共享并与其它命名空间和 Amazon Web Services 账户 共享。
- Datashares from other namespaces and Amazon Web Services 账户（来自其他命名空间和 Amazon Web Services 账户 数据共享）– 您可以从来自其他命名空间和 Amazon Web Services 账户的数据共享创建数据库。

有关数据共享的更多信息，请参阅Amazon Redshift Serverless 中的数据共享 (p. 47)。

在 Query and database monitoring（查询和数据库监控）页面上，您可以查看您的 Query history（查询历史记录）和 Database performance（数据库性能）图表。您可以根据多个维度筛选数据。

在 Query history（查询历史记录）选项卡上，您会看到以下图表 [您可以在 Query list（查询列表）和 Resource metrics（资源指标）之间进行选择]：

- Query runtime（查询运行时间）– 此图表显示哪些查询在同一时间范围内运行。在图表中选择栏以查看更多查询执行详细信息。
- Queries and loads（查询和加载）– 本部分列出了按 Query ID（查询 ID）进行的查询和加载。
- RPU capacity used（已使用的 RPU 容量）– 此图表显示了以 Redshift 处理单元 (RPU) 表示的总容量。
- Database connections（数据库连接数）– 此图表显示了活动的数据库连接数。

在 Database performance（数据库性能）选项卡上，您会看到以下图表：

- Queries completed per second（每秒完成的查询数）– 此图表显示了每秒完成的平均查询数。
- Query duration（查询持续时间）– 此图表显示了完成查询的平均时间量。
- Database connections（数据库连接数）– 此图表显示了活动的数据库连接数。
- Running queries（正在运行的查询数）– 此图表显示了在给定时间内正在运行的查询总数。
- Queued queries（排队的查询）– 此图表显示了在给定时间排队的查询总数。
- Query run time breakdown（查询运行时间细分）– 此图表显示了查询类型运行的查询所花费的总时间。

在 Resource monitoring（资源监控）页面上，您可以查看已消耗资源的图表。您可以根据几个方面来筛选数据。

- Metric filter（筛选指标）– 您可以使用指标筛选条件为特定工作组选择筛选条件，也可以选择时间范围和时间间隔。
- RPU capacity used（已使用的 RPU 容量）– 此图表显示了 Redshift 处理单元（RPU）的总容量。
- Compute usage（计算使用率）– 此图表显示了所选时间范围内按时间段划分的 Amazon Redshift Serverless 的累计使用情况。

在 Datashares（数据共享）页面上，您可以管理 In my account（在我的账户）和 From other accounts（从其它账户）的数据共享。有关数据共享的更多信息，请参阅Amazon Redshift Serverless 中的数据共享 (p. 47)。

Amazon Redshift Serverless 的计算容量

了解 Amazon Redshift Serverless 容量

PRU

Amazon Redshift Serverless 以 Redshift 处理单元 (RPU) 为单位测量数据仓库容量。RPU 是用于处理工作负载的资源。

基本容量

此设置指定 Amazon Redshift Serverless 用于处理查询的基本数据仓库容量。基本容量以 RPU 为单位指定。设置更高的基本容量可提高查询性能，尤其是对于消耗大量资源的数据处理任务。Amazon Redshift Serverless 的原定设置基本容量为 128 个 RPU。您可以使用管理控制台，以 8（32、40、48...512）为单位将 Base capacity（基本容量）设置从 32 个 RPU 调整为 512 个 RPU。

Amazon Redshift Serverless 的计费

了解 Amazon Redshift Serverless 计费

计算容量的计费

基本容量及其对计费的影响

当查询运行时，系统将根据给定持续时间内使用的容量（以 RPU 小时为单位）按秒对您进行收费。如果没有任何查询在运行，则您不需要为计算容量付费。您还需要根据存储的数据量为 Redshift 托管式存储付费。您可以在创建工作组时设置 Base capacity（基本容量）。您可以调高或调低现有工作组的基本容量，以满足工作组级别的工作负载的性价比要求。随着查询数量增加，Amazon Redshift Serverless 会自动扩缩以提供一致的性能。您可以使用控制台更改基本容量，方法是从 Workgroup configuration（工作组配置）中选择工作组，然后选择 Limits（限制）选项卡。

最大 RPU 小时数

为了使 Amazon Redshift Serverless 的成本保持可预测，您可以设置每天、每周或每月使用的 Maximum RPU hours（最大 RPU 小时数）。您可以使用控制台或 API 来设置该值。达到限制后，您可以指定将日志条目写入系统表，或者接收告警，或者关闭用户查询。设置最大 RPU 小时数有助于控制成本。对于访问数据仓库中数据的查询和访问外部数据的查询（例如 Amazon S3 中的外部表），有关最大 RPU 小时数的设置适用于您的工作组。

为工作组设置最大 RPU 小时数不会限制性能。您可以随时对此设置进行调整，而不会中断查询处理。

设置基本容量和最大 RPU 小时数可以帮助您满足性价比要求，同时保持成本可预测。有关基本容量设置的更多信息，请参阅了解 Amazon Redshift Serverless 容量 (p. 17)。有关无服务器计费的更多信息，请参阅 Amazon Redshift 定价。

保持 Amazon Redshift Serverless 成本可预测的另一种方法是使用 Amazon 成本异常检测，以减少账单中的意外情况并提供更多控制权。

说明计算成本计费方案

长期运行的任务

以下是一个示例场景，用于说明目的，不考虑最低计费要求：您在美国东部（弗吉尼亚北部）区域的 Amazon Redshift 数据仓库上，在上午 7:00 至晚上 7:00 之间每小时运行一次数据处理任务。假设每次任务运行时，需要 10 分 30 秒钟才能完成，这不会改变。并且假设在任务期间，Amazon Redshift 以 128 个 RPU 容量运行。以下结果显示了当天的总使用量和成本：

- 查询持续时间 - 任务在上午 7:00 至下午 7:00 之间运行 13 次，每次运行需要 10 分 30 秒。这加起来长达 8190 秒。
- 使用的容量 - 128 个 RPU
- 每日收费：109.20 美元（（8190 秒 x 128 RPU * 该区域每 RPU 小时 0.375 美元）/一小时 3600 秒）

有关最新的定价信息，请参阅 Amazon Redshift 定价。

监控使用情况和成本

您可以通过多种方法来估计 Amazon Redshift Serverless 的使用情况和计费。系统视图可能会很有用，因为系统元数据（包括查询和使用情况数据）是及时的，并且您无需进行任何设置即可查询到。CloudWatch 还可用于监控 Amazon Redshift Serverless 实例的使用情况，并具有提供洞察和设置操作的附加功能。

通过查询系统视图可视化使用情况

您可以查询 `sys_serverless_usage` 系统表以跟踪使用情况。查询它以检索处理查询的持续时间的近似值：

```
select
  trunc(start_time) "Day",
  sum(compute_seconds)/60/60 * <Price for 1 RPU>
from sys_serverless_usage
group by trunc(start_time)
order by 1
```

此查询概略估算 Amazon Redshift Serverless 每天产生的成本。Amazon Redshift Serverless 向 Amazon 账单报告的方式、聚合频率的差异和舍入等变化可能会影响账单。它可能与来自 `sys_serverless_usage` 的结果略有不同。此外，`sys_serverless_usage` 几乎实时显示您的使用情况。账单报告是在查询完成后创建的。`sys_serverless_usage` 中记录的使用情况可能未反映在账单报告中。因此，`sys_serverless_usage` 中的信息应该用于概略估算您的月末账单。它并不完全相符。有关监控表和视图的更多信息，请参阅使用 Amazon Redshift Serverless 监控查询和工作负载 (p. 35)。

使用 CloudWatch 可视化使用情况

您可以使用 CloudWatch 中提供的指标来跟踪使用情况。为 CloudWatch 生成的指标是 `ComputeSeconds` 和 `ComputeCapacity`，前者表示当前分钟内使用的总 RPU 秒数，后者表示该分钟的总计算容量。也可以在 Redshift 控制台上的 Redshift Serverless dashboard（无服务器控制面板）中找到使用情况指标。有关 CloudWatch 的更多信息，请参阅什么是 Amazon CloudWatch？

对存储计费

主存储容量按 Redshift 托管式存储 (RMS) 计费。存储按 GB/月计费。存储计费与计算资源的计费是分开的。用于用户快照的存储按标准备份账单费率计费，具体取决于使用套餐。

数据传输成本和机器学习 (ML) 成本单独计费，与预置集群适用相同的费率。跨 Amazon 区域的快照复制和数据共享按定价页面上列出的传输费率计费。有关更多信息，请参阅 Amazon Redshift 定价。

使用 CloudWatch 可视化使用情况计费

将生成指标 `SnapshotStorage`（用于跟踪快照存储使用情况）并发送到 CloudWatch。有关 CloudWatch 的更多信息，请参阅什么是 Amazon CloudWatch？

Amazon Redshift Serverless 免费试用

Amazon Redshift Serverless 提供免费试用。如果您参加免费试用，则可以在 Redshift 控制台中查看免费试用积分余额，然后在 SYS_SERVERLESS_USAGE 系统视图中检查免费试用使用情况。请注意，免费试用的账单详细信息不会显示在账单控制台中。免费试用结束后，您只能在账单控制台中查看使用情况。

账单使用注释

- 记录使用情况 - 查询或事务仅在事务完成、回滚或停止后才计量和记录。例如，如果事务运行两天，则在此事务完成后记录 RPU 使用情况。您可以通过查询 `sys_serverless_usage` 来实时监控正在进行的使用情况。事务记录可能反映为 RPU 使用情况变化，并影响特定小时数和每日使用情况的成本。

- 编写显式事务 - 作为结束事务的最佳实践，这一点很重要。如果您没有结束或回滚未结事务，Amazon Redshift Serverless 将继续使用 RPU。例如，如果您编写一个显式 `BEGIN TRAN`，务必具有相应的 `COMMIT` 和 `ROLLBACK` 语句。
- 已取消的查询 - 如果您运行了查询并在查询结束之前将其取消，您仍需要按查询运行时间付费。
- 扩缩 - Amazon Redshift Serverless 实例可以启动扩缩以处理较高负载时段，从而保持一致的性能。您的 Amazon Redshift Serverless 账单同时包括以相同 RPU 费率计算的基本计算和扩展容量。
- 缩减 - Amazon Redshift Serverless 从其基本 RPU 容量纵向扩展以处理负载较高的时期。在某些情况下，在查询负载下降后的一段时间内，RPU 容量可以保持在较高的设置。我们建议您在控制台中设置最大 RPU 小时数，以防止出现意外的成本。有关更多信息，请参阅 Amazon Redshift Serverless 的账单。
- 系统表 - 查询系统表时，会对查询时间进行计费。
- Redshift Spectrum - 当您拥有 Amazon Redshift Serverless 并运行查询时，不对数据湖查询单独收费。对于针对 Amazon S3 中存储的数据进行的查询，按事务时间计算，费用与针对本地数据进行的查询相同。
- 联合查询 - 联合查询按特定时间间隔内使用的 RPU 付费，与针对数据仓库或数据湖的查询相同。
- 存储 - 存储单独收费，按 GB/月计费。
- 最低收费 – 最低收取 60 秒的费用，按秒计费。
- 快照计费 - 快照计费不变。它根据存储空间收费，按每月 GB 的费率计费。您可以按 30 分钟的粒度将数据仓库还原到过去 24 小时内的特定点，无需付费。有关更多信息，请参阅 Amazon Redshift 定价。

Amazon Redshift Serverless 保持账单可预测性的最佳实践

有一些最佳实践可以遵循，一些内置设置可帮助您保持账单一致性。

正如本主题前面提到的那样，请务必结束每笔交易。当您使用 `BEGIN` 开始交易时，务必也要使用 `END` 结束交易。还可以使用最佳实践错误处理来从容地响应错误并结束每笔交易。尽量减少未结交易有助于避免不必要地使用 RPU。

`SESSION TIMEOUT` 可通过结束未结交易和空闲会话来提供帮助。它会导致任何会话保持打开达原定设置 3600 秒（1 小时），然后超时。可以为特定用户显式更改此超时设置，例如您希望为长时间运行的查询保持会话打开时。主题 CREATE USER 显示了如何为用户调整 `SESSION TIMEOUT`。

在大多数情况下，我们建议您不要延长 `SESSION TIMEOUT` 值，除非您的用例特别需要。如果会话保持空闲状态并且存在未结交易，则可能会导致在会话关闭之前使用 RPU 的情况。这将导致不必要的成本。

Amazon Redshift Serverless 在查询发生超时之前，运行查询的最长时间为四小时。此外，空闲交易的最大值为 6 小时，然后发生超时。有关更多信息，请参阅Amazon Redshift Serverless 对象的配额 (p. 517)。

连接到 Amazon Redshift Serverless

设置好 Amazon Redshift Serverless 实例后，您可以使用下面概述的各种方法连接到该实例。如果您有多个团队或项目并且想单独管理成本，则可以单独使用 Amazon Web Services 账户。

有关提供了 Amazon Redshift Serverless 的 Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中针对 Redshift Serverless API 列出的端点。

Amazon Redshift Serverless 连接到当前 Amazon Web Services 区域中您的 Amazon Web Services 账户中的无服务器环境。Amazon Redshift Serverless 在端口 5439 上的 VPC 中运行。

连接到 Amazon Redshift Serverless

您可以使用以下语法连接到 Amazon Redshift Serverless 实例中的数据库（名为 `dev`）。

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

例如，以下连接字符串指定区域 us-east-1。

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

通过 JDBC 驱动程序连接到 Amazon Redshift Serverless

通过 Amazon Redshift 提供的 JDBC 驱动程序版本 2 驱动程序，使用首选 SQL 客户端，您可以使用以下方法之一连接到 Amazon Redshift Serverless。

要使用 JDBC 驱动程序版本 2.1.x 或更高版本，通过用户名和密码进行连接以执行数据库身份验证，请使用以下语法。端口号是可选的；如果未包括在内，Amazon Redshift Serverless 原定设置使用端口号 5439。

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

例如，以下连接字符串指定原定设置工作组、账户 ID 123456789012 和区域 us-east-2。

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

要使用 JDBC 驱动程序版本 2.1.x 或更高版本连接 IAM，请使用以下语法。端口号是可选的；如果未包括在内，Amazon Redshift Serverless 原定设置使用端口号 5439。

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

例如，以下连接字符串指定原定设置工作组、账户 ID 123456789012 和区域 us-east-2。

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

对于 ODBC，使用以下语法。

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

如果您使用 2.1.0.9 之前的 JDBC 驱动程序版本并与 IAM 连接，则需要使用以下语法。

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

例如，以下连接字符串指定原定设置工作组和 Amazon Web Services 区域 us-east-1。

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

有关驱动程序的更多信息，请参阅《Amazon Redshift 集群管理指南》中的配置连接。

使用数据 API 连接到 Amazon Redshift Serverless

还可使用 Amazon Redshift 数据 API 连接到 Amazon Redshift Serverless。在 Amazon CLI 调用中使用 `workgroup-name` 参数而不是 `cluster-identifier` 参数。

有关数据 API 的更多信息，请参阅使用 Amazon Redshift 数据 API (p. 267)。

使用 SSL 连接到 Amazon Redshift Serverless

配置与 Amazon Redshift Serverless 的安全连接

Amazon Redshift 支持安全套接字层（SSL）连接，以加密查询和数据。要设置安全连接，您可以使用相同配置设置到预置 Redshift 集群的连接。按照 Configuring security options for connections（配置连接的安全选项）中的步骤进行操作，其中介绍了如何下载和安装可用的 SSL 证书捆绑包。该捆绑包适用于连接到无服务器 Redshift 实例和预置集群。连接到 Amazon Redshift Serverless 实例时，您无需设置任何参数即可接受 SSL 连接。

从 Amazon Redshift 托管式 VPC 端点连接到 Amazon Redshift Serverless

从其他 VPC 端点连接到 Amazon Redshift Serverless

您可以从其它 VPC 端点（包括本地和公有 VPC 端点）连接到 Amazon Redshift Serverless。

从 Redshift 托管式 VPC 端点连接到 Amazon Redshift Serverless

Amazon Redshift Serverless 在 VPC 中预置。通过创建 Redshift 托管式 VPC 端点，您可从其他 VPC 中的客户端应用程序以私有方式访问您的 Amazon Redshift Serverless。这样，流量不会通过互联网，也不使用公有 IP 地址。从而提高了通信的私密性和安全性。

使用控制台创建 Redshift 托管式 VPC 端点

1. 在控制台上，选择 Workgroup configuration（工作组配置），然后从列表中选择工作组。
2. 在 Redshift managed VPC endpoints（Redshift 托管式 VPC 端点）中，选择 Create endpoint（创建端点）。
3. 输入端点名称。创建一个对组织有意义的名称。
4. 选择 Amazon 账户 ID。这是您的 12 位账户 ID 或账户别名。
5. 选择该端点所在的 Amazon VPC。然后选择一个子网 ID。在最常见的使用案例中，这是一个子网，您在其中有一个要连接到 Amazon Redshift Serverless 实例的客户端。
6. 您可以选择要添加的 VPC 安全组。例如，每个安全组都充当一个虚拟防火墙，用来控制特定虚拟桌面实例的入站和出站流量。
7. 选择 Create endpoint（创建端点）。

使用控制台编辑 Redshift 托管式 VPC 端点

1. 在控制台上，选择 Workgroup configuration（工作组配置），然后从列表中选择工作组。
2. 在 Redshift managed VPC endpoints（Redshift 托管式 VPC 端点）中，选择 Edit（编辑）。
3. 添加或删除 VPC 安全组。这是在创建 Redshift 托管式 VPC 端点后，您唯一可更改的设置。
4. 选择保存更改。

在控制台上删除 Redshift 托管式 VPC 端点

1. 在控制台上，选择 Workgroup configuration（工作组配置），然后从列表中选择工作组。
2. 在 Redshift managed VPC endpoints（Redshift 托管式 VPC 端点）中，选择要删除的 VPC 端点。
3. 选择 Delete（删除）。

创建可公开访问的 Amazon Redshift Serverless 实例并连接到该实例

连接到可公开访问的 Amazon Redshift Serverless 实例

您可以配置 Amazon Redshift Serverless 实例，以便可以从公有互联网中的 SQL 客户端查询它。您不必始终从本地 VPC 或防火墙背后的子网进行连接。

这些步骤将引导您完成配置 Amazon Redshift Serverless 以接受来自互联网的连接。

1. 在 Redshift 控制台上，转到 Amazon Redshift Serverless 主菜单。选择 Create workgroup（创建工作组），然后按照以下步骤为其命名并选择关联的 VPC 和子网。选择 Next (下一步)。
2. 完成创建命名空间的步骤。该过程包括指定数据库和分配具有执行数据库任务权限的 IAM 角色。

   如果您已经创建了一个命名空间，这也有效。
3. 完成前面的步骤之后，或者如果您已经拥有现有的命名空间和工作组，请选择 Workgroup configuration（工作组配置），然后从列表中选择工作组。然后，在 Network and security（网络和安全性）面板中，选择 edit（编辑）。
4. 选择 Turn on Public Accessible（开启可公有访问）。执行此操作时，Amazon Redshift Serverless 实例将通过为其分配静态 IPv4 弹性 IP 地址来实现可公有访问。此 IP 地址分配给您的 Amazon 账户。

将 Amazon Redshift Serverless 配置为接受来自公有客户端的连接后，请按照以下步骤进行连接。

1. 在 Amazon Redshift 控制台上，选择 Serverless dashboard（无服务器控制面板），选择 Workgroup configuration（工作组配置），然后选择工作组。在 Data access（数据访问）下，选择 Edit（编辑）以查看 Network and security（网络和安全性）设置。记下适用于该工作组的 VPC 安全组。转到 Amazon VPC，然后从菜单中选择 Security groups（安全组）。在列表中选择您的安全组 ID。安全组包含多项配置设置，包括 Inbound rules（入站规则）。选择 Edit inbound rules（编辑入站规则），并创建一个规则，指定要允许的源 IP 地址和端口。Amazon Redshift 的默认端口为 5439。
2. 在 Amazon VPC 服务控制台上，验证并确保互联网网关已附加到您的 VPC。要从公共互联网连接到可公开访问的集群，必须将互联网网关附加到路由表。确认使用源 0.0.0.0/0 或公共 IP CIDR 设置该互联网网关的目标。路由表必须与您的集群所在的 VPC 子网相关联。

   有关附加互联网网关的更多信息，请参阅使用互联网网关连接到互联网中的创建并附加互联网网关一节。
3. 在客户端上，设置入站防火墙规则以接受端口 5439 上的流量。
4. 与您的客户端工具（如 PSQL）连接。使用您的 Amazon Redshift Serverless 域作为主机，输入以下内容：

```
psql "host=redshift-serverless-dns-name.region.amazonaws.com dbname=dev port=5439
 user=admin"
```

Amazon Redshift Serverless 中的安全性和连接

访问 Amazon Redshift 时需要可供 Amazon 用来验证您的请求的凭证。

Amazon Redshift Serverless 中的 Identity and Access Management

访问 Amazon Redshift 时需要可供 Amazon 用来验证您的请求的凭证。这些凭证必须有权访问 Amazon 资源，如 Amazon Redshift Serverless。

以下部分提供详细信息来说明如何使用 Amazon Identity and Access Management（IAM）和 Amazon Redshift 控制谁能访问您的资源，从而对这些资源进行保护：有关更多信息，请参阅Amazon Redshift 中的 Identity and Access Management (p. 356)。

向 Amazon Redshift Serverless 授予权限

要访问其它 Amazon 服务，Amazon Redshift Serverless 需要权限。

授权 Amazon Redshift Serverless 为您访问其它 Amazon 服务

某些 Amazon Redshift 功能要求 Amazon Redshift 代表您访问其他 Amazon 服务。为了让您的 Amazon Redshift Serverless 实例为您执行操作，请向它提供安全凭证。提供安全凭证的首选方法是指定一个 Amazon Identity and Access Management (IAM) 角色。您还可通过 Amazon Redshift 控制台创建 IAM 角色，并将其设置为默认角色。有关更多信息，请参阅创建一个 IAM 角色作为 Amazon Redshift 的默认角色 (p. 24)。

要访问其它 Amazon 服务，请创建具有适当权限的 IAM 角色。您还需要将角色与您的 Amazon Redshift Serverless 关联。此外，您可在运行 Amazon Redshift 命令时指定角色的 Amazon Resource Name（ARN），或者指定 `default` 关键字。

在 https://console.aws.amazon.com/iam/ 中更改 IAM 角色的信任关系时，请确保使用 `redshift.amazonaws.com` 作为服务名称。有关如何管理 IAM 角色以代表您访问其它 Amazon 服务的信息，请参阅授权 Amazon Redshift 代表您访问其他 Amazon 服务 (p. 425)。

创建一个 IAM 角色作为 Amazon Redshift 的默认角色

当您通过 Amazon Redshift 控制台创建 IAM 角色时，Amazon Redshift 以编程方式在您的 Amazon Web Services 账户 中创建角色。Amazon Redshift 还会自动为其附加现有 Amazon 托管式策略。这种方法表示您可以停留在 Amazon Redshift 控制台中，无需切换到 IAM 控制台进行角色创建。

您通过控制台为集群创建的 IAM 角色具有自动附加的 `AmazonRedshiftAllCommandsFullAccess` 托管式策略。此 IAM 角色允许 Amazon Redshift 为 Amazon IAM 账户中的资源复制、卸载、查询和分析数据。相关命令包括 UNLOAD、CREATE EXTERNAL FUNCTION、CREATE EXTERNAL TABLE、CREATE EXTERNAL SCHEMA、CREATE MODEL 和 CREATE LIBRARY。有关如何创建 IAM 角色作为 Amazon Redshift 的默认角色的更多信息，请参阅创建一个 IAM 角色作为 Amazon Redshift 的默认角色 (p. 24)。

要开始创建 IAM 角色作为 Amazon Redshift 的默认角色，请打开 Amazon Web Services Management Console，选择 Amazon Redshift 控制台，然后选择 Try Amazon Redshift Serverless（尝试 Amazon Redshift Serverless）。在 Amazon Redshift Serverless 控制台上，选择 Customize settings（自定义设置）。在 Permissions（权限）下，按照 使用控制台管理 IAM 角色关联 (p. 432) 中的步骤进行操作。

当您已经拥有 Amazon Redshift Serverless 并希望为它配置 IAM 角色时，请打开 Amazon Web Services Management Console。选择 Amazon Redshift 控制台，然后选择 Go to serverless（转到无服务器）。在 Amazon Redshift Serverless 控制台上，选择 Serverless configuration（无服务器配置），然后选择 Data access（数据访问）。在 Permissions（权限）下，按照 使用控制台管理 IAM 角色关联 (p. 432) 中的步骤进行操作。

向命名空间分配 IAM 角色

每个 IAM 角色都是一个 Amazon 身份，此身份的权限策略可确定每个角色可以在 Amazon 中执行哪些操作。该角色旨在让任何需要它的用户代入。此外，每个命名空间都是对象（如表和架构）和用户的集合。当

您使用 Amazon Redshift Serverless 时，您可以将多个 IAM 角色与命名空间关联。这样可以更轻松地为数据库对象集合适当地构建权限，以便角色可以对内部和外部数据执行操作。例如，您可以在 Amazon Redshift 数据库中运行 `COPY` 命令，以检索 Amazon S3 中的数据并填充 Redshift 表。

您可以使用控制台将多个角色与命名空间关联，如本节前面所述。您还可以使用 `CreateNamespace` API 命令或 CLI 命令 `create-namespace`。使用 API 或 CLI 命令，您可以通过用一个或多个角色填充 `IAMRoles`，以将 IAM 角色分配给命名空间。具体来说，您可以将特定角色的 ARN 添加到集合中。

管理命名空间相关 IAM 角色

在 Amazon Web Services Management Console上，可以管理 Amazon Identity and Access Management 中角色的权限策略。您可以使用 Namespace configuration（命名空间配置）下提供的设置管理命名空间的 IAM 角色。有关命名空间及其在 Amazon Redshift Serverless 中的使用情况的更多信息，请参阅Amazon Redshift Serverless 工作组和命名空间概览 (p. 27)。

Amazon Redshift 的 IAM 凭证入门

当您首次登录到 Amazon Redshift 控制台，并首次尝试 Amazon Redshift Serverless 时，您可以 IAM 用户或 IAM 角色身份登录。开始创建 Amazon Redshift Serverless 实例后，Amazon Redshift 会记录您在登录时使用的 IAM 用户名或角色名称。您可以使用相同的 IAM 凭证登录到 Amazon Redshift 控制台和 Amazon Redshift Serverless 控制台。

创建 Amazon Redshift Serverless 实例时，您可以创建数据库。使用查询编辑器 v2 通过临时凭证选项连接到数据库。

要添加持续用于数据库的新管理员用户名和密码，请选择 Customize admin user credentials（定制管理员用户凭证），然后输入新的管理员用户名和管理员用户密码。

要开始使用 Amazon Redshift Serverless 并首次在控制台中创建工作组和命名空间，请使用 IAM 用户或 IAM 角色。确保此用户或角色具有管理员权限 `arn:aws:iam::aws:policy/AdministratorAccess`，或者具有附加到您使用的 IAM policy 的完整 Amazon Redshift 权限 `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`。

以下场景概述了当您开始使用 Amazon Redshift Serverless 控制台时，Amazon Redshift Serverless 如何使用 IAM 凭证：

- 如果选择 Use default settings（使用默认设置）– Amazon Redshift Serverless 会将您当前的 IAM 身份转换为数据库超级用户。您可以将相同的 IAM 身份与 Amazon Redshift Serverless 控制台一起使用，以在 Amazon Redshift Serverless 的数据库中执行超级用户操作。
- 如果选择 Customize settings（自定义设置）而不指定 Amazon Redshift Serverless 的 Admin user name（管理员用户名）和密码，则您当前的 IAM 凭证用作原定设置管理员用户凭证。
- 如果选择 Customize settings（自定义设置），然后指定 Amazon Redshift Serverless 的 Admin user name（管理员用户名）和密码 – Amazon Redshift Serverless 会将您当前的 IAM 身份转换为数据库超级用户。Amazon Redshift Serverless 还会以超级用户身份创建另一个长期登录用户名和密码对。您可使用当前的 IAM 身份或创建的用户名和密码对以超级用户身份登录到数据库。

将预置集群迁移到 Amazon Redshift Serverless

要从预置集群迁移到 Amazon Redshift Serverless，请参阅以下步骤。

创建预置集群的快照

要将数据从您的预置集群传输到 Amazon Redshift Serverless，请为您的预置集群创建快照，然后在 Amazon Redshift Serverless 中还原该快照。

创建您的预置集群的快照

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）、Snapshots（快照），然后选择 Create snapshot（创建快照）。
3. 输入快照定义的属性，然后选择 Create snapshot（创建快照）。快照可能需要一段时间才可用。

将预置集群快照还原到 Amazon Redshift Serverless 实例

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在 Amazon Redshift 预置集群控制台上开始，导航到 Clusters（集群）、Snapshots（快照）页面。
3. 选择要使用的快照。
4. 选择 Restore snapshot（还原快照）、Restore to serverless namespace（还原到无服务器命名空间）。
5. 选择要将您的快照还原到的命名空间。
6. 确认想要从快照还原。此操作将以来自预置集群的数据替换无服务器端点中的所有数据库。选择 Restore（还原）。

有关预置集群快照的更多信息，请参阅 Amazon Redshift 快照。

使用驱动程序端点

要使用您的首选 SQL 客户端连接到 Amazon Redshift Serverless，您可以使用 Amazon Redshift 提供的 JDBC 驱动程序版本 2 驱动程序。我们建议使用 JDBC 驱动程序版本 2.1.x 或更高版本进行连接。端口号是可选的。如果您未将端口号包括在内，则 Amazon Redshift Serverless 将默认使用端口号 5439。

要查找用于 JDBC 或 ODBC 驱动程序的确切端点，请参阅您的 Amazon Redshift Serverless 实例中的 Workgroup configuration（工作组配置）。您还可以使用 Amazon Redshift Serverless API 操作 `GetWorkgroup` 操作或 Amazon CLI 操作 `get-workgroups`，以返回有关您的工作组的信息，然后进行连接。

使用基于密码的身份验证进行连接

要使用基于密码的身份验证进行连接，请使用以下语法。

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

使用 IAM 进行连接

如果您更喜欢使用 IAM 登录，请使用以下驱动程序端点。此驱动程序端点使您可以连接到特定数据库，并使用 Amazon Redshift Serverless `GetCredentials` API 操作。

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

此驱动程序端点不支持自定义 `dbUser`、`dbGroup` 和 `auto-create`。默认情况下，该驱动程序会在登录时自动创建数据库用户，并根据您在 IAM 中定义的 IAM 用户组将这些数据库用户分配到组。注意：您在 IAM

中指定的 IAM 用户组名称只能包含小写字母、数字、下划线 (“_”) 、加号 (“+”) 、句点 (.)、at 符号 (@) 或连字符 (“-”) 。否则，驱动程序可能无法连接到 dbGroup。

请确保您的 Amazon 身份具有适用于 RedshiftServerlessGetCredentials 操作的正确 IAM policy。下面是一个示例 IAM policy，它授予对 Amazon 身份的正确权限，用于连接到 Amazon Redshift Serverless。有关 IAM 权限的更多信息，请参阅 Add IAM Identity Permissions (添加 IAM 身份权限) 。

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

使用 IAM 与 dbUser 和 dbGroup 连接

如果您要使用自定义 dbUser 和 dbGroup，请使用以下驱动程序端点。与其他 Amazon Redshift Serverless 驱动程序端点一样，此语法会在登录时自动创建数据库用户。此驱动程序端点使用 Amazon Redshift GetClusterCredentials API 操作。dbUser 必须以字母开头，只能包含字母数字字符、下划线 (“_”) 、加号 (“+”) 、句点 (“.”) 、at (“@”) 或连字符 (“-”) ，并且必须少于 128 个字符。dbGroup 只能包含小写字母、数字、下划线 (“_”) 、加号 (“+”) 、句点 (.)、at 符号 (@) 或连字符。

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

使用 ODBC 进行连接

要使用 ODBC 进行连接，请使用以下语法。

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

使用 Amazon Redshift Serverless SDK

如果您使用 Amazon Redshift SDK 编写了任何管理脚本，则必须使用新的 Amazon Redshift Serverless SDK 来管理您的 Amazon Redshift Serverless 实例和资源。有关可用 API 操作的更多信息，请参阅《Amazon Redshift Serverless API 参考指南》。

Amazon Redshift Serverless 工作组和命名空间概览

要在 Amazon Redshift Serverless 中隔离工作负载并管理不同的资源，您可以创建命名空间和工作组，并分别管理存储和计算资源。

Amazon Redshift Serverless 工作组和命名空间概览

命名空间是数据库对象和用户的集合。与存储相关的命名空间会将架构、表、用户或用于加密数据的 Amazon Key Management Service 密钥组合在一起。存储属性包括管理员用户的数据库名称和密码、权限

以及加密和安全性。按命名空间分组的其他资源包括数据共享、恢复点和使用限制。您可以使用 Amazon Redshift Serverless 控制台、Amazon Command Line Interface 或 Amazon Redshift Serverless API 针对特定资源配置这些存储属性。

工作组是计算资源的集合。与计算相关的工作组将计算资源组合在一起，例如 RPU、VPC 子网组和安全组。工作组的属性包括网络和安全设置。按工作组分组的其他资源包括访问权限和使用限制。您可以使用 Amazon Redshift Serverless 控制台、Amazon Command Line Interface 或 Amazon Redshift Serverless API 来配置这些计算属性。

您可以创建一个或多个命名空间和工作组。命名空间可以不关联任何工作组而存在。每个命名空间只能有一个工作组与其关联。反过来，每个工作组只能与一个命名空间关联。

通过控制台开始使用 Amazon Redshift Serverless

设置 Amazon Redshift Serverless 涉及完成数个配置步骤。当您按照这些步骤设置 Amazon Redshift Serverless 时，您将创建命名空间和工作组，然后将它们相互关联。要通过 Amazon Redshift Serverless 控制台开始设置 Amazon Redshift Serverless 配置，您可以选择 Get started with Amazon Redshift Serverless（Amazon Redshift Serverless 入门），以设置 Amazon Redshift Serverless 并开始与之交互。您可以选择具有原定设置的环境，这样可以更快地进行设置，也可以根据企业的要求明确配置设置。在此过程中，您可以为工作组和命名空间指定设置。

设置环境之后，配置工作组 (p. 31)和配置命名空间 (p. 33)可帮助您熟悉这些设置。

使用 Amazon Command Line Interface 和 Amazon Redshift Serverless API 管理 Amazon Redshift Serverless

要创建命名空间，您可以使用 Amazon Command Line Interface 操作 `create-namespace` 或 Amazon Redshift Serverless API 操作 `CreateNamespace`。Amazon Redshift Serverless 使用原定设置 Amazon Key Management Service 密钥创建原定设置命名空间。您还可以指定另一个密钥来加密数据。此外，也可以使用 Amazon Command Line Interface 操作 `restore-from-snapshot` 从快照还原现有命名空间。然后，Amazon Redshift Serverless 会使用从指定快照还原的数据填充命名空间。还可以使用 API 操作 `RestoreFromSnapshot`。

要创建工作组，请确保您拥有现有的命名空间。您可以使用 Amazon Command Line Interface 操作 `create-workgroup` 或 Amazon Redshift Serverless API 操作 `CreateWorkgroup`。指定与工作组关联的目标命名空间。您可以在创建工作组时指定任何计算资源，例如子网、安全组或 RPU。创建后，您可以访问与工作组关联的命名空间。

要更新命名空间或工作组，可以使用 Amazon Command Line Interface 操作 `update-namespace` 或 `update-workgroup`，也可以使用 Amazon Redshift Serverless API 操作 `UpdateNamespace` 或 `UpdateWorkgroup`。

要检索命名空间和工作组的实例列表，请使用 Amazon Command Line Interface 操作 `list-namespaces` 或 `list-workgroups`，或者使用 Amazon Redshift Serverless API 操作 `ListNamespaces` 或 `ListWorkgroups`。

要检索命名空间或工作组的内容或元数据，请使用 Amazon Command Line Interface 操作 `get-namespaces` 或 `get-workgroups`，或者使用 Amazon Redshift Serverless API 操作 `GetNamespace` 或 `GetWorkgroup`。

删除工作组，请使用 Amazon Command Line Interface 操作 `delete-workgroup` 或 Amazon Redshift Serverless API 操作 `DeleteWorkgroup`。删除工作组后，您将无法访问数据库。

要删除命名空间，请首先删除关联的工作组。使用 Amazon Command Line Interface 操作 `delete-namespace` 或 Amazon Redshift Serverless API 操作 `DeleteNamespace`。然后，Amazon Redshift Serverless 会删除指定命名空间中的所有数据。删除命名空间之前，您可以在指定的命名空间上拍摄最终快照，以便根据需要从快照还原数据。为此，请先使用 Amazon Command Line Interface 操作 `create-`

`snapshot` 或 Amazon Redshift Serverless API 操作 `CreateSnapshot`，然后使用 Amazon Command Line Interface 操作 `delete-namespace` 或 Amazon Redshift Serverless API 操作 `DeleteNamespace`。

通过控制台开始使用 Amazon Redshift Serverless

要创建、编辑和删除 Amazon Redshift Serverless 实例，请使用 Amazon Redshift 控制台的 Serverless dashboard（无服务器控制面板）部分。对特定控制台设置的访问权限取决于您的 IAM 角色和您拥有的权限。

首次设置 Amazon Redshift Serverless

第一次选择 Serverless dashboard（无服务器控制面板）时，您将完成设置 Amazon Redshift Serverless 的步骤。在 Get started with the serverless experience（无服务器体验入门）下，您可以使用示例数据集创建 Amazon Redshift Serverless 实例。当您创建新的 Amazon Redshift Serverless 实例时，Amazon Redshift Serverless 会自动加载示例数据集。创建实例后，您可以立即查询数据。有关如何首次设置 Amazon Redshift Serverless 的更多信息，请参阅首次设置 Amazon Redshift Serverless。

配置 Amazon Redshift Serverless

使用 Namespace configuration（命名空间配置）和 Workgroup configuration（工作组配置）以更新 Amazon Redshift Serverless 实例的设置。

对特定控制台设置的访问权限取决于您的 IAM 角色和您拥有的权限。

更改管理员密码

1. 选择 Change admin password（更改管理员密码）。此时将显示对话框。
2. 您可以指定 New admin username（新的管理员用户名）和 New admin user password（新的管理员用户密码）。
3. 选择保存。

使用控制面板检查 Amazon Redshift Serverless

Amazon Redshift Serverless 控制面板包含一系列面板，这些面板一目了然地显示指标和其他信息。这些面板包括：

- Resources summary（资源摘要）：显示有关 Amazon Redshift Serverless 的概括性信息，如使用的存储空间和其他指标。
- Query summary（查询摘要）- 显示有关查询的信息，包括已完成的查询和正在运行的查询。选择 View details（查看详细信息）可转到具有其他筛选条件的屏幕。
- RPU capacity used（已用 RPU 容量）- 显示给定时间段内使用的总容量，例如前十个小时。
- Datashares（数据共享）- 显示数据共享的计数，例如，用于在 Amazon 账户之间共享数据的数据共享的计数。这些指标显示哪些数据共享需要授权以及其他信息。

从控制面板中，您可以快速了解这些可用的指标，以查看有关 Amazon Redshift Serverless 的详细信息，或查看查询或跟踪工作项目。

筛选查询

您可以使用无服务器控制面板上提供的筛选条件。要筛选查询，请执行以下步骤。

1. 在 Query summary（查询摘要）面板的左侧，选择下拉列表以按已完成的查询和/或失败的查询进行筛选。
2. 在 Query summary（查询摘要）面板的右侧，选择下拉列表以按正在运行的查询和/或排队的查询进行筛选。

搜索工作组

在 Amazon Redshift Serverless 中，工作组是可供使用的资源的集合。当您选择 Amazon Redshift Serverless 时，在 Amazon 控制台中，您可以从导航菜单选择 Workgroup configuration（工作组配置）以查看列表。您可以使用 Search（搜索）框以查找符合搜索条件的工作组。每个工作组条目都显示了一些属性：

- Workgroup（工作组）- 工作组的名称。您可以选择它来查看和编辑工作组的属性。
- Status（状态）- 显示工作组是否可用。
- Namespace（命名空间）- 与工作组关联的命名空间。每个工作组都与一个命名空间相关联。
- Creation date（创建日期）- 工作组的创建日期。

创建带有伴随命名空间的工作组

创建工作组

1. 选择 Create workgroup (创建工作组)。
2. 输入工作组名称。
3. 选择 Amazon Redshift Serverless 的 Virtual Private Cloud (VPC) [虚拟私有云 (VPC)]。这会将工作组分配给您的 Amazon 环境中的特定虚拟网络。有关 VPC 的更多信息，请参阅 VPC 和子网概览。
4. 选择一个或多个 VPC security groups（VPC 安全组）。有关更多信息，请参阅使用安全组控制到资源的流量。
5. 在 Subnet（子网）下，指定要与数据库关联的一个或多个子网。这些子网包含在您之前选择的 VPC 中，并且必须位于三个不同的可用区中。选择 Continue（继续）。

选择命名空间

1. 选择 Create a new namespace（创建新的命名空间），然后输入命名空间名称；或者选择 Add to an existing namespace（添加到现有命名空间），然后从下拉列表中选择命名空间。
2. 对于 Database name and password（数据库名称和密码），指定第一个数据库的名称。还可以通过编辑 Admin user credentials（管理员用户凭证），指定原定设置控制台管理员以外的管理员。
3. 对于 Permissions（权限），您选择 Associate IAM role（关联 IAM 角色）以将特定的 IAM 角色与命名空间和工作组关联。有关将 IAM 角色与 Amazon Redshift 关联的更多信息，请参阅 Amazon Redshift 中的 Identity and Access Management。
4. 您可以通过创建新密钥或选择原定设置密钥以外的密钥来自定义加密设置。对于 Audit logging（审计日志记录），选择要导出的日志。每种日志类型指定不同的元数据。选择 Continue（继续）以查看您的选择。

检查工作组选择

1. 在 Review and create（审核和创建）下检查您的设置。它显示了您在前面的步骤中选择的设置。
2. 选择保存。

创建工作组后，它将添加到 Workgroups（工作组）列表。

配置工作组

您可以通过在左侧菜单中选择 Workgroup configuration（工作组配置）以列出工作组。然后，您可以从列表中选择工作组。几个面板显示了工作组的属性。您还可以执行操作。General information（一般信息）显示以下内容：

- Workgroup（工作组）- 工作组的名称。
- Namespace（命名空间）- 与工作组关联的命名空间。您可以选择它以查看其属性。工作组与单个命名空间相关联。
- Date created（创建日期）- 创建工作组的时间。
- Status（状态）- 指示工作组资源是否可用。如果可用，您可以使用客户端连接到 Amazon Redshift Serverless 实例，以便查询数据或创建数据库资源，也可以使用查询编辑器 v2 进行连接。
- Endpoint（端点）- URL。
- JDBC URL（JDBC 网址）- 用于建立 JDBC 客户端连接的 URL。您可以使用此 URL 连接 Amazon Redshift 的 JDBC 驱动程序。有关更多信息，请参阅为 Amazon Redshift 配置 JDBC 驱动程序版本 2.1 连接。
- ODBC URL（ODBC 网址）- 用于建立 ODBC 客户端连接的 URL。它包含数据库和用户 ID 等属性以及它们的值。

Data access（数据访问）选项卡包含几个面板：

- Network and security（网络和安全性）- 您可以看到网络属性，例如 Virtual Private Cloud (VPC) [虚拟私有云 (VPC)] 标识符，VPC security group（VPC 安全组）列表，Enhanced VPC routing（增强型 VPC 路由），以及 Publicly accessible（可公开访问）设置。如果选择 Edit（编辑），您可以更改这些设置。此外，还可以选择 Turn on enhanced VPC routing（启用增强型 VPC 路由），它通过 VPC 在无服务器数据库和数据存储库之间路由网络流量，以增强隐私和安全性。您还可以选择 Turn on Public Accessible（开启可公有访问），这使得数据库可以从 VPC 外部公开访问，从而允许实例和设备进行连接。
- Redshift managed VPC endpoints（Redshift 托管式 VPC 端点）- 您可以创建托管式 VPC 端点以从另一个 VPC 访问 Amazon Redshift Serverless。

Limits（限制）选项卡中有用于控制 Amazon Redshift Serverless 的容量和使用限制的设置。它包含以下面板：

- Base capacity in Redshift processing units (RPUs)（以 Redshift 处理单元 (RPU) 表示的基本容量）– 您可以设置用于处理工作负载的计算资源的基本容量。有关更多信息，请参阅了解 Amazon Redshift Serverless 容量 (p. 17)。
- Usage limits（使用限制）- 您可以设置不同频率下的最大 RPU 小时数。例如，您可以设置每日 RPU 最大值。这些限制有助于控制成本并使其更具可预测性。
- Query limits（查询限制）- 您可以对查询设置限制，例如超时设置。这些限制有助于您优化成本和性能。

管理使用限制

在工作组的 Limits（限制）选项卡中，您可以添加一个或多个使用限制，以控制在给定时间段内使用的最大 RPU 数，或设置数据共享使用限制。

1. 选择 Manage usage limits（管理使用限制）。在 Redshift processing units (RPUs) maximum（Redshift 处理单元 (RPU) 最大值）面板上选择 Add limit（添加限制）。
2. 首先，选择 Frequency（频率），即 Daily（每天）、Weekly（每周）或 Monthly（每月）。这将设置限制的时间段。在这种情况下选择 Daily（每天）可向您提供更详细的控制权。
3. 设置使用限制（以小时数为单位）。
4. 选择操作。这些操作包括：

- Log to system table（登录系统表）- 将记录添加到系统表中，您可以查询该表以确定是否超过限制。
- Alert（提醒）- 使用 Amazon SNS 设置通知订阅，并在违反限制时发送通知。您可以选择现有的 Amazon SNS 主题或创建一个新主题。
- Turn off user queries（关闭用户查询）- 禁用查询以停止使用 Amazon Redshift Serverless。它还会发送通知。

前两个操作是信息性的，但最后一个操作会关闭查询处理。

5. （可选）您可以设置 Cross-Region data sharing usage limit（跨区域数据共享使用限制），这限制了使用者可以查询的从生产者区域传输到使用者区域的数据量。为此，请选择 Add limit（添加限制），然后按以下步骤操作。
6. 选择 Save changes（保存更改）以保存限制。

管理查询限制

在工作组的 Limits（限制）选项卡中，您可以添加限制以指定查询执行超时。

1. 选择 Manage query limits（管理查询限制）。在 Manage query limits（管理查询限制）对话框中选择 Add limit（添加限制）。
2. 为 Limit（限制）输入一个整数值（以秒为单位）。这指定查询发生超时之前经过的时间。

   如果之前设置了超时限制，您可以删除它并指定新值。
3. 选择 Save changes（保存更改）以保存限制。

当您更改查询限制和配置参数时，数据库将重新启动。

删除工作组

您可以使用控制台删除工作组。在执行此操作之前，请确保已备份数据并已准备好快照。在许多情况下，无法检索作为工作组一部分删除的资源。

完成以下步骤：

1. 选择 Amazon Redshift Serverless，选择 Workgroup configuration（工作组配置），然后选择 Delete Amazon Redshift Serverless instance（删除 Amazon Redshift Serverless 实例）。
2. 此时将打开一个对话框。当您选择删除工作组时，将删除所有使用限制，删除所有 VPC 端点，并删除对 VPC 端点的访问权限。

   键入 delete，并选择 Delete（删除）以进行确认。

完成这些步骤后，工作组的状态为 Deleting（正在删除），并且横幅表明正在删除工作组。正在执行删除过程时，Serverless dashboard（无服务器控制面板）下的某些功能将被禁用。但是，您可以在 Provisioned clusters dashboard（预置集群控制面板）上配置预置的集群。

删除工作组后，它不会随命名空间一起显示。您可以选择 Create workgroup（创建工作组）按钮以创建新的工作组。

您可以删除现有工作组，然后将具有不同配置的新工作组关联到同一命名空间。创建新工作组时，请选择基本容量，用于确定与命名空间关联的数据大小。

您可以将工作组与使用客户托管式密钥 (CMK) 创建的命名空间相关联。有关 Amazon KMS 的更多信息，请参阅 Amazon KMS 概念。

搜索命名空间

在 Amazon Redshift Serverless 中，命名空间定义了数据库对象的逻辑容器。它可以存放表、工作组和其他数据库资源。从 Amazon Redshift 菜单中，您可以从 Namespaces（命名空间）列表中进行选择，以查看或编辑命名空间的属性。控制台上的信息包括命名空间名称、管理员名称和其他属性。

命名空间的设置和属性位于多个选项卡上。这些功能包括：

- Workgroup（工作组）- 显示与命名空间关联的工作组。
- Data back up（数据备份）- 您可以配置和创建快照，并配置恢复点。
- Security and encryption（安全性和加密）- 您可以管理 IAM 角色权限以及查看或编辑安全和加密设置。其中包括您的加密密钥状态和审计日志记录设置。
- Datashares（数据共享）- 显示数据共享。

配置命名空间

在 Amazon Redshift Serverless 中，命名空间定义了数据库对象的容器。您可以从导航列表中选择 Namespace configuration（配置命名空间），从列表中选择命名空间，然后编辑其设置。

命名空间的一般信息包括以下内容：

- Namespace（命名空间）- 名称。
- Namespace ID（命名空间 ID）- 唯一标识符。
- ARN - 用于跨 Amazon 指定资源的唯一标识符。它包含区域和服务等属性。
- Status（状态）- 状态，例如 Available（可用）。
- Date created（创建日期）- 创建命名空间的日期。
- Storage used（使用的存储空间）- 命名空间及其所有对象使用的存储空间。
- Admin user name（管理员用户名）- 管理员账户。这通常是用于创建命名空间的账户。
- Database name（数据库名称）- 命名空间中包含的数据库的名称。
- Total table count（总表数）- 所有架构中表的计数。

命名空间的其他设置和属性位于多个选项卡上。这些功能包括：

- Workgroup（工作组）- 显示与命名空间关联的工作组。
- Data back up（数据备份）- 在此面板上，您可以配置和创建快照，并配置恢复点。
- Security and encryption（安全性和加密）- 您可以管理 IAM 角色权限以及查看或编辑安全和加密设置。其中包括您的加密密钥状态以及开启审计日志记录的设置。有关 Amazon Redshift Serverless 的审计日志记录的更多信息，请参阅 Amazon Redshift Serverless 的审计日志记录。
- Datashares（数据共享）- 显示数据共享。通过数据共享，您可提供对数据的访问，而无需复制或移动数据。有关数据共享的更多信息，请参阅 Amazon Redshift Serverless 中的数据共享。

编辑安全性和加密

1. 从控制台的主菜单中选择 Namespace configuration（配置命名空间），选择要编辑的命名空间，然后选择 Edit security and encryption（编辑安全性和加密）。此时将显示对话框。
2. 您可以选择 Customize encryption settings（自定义加密设置），然后选择 Amazoncustomer managed key（客户托管式密钥）以更改用于加密资源的密钥。
3. 对于 Audit logging（审计日志记录），选择要导出的日志。每种日志类型指定不同的元数据。
4. 要完成配置更新，请选择 Save changes（保存更改）。

删除命名空间

如果要删除具有关联工作组的命名空间，则必须先删除该工作组。

在 Amazon Redshift Serverless 控制台上，完成以下步骤：

1. 从左侧菜单中选择 Namespace configuration（配置命名空间），然后选择要从列表中删除的命名空间。
2. 选择 Actions（操作），然后选择 Delete namespace（删除命名空间）。
3. 此时会显示对话框。在完成删除操作之前，您可以通过创建手动快照来保留数据。

   键入 delete，并选择 Delete（删除）以进行确认。

更改命名空间的 Amazon KMS 密钥

在 Amazon Redshift 中，加密为静态数据提供保护。Amazon Redshift Serverless 自动使用 Amazon KMS 密钥加密来加密您的 Amazon Redshift Serverless 资源和快照。作为最佳实践，大多数企业会审查其存储的数据类型，并计划按时间表轮换加密密钥。轮换密钥的频率可能会有所不同，具体取决于您的数据安全策略。Amazon Redshift Serverless 支持更改命名空间的 Amazon KMS 密钥，以便您可以遵守企业的安全策略。

当您更改 Amazon KMS 密钥时，数据保持不变。

使用控制台更改 Amazon KMS 密钥

在 Amazon Redshift 中，加密为静态数据提供保护。Amazon Redshift Serverless 自动使用 Amazon KMS 密钥加密来加密 Amazon Redshift Serverless 和快照。作为最佳实践，大多数企业会审查其存储的数据类型，并计划按时间表轮换加密密钥。轮换密钥的频率可能会有所不同，具体取决于您的数据安全策略。Amazon Redshift Serverless 支持更改命名空间的 Amazon KMS 密钥，以便您可以遵守企业的安全策略。

当您更改 Amazon KMS 密钥时，数据保持不变。

1. 登录到 Amazon 控制台。选择 Amazon Redshift 控制台。
2. 在导航菜单上，选择 Namespace configuration（命名空间配置）。从列表中选择命名空间。
3. 从 Security and encryption（安全性和加密）选项卡上，选择 Edit（编辑）。
4. 选择 Customize encryption settings（自定义加密设置），然后为命名空间选择密钥。您可以选择创建新密钥。

使用 Amazon CLI 更改 Amazon KMS 加密密钥

使用 `update-namespace` 更改命名空间的 Amazon KMS 密钥。下面说明此命令的语法：

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

必须已创建命名空间，否则 CLI 命令会导致错误。

更改密钥所需的时间取决于 Amazon Redshift Serverless 中的数据量。通常，对于每 8TB 存储数据，此过程需要 15 分钟。

限制

您无法将客户托管式 KMS 密钥更改为 Amazon KMS 密钥。在这种情况下，您必须创建一个新的命名空间。

更改密钥时，您无法执行其他操作。

使用 Amazon Redshift Serverless 监控查询和工作负载

使用 Amazon Redshift Serverless 监控查询和工作负载

您可以使用提供的系统视图监控 Amazon Redshift Serverless 查询和工作负载。

授予监控查询的访问权限

超级用户可以向不是超级用户的用户提供访问权限，以便他们可以对所有用户执行查询监控。首先，您可以为用户或角色添加策略以提供查询监控访问权限。然后，您可以授予用户或角色查询监控权限。

添加查询监控策略

1. 选择 https://console.aws.amazon.com/iam/。
2. 在 Access management (访问管理) 下，选择 Policies (策略)。
3. 请选择Create Policy（创建策略）。
4. 选择 JSON，然后粘贴以下策略定义。

```
{
"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. 选择Review policy（查看策略）。
6. 对于 Name (名称)，输入策略的名称，如 `query-monitoring`。
7. 选择 Create policy（创建策略）。
8. 在 Policies（策略）下，选择您创建的策略。
9. 在 Actions（操作）下，选择 Attach（附加）。
10. 选择要附加该策略的用户或角色，然后选择 Attach policy（附加策略）。

授予用户查询监控权限

具有 sys:monitor 权限的用户可以查看所有查询。此外，具有 sys:operator 权限的用户可以取消查询、分析查询历史记录和执行 vacuum 操作。

1. 输入以下命令以提供系统监控访问权限，其中 user-name 是您想要为其提供访问权限的用户的名称。

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

2. （可选）输入以下命令以提供系统操作员访问权限，其中 user name 是您想要为其提供访问权限的用户的名称。

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

授予角色查询监控权限

具有 sys:monitor 权限的角色的用户可以查看所有查询。此外，具有 sys:operator 权限的角色的用户可以取消查询、分析查询历史记录和执行 vacuum 操作。

1. 输入以下命令以提供系统监控访问权限，其中 role-name 是您想要为其提供访问权限的角色的名称。

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

2. （可选）输入以下命令以提供系统操作员访问权限，其中 role-name 是您想要为其提供访问权限的角色的名称。

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

监控视图

Monitoring views（监控视图）是 Amazon Redshift Serverless 中用于监控查询和工作负载使用情况的系统视图。这些视图位于 pg_catalog 架构中。可用的系统视图旨在为您提供监控 Amazon Redshift Serverless 所需的信息，这比预置集群所需的信息简单得多。SYS 系统视图旨在与 Amazon Redshift Serverless 配合使用。要显示这些视图提供的信息，请运行 SQL SELECT 语句。

系统视图的定义是为了支持以下监控目标。

工作负载监控

您可以随时间推移监控查询活动，以便：

- 了解工作负载模式，这样您就可以了解正常运行状况（基准）以及业务服务级别协议（SLA）中的内容。
- 快速识别偏离正常运行的状况，这可能是个暂时性问题，或是需要采取进一步操作的问题。

数据加载和卸载监控

进出 Amazon Redshift Serverless 的数据移动是一项关键功能。您可以使用 COPY 和 UNLOAD 来加载和卸载数据，并且必须密切监控传输的字节/行数和文件的完成进度，以跟踪遵守业务 SLA 的情况。这通常是通过频繁运行系统表查询（即每分钟）来完成，以便跟踪进度，并在检测到重大偏差时发出调查/纠正操作的提示。

故障和问题诊断

某些情况下，必须对查询或运行时故障采取措施。开发人员依靠系统表自行诊断问题，并确定正确的纠正补救措施。

性能优化

您可能需要优化从一开始就不符合 SLA 要求的查询或随时间推移而降级的查询。要进行优化，您必须具有运行时详细信息，包括运行计划、统计数据、持续时间和资源占用情况。您需要用于违规查询的基准数据，以确定偏差的原因并指导您如何改进性能。

用户对象事件监控

您需要监控用户对象上的操作和活动，例如刷新具体化视图、VACUUM 和分析。这包括系统管理的事件，例如具体化视图的自动刷新。如果事件是用户启动的，您想监控事件结束时间，或者如果事件是系统启动的，则监控最后一次成功运行。

计费的使用情况跟踪

您可以随时间转移监控您的使用情况趋势，以便：

- 告知预算计划和业务扩展估计值。
- 确定潜在的成本节约机会，例如删除冷数据。

您无法使用 Amazon Redshift Serverless 查询 STL、STV、SVCS、SVL 以及某些 SVV 系统表和视图，但以下情况除外：

- SVV_ALL_COLUMNS
- SVV_ALL_SCHEMAS
- SVV_ALL_TABLES
- SVV_COLUMNS
- SVV_DATASHARES
- SVV_DATASHARE_CONSUMERS
- SVV_DATASHARE_OBJECTS
- SVV_EXTERNAL_COLUMNS
- SVV_EXTERNAL_DATABASES
- SVV_EXTERNAL_PARTITIONS
- SVV_EXTERNAL_SCHEMAS
- SVV_EXTERNAL_TABLES
- SVV_REDSHIFT_COLUMNS
- SVV_REDSHIFT_DATABASES
- SVV_REDSHIFT_FUNCTIONS
- SVV_REDSHIFT_SCHEMAS
- SVV_REDSHIFT_TABLES
- SVV_TABLES
- SVV_TABLE_INFO
- SVV_TRANSACTIONS

您可以查询以下 SYS 系统视图，以监控 Amazon Redshift Serverless。

- SYS_QUERY_HISTORY
- SYS_QUERY_DETAIL
- SYS_EXTERNAL_QUERY_DETAIL
- SYS_LOAD_HISTORY
- SYS_LOAD_ERROR_DETAIL
- SYS_UNLOAD_HISTORY
- SYS_SERVERLESS_USAGE

Amazon Redshift Serverless 事件通知

使用 Amazon EventBridge 发送事件通知

Amazon Redshift Serverless 使用 Amazon EventBridge 管理事件通知，以便随时了解数据仓库中的更改。Amazon EventBridge 是一种无服务器事件总线服务，让您可以轻松地将应用程序与来自各种源的数据相连接。在这种情况下，事件源是 Amazon Redshift。事件（在环境中监控到的变化）将从您的 Amazon Redshift 数据仓库自动发送到 EventBridge。事件将近乎实时地进行传输。

EventBridge 的功能包括为您编写事件规则提供一个环境，这些规则可以指定针对特定事件采取的操作。您还可以设置目标，这些目标是 EventBridge 可以向其发送事件的资源。目标可以包括 API 目标、Amazon CloudWatch 日志组等。有关规则的更多信息，请参阅 Amazon EventBridge 规则。有关目标的更多信息，请参阅 Amazon EventBridge 目标。

事件可以按严重性和类别分类。提供以下筛选条件：

- 资源筛选：接收基于与事件关联的资源的消息。资源包括工作组、快照等。
- 时间窗口筛选：确定特定时间段内事件的范围。
- 类别筛选：接收指定类别中所有事件的事件通知。

下表包括 Amazon Redshift Serverless 事件以及其他元数据：

Amazon Redshift 类别	外部事件 ID	事件严重性	消息描述
RateChange	REDSHIFT-SERVERLESS-EVENT-1001	INFO	工作组基础 RPU 更改已于 <time in UTC> 成功完成。
RateChange	REDSHIFT-SERVERLESS-EVENT-1002	ERROR (错误)	工作组基础 RPU 更改已于 <time in UTC> 失败。
监控	REDSHIFT-SERVERLESS-EVENT-1003	INFO	该软件已于 <time in UTC> 在您的 Amazon Redshift 数据仓库 <endpoint name> 上更新。
监控	REDSHIFT-SERVERLESS-EVENT-1500	ERROR (错误)	无法创建或更新工作组 <workgroup name>，因为您已超出账户的弹性 IP 地址限制。请删除未使用的弹性 IP 地址，或者使用 Amazon EC2 请求提高限制。
监控	REDSHIFT-SERVERLESS-EVENT-1501	ERROR (错误)	子网 <subnet id> 没有可用的 IP 地址。这将阻止以下查询类型在工作组 <workgroup name> 中成功运行：EMR、联合查询、来自 Amazon EC2 的 COPY/UNLOAD。要解决该问

Amazon Redshift 类别	外部事件 ID	事件严重性	消息描述
			题，请通过删除 ENI 来释放您的子网中的 IP。
监控	REDSHIFT-SERVERLESS-EVENT-1502	ERROR (错误)	子网 <subnet id> 没有可用的 IP 地址。这将阻止 Amazon EMR、Redshift 联合查询、Redshift COPY/UNLOAD、Redshift ML 查询类型在工作组 <workgroup name> 中成功运行。要解决该问题，请通过删除未使用的弹性网络接口 (ENI) 来释放您的子网中的 IP。
管理	REDSHIFT-SERVERLESS-EVENT-1008	INFO	您的 Amazon Redshift 工作组 <workgroup name> 已创建，并且随时可用。
管理	REDSHIFT-SERVERLESS-EVENT-1009	INFO	您的 Amazon Redshift 工作组 <workgroup name> 已于 <time in UTC> 删除。
监控	REDSHIFT-SERVERLESS-EVENT-1000	INFO	快照 <snapshot name> 已于 <time in UTC> 成功完成。
管理	REDSHIFT-SERVERLESS-EVENT-1004	INFO	从命名空间 <namespace name> 上的快照还原已于 <time in UTC> 成功完成。
管理	REDSHIFT-SERVERLESS-EVENT-1005	ERROR (错误)	从命名空间 <namespace name> 上的快照还原已于 <time in UTC> 失败。
管理	REDSHIFT-SERVERLESS-EVENT-1006	INFO	从命名空间 <namespace name> 上的恢复点还原已于 <time in UTC> 成功完成。
管理	REDSHIFT-SERVERLESS-EVENT-1007	INFO	从命名空间 <namespace name> 上的恢复点还原已于 <time in UTC> 失败。

管理 Amazon Redshift Serverless 告警

您在 Amazon Redshift Serverless 控制台中创建的告警是 CloudWatch 告警。通过跟踪 Amazon Redshift Serverless 的审计日志记录 (p. 40) 中列出的任何指标，它们可以帮助您就无服务器命名空间、工作组和数据库做出主动决策。

例如，您可以为高 `DatabaseConnections` 设置一个告警，以查看工作组何时经历高负载；或为高 `DataStorage` 设置一个告警，以便跟踪命名空间用于数据的存储空间。

您可以编辑或删除使用 Alarms（告警）页面中的 Actions（操作）下拉列表创建的告警。您还可以创建 Slack 或 Amazon Chime 提示，以通过指定 Slack 或 Amazon Chime Webhook URL 将提示从 CloudWatch 发送到 Slack 或 Amazon Chime。

您可使用 CloudWatch 控制台、Amazon Redshift Serverless 控制台或您用于处理指标的任何其他方法（如 Amazon CLI 或 Amazon 开发工具包）创建告警。

使用 Amazon Redshift Serverless 控制台创建 CloudWatch 告警

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 选择控制面板右上角的 Go to Serverless（转到无服务器）。
3. 在导航菜单中，选择 Alarms（告警），然后选择 Create alarm（创建告警）。
4. 在 Create alarm（创建告警）页面上，输入相应属性以创建 CloudWatch 告警。
5. 选择Create alarm（创建警报）。

Amazon Redshift Serverless 的审计日志记录

导出日志

您可以配置 Amazon Redshift Serverless，以将连接、用户和用户活动日志数据导出到 Amazon CloudWatch Logs 中的日志组。利用 Amazon CloudWatch Logs 可以对日志数据进行实时分析，并使用 CloudWatch 创建告警和查看指标。您可使用 CloudWatch Logs 在持久性存储中存储日志记录。

要将生成的日志数据导出到 Amazon CloudWatch Logs，必须在控制台上的 Amazon Redshift Serverless 配置设置中选择要导出的相应日志。

在 CloudWatch 中监控日志事件

在选择要导出的 Redshift 日志后，您可以在 Amazon CloudWatch Logs 中监控事件。将使用以下前缀为 Amazon Redshift Serverless 自动创建新的日志组，其中 `log_type` 表示日志类型。

```
/aws/redshift/serverless/<log_type>
```

例如，如果您选择导出连接日志，则日志数据将存储在以下日志组中。

```
/aws/redshift/serverless/connectionlog
```

使用无服务器日志流将日志事件导出到日志组。该行为取决于以下哪些条件为真：

- 存在包含指定名称的日志组。Redshift 使用现有日志组导出日志数据。您可以使用自动化配置，例如由 Amazon CloudFormation 提供的配置，创建具有预定义日志保留期、指标筛选条件和客户访问的日志组。
- 具有指定名称的日志组不存在。当在实例的日志中检测到匹配的日志条目时，Amazon Redshift Serverless 会自动在 Amazon CloudWatch Logs 中创建一个新的日志组。日志组使用 Never Expire（永不过期）的默

认日志保留期。要更改日志保留期，请使用 Amazon CloudWatch Logs 控制台、Amazon CLI 或 Amazon CloudWatch Logs API。有关在 CloudWatch Logs 中更改日志留存期的更多信息，请参阅使用日志组和日志流中的更改日志数据留存。

要在日志事件中搜索信息，请使用 Amazon CloudWatch Logs 控制台、Amazon CLI 或 Amazon CloudWatch Logs API。有关搜索和筛选日志数据的更多信息，请参阅搜索和筛选日志数据。

Amazon Redshift Serverless 指标

Amazon Redshift Serverless 指标分为计算指标以及数据和存储指标，分别属于工作组和命名空间维度集。有关工作组和命名空间的更多信息，请参阅 Amazon Redshift Serverless 工作组和命名空间概览。

CloudWatch 计算指标如下所示：

CloudWatch 计算指标

指标名称	单位	描述	维度集
QueriesCompletedPerSecond	查询数	每秒完成的查询数。	{Database、LatencyRange、Workgro {LatencyRange、Workgroup}
QueryDuration	微秒	完成查询的平均时间量。	{Database、LatencyRange、Workgro {LatencyRange、Workgroup}
QueriesRunning	查询数	一个时间点运行的查询数。	{Database、QueryType、Workgroup} {QueryType、Workgroup}
QueriesQueued	查询数	某个时间点在队列中的查询数。	{Database、QueryType、Workgroup} {QueryType、Workgroup}
DatabaseConnections	连接数	一个时间点与数据库的连接数。	{Database、Workgroup}， {Workgroup}
QueryRuntimeBreakdown	毫秒	查询在各个查询阶段运行所花费的总时间。	{Database、Stage、Workgroup}， {Stage、Workgroup}
ComputeCapacity	RPU	过去 30 分钟内分配的平均计算单位数，向上舍入到最近的整数。	{Workgroup}
ComputeSeconds	RPU 秒	过去 30 分钟内消耗的累计计算单位秒数。	{Workgroup}
QueriesSucceeded	查询数	过去 5 分钟内成功的查询数。	{Database、QueryType、Workgroup} {QueryType、Workgroup}
QueriesFailed	查询数	过去 5 分钟内失败的查询数。	{Database、QueryType、Workgroup} {QueryType、Workgroup}
UsageLimitAvailable	RPU 小时或 TB	根据 UsageType，UsageLimitAvailable 将返回以下内容： • 如果 UsageType 为 SERVERLESS_COMPUTE，	{UsageLimitId、UsageType、Workgro

指标名称	单位	描述	维度集
		则 UsageLimitAvailable 将返回工作组可以在给定限制内查询的剩余 RPU 小时数。 • 如果 UsageType 是 CROSS-REGION-DATASHARING，则 UsageLimitAvailable 将返回客户可以在给定限制内扫描的剩余 TB 数量。	
`UsageLimitConsumed`	RPU 小时或 TB	根据 UsageType，UsageLimitConsumed 会返回以下内容： • 如果 UsageType 为 SERVERLESS_COMPUTE，则 UsageLimitConsumed 将返回工作组在给定限制内已查询的 RPU 小时数。 • 如果 UsageType 是 CROSS-REGION-DATASHARING，则 UsageLimitConsumed 将返回客户在给定限制内已经用于扫描的 TB 数量。	{UsageLimitId、UsageType、Workgro

CloudWatch 数据和存储指标如下所示：

CloudWatch 数据和存储指标

指标名称	单位	描述	维度集
`TotalTableCount`	表的数量	在特定时间点存在的用户表的数量。此总数不包括 Amazon Redshift Spectrum 表。	{Database、Namespace}

指标名称	单位	描述	维度集
DataStorage	兆字节	在磁盘或存储空间中用于 Redshift 数据的兆字节数。	{Namespace}

SnapshotStorage 指标与命名空间和工作组无关。CloudWatch 的 SnapshotStorage 指标如下所示：

CloudWatch SnapshotStorage 指标

指标名称	单位	描述	维度集
SnapshotStorage	兆字节	在磁盘或存储空间中用于快照的兆字节数。	{}

维度集是应用于指标的分组维度。您可以使用这些维度组来指定如何检索统计数据。

下表详细说明了特定指标的维度和维度值：

CloudWatch 维度和维度值

维度	描述和值
DatabaseName	数据库的名称。自定义值。
Latency	可能值如下所示： • Short– 不到 10 秒 • Medium – 在 10 秒到 10 分钟之间 • Long – 超过 10 分钟
QueryType	可能的值为 INSERT、DELETE、UPDATE、UNLOAD、LOAD、SELECT、CTAS 和 OTHER。
stage	查询的执行阶段。可能值如下所示： • QueryPlanning：分析和优化 SQL 语句所花的时间。 • QueryWaiting：在 WLM 队列中等待所花的时间。 • QueryExecutingRead：执行读取查询所花的时间。 • QueryExecutingInsert：执行插入查询所花的时间。 • QueryExecutingDelete：执行删除查询所花的时间。 • QueryExecutingUpdate：执行更新查询所花的时间。 • QueryExecutingCtas：执行 create table as 查询所花的时间。 • QueryExecutingUnload：执行卸载查询所花的时间。

维度	描述和值
	• QueryExecutingCopy：执行复制查询所花的时间。 • QueryCommit：提交所花的时间。
`Namespace`	命名空间的名称。自定义值。
`Workgroup`	工作组的名称。自定义值。
`UsageLimitId`	使用限制的标识符。
`UsageType`	受限制的 Amazon Redshift Serverless 功能。可能值如下所示： • SERVERLESS_COMPUTE • CROSS_REGION_DATASHARING

使用快照和恢复点

使用快照和恢复点

无服务器快照包括命名空间内的所有对象和数据。您可以在以下三种情况下还原快照：

- 将无服务器快照还原到无服务器命名空间。
- 将无服务器快照还原到预置集群。
- 将预置集群快照还原到无服务器命名空间。

您可以将在 Amazon Redshift Serverless 控制台上创建的快照还原到预置 Amazon Redshift 集群。执行此操作时，您可以选择要使用的节点类型（例如 RA3）和节点数量，以便您在集群或节点级别控制设置。要启动还原，您可以从 Amazon Redshift Serverless 控制台中选择快照，然后指定要还原到的预置集群的 ID。要将预置的集群快照还原到无服务器命名空间，请从 Redshift 预置的控制台开始，选择要还原的快照，然后选择 Restore from snapshot（从快照还原）、Restore to serverless namespace（恢复到无服务器命名空间）。

将快照还原到无服务器命名空间，会将数据库替换为快照中的数据库。您还可以将恢复点（每 30 分钟创建一次并保留 24 小时）还原到无服务器命名空间。

要将预置的集群快照还原到无服务器命名空间，请导航到 Redshift 预置控制台。

将快照还原到无服务器命名空间分两个阶段完成。第一阶段在几分钟内完成，将数据还原到命名空间，并使其可用于查询。还原的第二阶段是优化数据库，这可能会导致轻微的性能问题。第二阶段可持续几个小时到几天，在某些情况下可持续几周。时间量取决于数据大小，但随着数据库进行优化，性能会逐步提高。在此阶段结束时，您的无服务器命名空间已充分优化，您可在没有性能问题的情况下提交查询。

最后，您还可以与其他 Amazon 账户共享快照，允许他们访问快照中的数据并运行查询。

您可以通过查看 Amazon Redshift Serverless 控制台中的详细信息页面，或者通过调用 Amazon Redshift Serverless API 操作 `ListSnapshots` 或 Amazon CLI 中的 `list-snapshots` 操作，来查看快照的详细信息。Amazon Redshift Serverless 控制台还包含恢复点的详细信息页面，或者您也可以调用 Amazon CLI 中的 `list-recovery-points` 或 `ListRecoveryPoints` API 操作。

快照

您可以将在 Amazon Redshift Serverless 控制台上创建的快照还原到与工作组关联的可用命名空间。命名空间一旦准备好进行查询和/或修改，就可以使用了。您可以将使用 Amazon 托管式 KMS 密钥加密的快照还原到无服务器命名空间。

要查看所有快照的列表，请在 Amazon Redshift Serverless 控制台上，选择 Data backup（数据备份）。

要创建快照

1. 在 Amazon Redshift Serverless 控制台上，选择 Data backup（数据备份）。
2. 选择 Create snapshot (创建快照)。
3. 选择要创建其快照的命名空间。
4. 输入快照标识符。
5. （可选）选择保留期。如果您选择 Custom value（自定义值），请选择天数。您选择的数值必须在 1-3653（含）天之间。原定设置值是无限期保留。
6. 选择 Create (创建) 。

从命名空间配置创建快照

1. 在 Amazon Redshift Serverless 控制台上，选择 Namespace configuration（命名空间配置）。
2. 选择要创建其快照的命名空间。您只能创建与工作组关联且其状态为“可用”的命名空间的快照。
3. 选择 Data backup（数据备份）选项卡。
4. 选择 Create snapshot (创建快照)。
5. 输入快照标识符。
6. （可选）选择保留期。如果您选择 Custom value（自定义值），请选择天数。您选择的数值必须在 1-3653（含）天之间。
7. 选择 Create (创建) 。

将快照还原到无服务器命名空间

1. 在 Amazon Redshift Serverless 控制台上，选择 Data backup（数据备份）。
2. 选择要还原的快照。一次只能还原一个快照。
3. 依次选择 Actions（操作）和 Restore to serverless namespace（恢复到无服务器命名空间）。
4. 选择要还原到的可用命名空间。只能还原到其状态为“可用”的命名空间。
5. 选择 Restore（还原）。

将快照还原到预置集群

1. 在 Amazon Redshift Serverless 控制台上，选择 Data backup（数据备份）。
2. 选择要还原的快照。
3. 依次选择 Action（操作）和 Restore to provisioned cluster（还原到预置集群）。
4. 输入集群标识符。
5. 选择 Node type（节点类型）。节点的数量取决于节点类型。
6. 按照控制台页面上的说明进行操作，为 Cluster configuration（集群配置）输入属性。有关更多信息，请参阅创建集群。

更新快照的保留期

1. 在 Amazon Redshift Serverless 控制台上，选择 Data backup（数据备份）。
2. 选择要更新的快照。
3. 依次选择 Actions（操作）和 Set manual snapshot settings（设置手动快照设置）。
4. 选择保留期。如果您选择 Custom value（自定义值），请选择天数。
5. 选择保存更改。

如何删除快照

1. 在 Amazon Redshift Serverless 控制台上，选择 Data backup（数据备份）。
2. 选择要删除的快照。
3. 依次选择 Actions 和 Delete。
4. 选择 Delete（删除）。

在删除命名空间之前创建命名空间内所有数据的最终快照。

1. 在 Amazon Redshift Serverless 控制台上，选择 Namespace configuration（命名空间配置）。
2. 选择要删除的命名空间。
3. 依次选择 Actions（操作） 和 Delete（删除）。
4. 选择 Create final snapshot（创建最终快照）。
5. 输入快照的名称。
6. 输入 delete。
7. 选择 Delete（删除）。

与另一个 Amazon 账户共享快照

1. 在 Amazon Redshift Serverless 控制台上，选择 Data backup（数据备份）。
2. 选择要共享的快照。
3. 依次选择 Action（操作）和 Manage access（管理访问）。
4. 输入 Amazon Web Services 账户 ID。
5. 选择保存更改。

有关预置集群快照的更多信息，请参阅《Amazon Redshift 集群管理指南》中的 Amazon Redshift 快照。

恢复点

Amazon Redshift Serverless 中的恢复点每 30 分钟创建一次，并保存 24 小时。

在 Amazon Redshift Serverless 控制台上，选择 Data backup（数据备份）来管理恢复点。您还可以进行以下操作：

- 将恢复点还原到无服务器命名空间。
- 将恢复点转换为快照。

将恢复点还原到无服务器命名空间

1. 在 Amazon Redshift Serverless 控制台上，选择 Data backup（数据备份）。
2. 在 Recovery points（恢复点）下，选择要还原的恢复点的 Creation time（创建时间）。
3. 选择 Restore（还原）。只能还原到其状态为“可用”的命名空间。
4. 在文本输入字段中输入 restore（还原），然后选择 Restore（还原）。

将恢复点转换为快照

1. 在 Amazon Redshift Serverless 控制台上，选择 Data backup（数据备份）。
2. 在 Recovery points（恢复点）下，选择要转换为快照的恢复点的 Creation time（创建时间）。
3. 选择 Create snapshot from recovery point（从恢复点创建快照）。

4. 输入 Snapshot identifier（快照标识符）。
5. 选择 Create (创建) 。

使用 Amazon Command Line Interface 和 Amazon Redshift Serverless API 管理快照和恢复点

除了使用 Amazon 控制台，您还可以使用 Amazon CLI 或 Amazon Redshift Serverless API 与快照和恢复点进行交互。

要创建快照，请使用 Amazon Command Line Interface 操作 create-snapshot。还可以使用 Amazon Redshift Serverless API 操作 `CreateSnapshot`。快照必须与命名空间关联，因此您必须在请求中包含命名空间的名称。原定设置情况下，Amazon Redshift Serverless 无限期地保留快照，但您可以在请求中指定保留期。

要还原快照，请使用 `restore-from-snapshot` 或 `RestoreFromSnapshot`。如果要将快照从 Amazon Redshift Serverless 还原到预调配集群，则必须指定要还原的快照的 `snapshotArn`。否则，如果您要从无服务器还原到无服务器，则可以指定 `snapshotArn` 或 `snapshotName`，但不能同时指定两者。

要检索有关快照的信息，例如它与哪个命名空间关联或快照中的数据有多大，请使用 Amazon CLI 操作 `get-snapshot`。或者，也可以使用 API 操作 `GetSnapshot`。要同时获取有关多个快照的信息，请使用 `list-snapshots` 或 `ListSnapshots`。

要删除快照，请使用 CLI 操作 `delete-snapshot` 或 API 操作 `DeleteSnapshot`。

恢复点由 Amazon Redshift Serverless 自动创建，因此您无法使用 Amazon CLI 或 API 操作来创建恢复点。您可以使用 `restore-from-recovery-point` 或 `RestoreFromRecoveryPoint` 将恢复点内的数据还原到命名空间，就像从快照还原数据一样。还可以使用 `convert-recovery-point-to-snapshot` 或 `ConvertRecoveryPointToSnapshot` 将恢复点转换为快照。

要查看有关特定恢复点的信息，请使用 `get-recovery-point` 或 `GetRecoveryPoint`。要检索有关多个恢复点的信息，请使用 `list-recovery-points` 或 `ListRecoveryPoints`。

Amazon Redshift Serverless 中的数据共享

当数据共享 在 Amazon Redshift Serverless 中更新时，使用它共享最新和一致的信息。

Amazon Redshift Serverless 中的数据共享

通过数据共享，您可以实时访问数据，以便您的用户可以在 Amazon Redshift Serverless 中查看更新后的最新、最一致的信息。

在 Amazon Redshift Serverless 中共享数据入门

您可以在 Amazon Web Services 账户中或跨这些账户，在不同 Amazon Redshift Serverless 实例之间共享数据以进行读取。

您可以使用 SQL 界面或 Amazon Redshift 控制台开始使用数据共享。有关更多信息，请参阅使用 SQL 界面开始共享数据或通过控制台开始使用数据共享，其位于《Amazon Redshift 数据库开发人员指南》的《Amazon Redshift 数据库开发人员指南》中。

在 Amazon Web Services 账户中，您可以将数据从 Amazon Redshift Serverless 共享到另一个实例，从预置集群共享到 Amazon Redshift Serverless，或从 Amazon Redshift Serverless 共享到预置集群，以用于读取目的。有关使用 SQL 接口在 Amazon Web Services 账户 中共享数据的信息，请参阅《Amazon Redshift 数据库开发人员指南》中的在 Amazon Web Services 账户 中共享数据。

跨 Amazon Web Services 账户，您可以将数据从 Amazon Redshift Serverless 共享到另一个实例，从预置集群共享到 Amazon Redshift Serverless，或从 Amazon Redshift Serverless 共享到预置集群，以用于读取目的。有关跨 Amazon Web Services 账户 数据共享的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的跨 Amazon Web Services 账户 共享数据。

要在 Amazon Web Services 账户 中开始共享数据，请打开 Amazon Web Services Management Console，然后选择 Amazon Redshift 控制台。选择 Namespace configuration（命名空间配置），然后选择 Datashares（数据共享）。按照《Amazon Redshift 数据库开发人员指南》中的使用控制台开始数据共享中的步骤进行操作。

要开始跨 Amazon Web Services 账户 共享数据，请打开 Amazon Web Services Management Console，然后选择 Amazon Redshift 控制台。选择 Datashares（数据共享）。按照《Amazon Redshift 数据库开发人员指南》中的使用控制台开始数据共享中的步骤进行操作。

要开始在数据共享中查询数据，请在具有关联工作组的命名空间中创建一个数据库。从指定的数据共享中，选择具有关联工作组的命名空间，然后创建数据库来查询数据。按照通过数据共享创建数据库中的过程操作。

Amazon Redshift Serverless 中的数据共享注意事项

以下是使用 Amazon Redshift Serverless 中的数据共享时的注意事项：

- 与预置集群共享数据时，Amazon Redshift 仅支持生产者和使用者集群的 ra3.16xlarge、ra3.4xlarge 和 ra3.xlplus 实例类型上的数据共享。
- 原定设置情况下，Amazon Redshift Serverless 会加密。

有关数据共享限制的列表，请参阅《Amazon Redshift 数据库开发人员指南》中的数据共享的限制。

为资源添加标签

为资源添加标签概览

在 Amazon 中，标签是用户定义的标记，由键-值对组成。Amazon Redshift Serverless 支持添加标签，以便一目了然地提供有关资源的元数据。

虽然标签对资源来说并非必不可少，但它们却有助于提供上下文信息。您可能想使用与资源相关的信息，通过元数据来为资源添加标签。例如，假设您要跟踪属于测试环境和生产环境的资源。您可以创建名为 environment 的键并提供值 test 或 production，以确定在每种环境中使用的资源。如果您在其他 Amazon 服务中使用了标签或者具有针对您业务的标准类别，那么，我们建议您为资源创建相同的键值对以保持一致性。

如果删除资源，则会删除所有关联的标签。目前，您只能使用 Amazon CLI 为无服务器资源添加标签。可用的操作包括 `TagResource`、`UntagResource` 和 `ListTagsForResource`。一旦创建了标签，就不能更新它。

每个资源都有一个标签集，它是分配给该资源的一个或多个标签的集合。每个资源的每个标签集内最多有 50 个标签。您可以在创建资源时以及资源创建完成后添加标签。您可以向以下无服务器资源类型添加标签：

- 工作组
- 命名空间

标签具有以下要求：

- 键不得以 `aws:` 作为前缀。

- 每个标签集中的各个键必须是独一无二的。
- 键的长度必须介于 1 到 128 个允许的字符之间。
- 值的长度必须介于 0 到 256 个允许的字符之间。
- 每个标签集中的值不需要是唯一的。
- 可以用作键和值的字符包括 Unicode 字符、数字、空格及以下符号：_ . : / = + - @。
- 键和值区分大小写。

使用 Amazon Redshift Serverless 时的注意事项

有关提供了 Amazon Redshift Serverless 的 Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中针对 Redshift Serverless API 列出的端点。

Amazon Redshift Serverless 使用的某些资源受限于配额。有关更多信息，请参阅Amazon Redshift Serverless 对象的配额 (p. 517)。

当您 DECLARE（声明）游标时，将在 DECLARE 中指定 Amazon Redshift Serverless 的结果集大小规范。

维护时段 - Amazon Redshift Serverless 没有维护时段。软件版本更新将自动应用。当 Amazon Redshift 切换版本时，现有连接或查询执行不会中断。新连接将始终立即与 Amazon Redshift Serverless 连接和发挥作用。

AQUA – Amazon Redshift Serverless 不支持适用于 Amazon Redshift 的 AQUA（高级查询加速器）。

可用区 ID – 在配置 Amazon Redshift Serverless 实例时，打开 Additional considerations（其他考虑事项），确保 Subnet（子网）中提供的子网 ID 至少包含三个受支持的可用区 ID。要查看子网到可用区 ID 映射，请转到 VPC 控制台并选择 Subnets（子网），以通过可用区 ID 来查看子网 ID 列表。验证您的子网已映射到受支持的可用区 ID。要创建子网，请参阅《Amazon VPC 用户指南》中的在 VPC 中创建子网。

三个子网 - 您必须至少有三个子网，并且这些子网必须跨三个可用区。例如，您可以使用三个子网。这些子网将映射到可用区 us-east-1a、us-east-1b 和 us-east-1c。

迁移后的存储空间 – 如果将小型 Amazon Redshift 预调配集群迁移到 Amazon Redshift Serverless，则在迁移后，您可能会发现分配的存储空间已增大。这是优化的存储空间分配的结果，从而产生了预分配的存储空间。随着 Amazon Redshift Serverless 中数据的增长，此空间将在一段时间内使用。

Amazon Redshift Serverless 和 Amazon Redshift 预调配集群之间的数据共享 - 在 Amazon Redshift Server 作为创建者且预调配集群作为使用者的数据共享中，预调配集群必须具有高于 1.0.38214 的集群版本。如果您使用的集群版本低于此值，则运行查询时会出错。您可以在 Amazon Redshift 控制台上的 Maintenance（维护）选项卡中查看集群版本。您也可以运行 `SELECT version();`。

最大查询执行时间：查询已用的执行时间（以秒为单位）。执行时间不包括在队列中等待的时间。如果查询超出设置的执行时间，Amazon Redshift Serverless 将停止查询。有效值为 0–86,399。

Amazon Redshift 集群

在以下部分中，您可以通过启动一组计算节点（称为 Amazon Redshift 集群）了解创建数据仓库的基础知识。

主题

- Amazon Redshift 集群概览 (p. 50)
- 在创建集群时使用 EC2-VPC (p. 54)
- RA3 节点类型概述 (p. 55)
- 升级到 RA3 节点类型 (p. 57)
- 从 DC1 节点类型升级到 DC2 节点类型 (p. 59)
- 将 EC2-Classic 上的 DS2 集群升级为 EC2-VPC (p. 60)
- 区域和可用区注意事项 (p. 60)
- 集群维护 (p. 60)
- 默认磁盘空间警报 (p. 64)
- 集群状态 (p. 64)
- Amazon Redshift 中的集群管理概览 (p. 65)
- 使用 AQUA（高级查询加速器） (p. 74)
- 管理 Amazon Redshift 中的使用限制 (p. 77)
- 在 Amazon Redshift 中管理集群重新定位 (p. 78)
- 在 Amazon Redshift 中使用 Redshift 托管的 VPC 终端节点 (p. 81)
- 使用控制台管理集群 (p. 83)
- 使用 Amazon CLI 和 Amazon Redshift API 管理集群 (p. 89)
- 使用 Amazon SDK for Java 管理集群 (p. 90)
- 在 VPC 中管理集群 (p. 92)
- 集群版本历史记录 (p. 98)

Amazon Redshift 集群概览

Amazon Redshift 数据仓库是一个由称作节点的各种计算资源构成的集合，这些节点已整理到名为集群的组中。每个集群运行一个 Amazon Redshift 引擎并包含一个或多个数据库。

Note

目前提供 Amazon Redshift 版本 1.0 引擎。不过，随着引擎不断更新，我们可能会提供多个 Amazon Redshift 引擎版本供您选择。

Amazon Redshift 中的集群和节点

Amazon Redshift 集群由节点组成。每个集群包括一个领导节点以及一个或多个计算节点。领导节点接收来自客户端应用程序的查询、解析查询并制定查询执行计划。然后，领导节点和计算节点协调这些计划并行执行，之后，领导节点聚合来自计算节点的中间结果。然后，领导节点会将这些结果最终返回至客户端应用程序。

Compute nodes（计算节点）运行查询执行计划，并在节点自身之间传输数据以对这些查询提供服务。中间结果被送回至客户端应用程序之前，会先发送至领导节点进行聚合。有关领导节点和计算节点的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的数据仓库系统架构。

Note

当您在 Amazon Redshift 控制台 (https://console.aws.amazon.com/redshift/) 上创建集群时，您可以获得基于数据大小和查询特征的集群配置建议。要使用此大小调整计算器，请查找在支持 RA3 节点类型的 Amazon 区域中在控制台上查找 Help me choose（帮我选择）。有关更多信息，请参阅创建集群 (p. 84)。

当您启动集群时，您指定的一个选项是节点类型。节点类型决定了每个节点的 CPU、RAM、存储容量和存储驱动类型。

Amazon Redshift 提供不同的节点类型以满足您的工作负载要求，我们建议根据所需的性能、数据大小和预期数据增长选择 RA3 或 DC2。

通过使用具有托管存储的 RA3 节点，您可以单独扩展和支付计算和托管存储以优化数据仓库。通过使用 RA3，您可以根据性能要求选择节点数，并且仅为您使用的托管存储支付费用。根据您每天处理的数据量调整 RA3 集群大小。您可以在 Virtual Private Cloud (VPC) 中启动使用 RA3 节点类型的集群。您无法在 EC2-Classic 中启动 RA3 集群。有关更多信息，请参阅在 VPC 中创建集群 (p. 93)。

Amazon Redshift 托管存储在每个 RA3 节点中使用大型高性能 SSD 以提供快速的本地存储，并使用 Simple Storage Service（Amazon S3）提供更长时间的持久存储。如果节点中的数据超过大型本地 SSD 的大小，Amazon Redshift 托管存储自动将该数据分流到Simple Storage Service（Amazon S3）。无论数据存储在高性能 SSD 还是 Simple Storage Service（Amazon S3）中，Amazon Redshift 托管存储采用相同的费率，而且费用较低。对于需要不断增长的存储的工作负载，您可以通过托管存储自动扩展数据仓库存储容量，而不添加额外节点和支付费用。

通过使用 DC2 节点，您可以创建包含本地 SSD 存储的计算密集型数据仓库。您可以根据数据大小和性能要求选择所需的节点数。DC2 节点在本地存储数据以获得较高的性能；随着数据大小增长，您可以添加更多计算节点以增加集群的存储容量。对于 1 TB 以下的数据集（压缩），我们建议使用 DC2 节点类型，从而以最低的价格获得最佳的性能。如果预计数据将会增长，我们建议您使用 RA3 节点，以便单独调整计算和存储大小以降低价格并提高性能。您可以在 Virtual Private Cloud (VPC) 中启动使用 DC2 节点类型的集群。您无法在 EC2-Classic 中启动 DC2 集群。有关更多信息，请参阅在 VPC 中创建集群 (p. 93)。

通过使用 DS2 节点，您可以使用硬盘驱动器 (HDD) 创建大型数据仓库，我们建议您改用 RA3 节点。如果您使用 DS2 节点，请参阅升级到 RA3 节点类型 (p. 57)以了解升级准则。如果使用 8 个或更多 ds2.xlarge 节点或任意数量的 ds2.8xlarge 节点，您现在可以升级到 RA3，从而以相同的按需成本获得 2 倍的存储和更高的性能。

节点类型有各种不同的大小。节点大小和节点数决定了集群的总存储容量。有关更多信息，请参阅节点类型详细信息 (p. 51)。

一些节点类型允许一个节点（单节点）或者两个/更多节点（多节点）。某些节点类型的集群的最小节点数为两个节点。在单节点集群上，该节点由领导功能和计算功能共用。不建议使用单节点集群运行生产工作负载。在多节点集群上，领导节点与计算节点是分开的。领导节点与计算节点的节点类型相同。您仅需为计算节点付费。

Amazon Redshift 为每个 Amazon 区域内的每个 Amazon 账户应用资源配额。配额限制您的账户可以在 Amazon 区域中为给定资源类型（如节点或快照）创建的资源数。有关适用于 Amazon Redshift 资源的默认配额的更多信息，请参阅 Amazon Web Services 一般参考中的 Amazon Redshift 限制。要申请增加限制，请提交 Amazon Redshift 限制增加表单。

您的集群成本取决于 Amazon 区域、节点类型、节点数以及是否提前预留节点。有关节点成本的更多信息，请参阅 Amazon Redshift 定价页面。

节点类型详细信息

以下各表总结了每个节点类型和大小的节点规范。表中的标题具有以下含义：

- vCPU 指的是每个节点的虚拟 CPU 数。
- RAM 指的是每个节点的内存量，以吉字节 (GiB) 为单位。
- 每个节点的默认切片数 是指，在创建集群或使用经典调整大小调整集群大小时，将计算节点划分到的切片数。

  如果使用弹性调整大小来调整集群大小，则每个节点的切片数可能会发生变化。不过，在进行弹性调整大小后，集群中所有计算节点上的切片总数将保持不变。

  在使用从快照中还原操作创建集群时，如果更改节点类型，创建的集群的切片数可能与原始集群不同。
- 存储指的是每个节点的容量和存储类型。
- 节点范围指的是针对节点类型和大小，Amazon Redshift 支持的最少和最多节点数。

  Note

  根据应用到所选 Amazon 区域中您的 Amazon 账户的配额，您可能只能使用少量节点。要申请增加限制，请提交 Amazon Redshift 限制增加表单。
- 总容量指的是集群的总存储容量（如果您部署了节点范围中指定的最大数目的节点）。

R3 节点类型

节点类型	vCPU	RAM (GiB)	每个节点的默认切片数	每个节点的托管式存储限制 [1]	创建集群的节点范围	总托管式存储容量 [2]	
ra3.xlplus（单节点）	4	32	2	4 TB	1	4 TB[3]	
ra3.xlplus（多节点）	4	32	2	32 TB	2–16[4]	1024 TB[4]	
ra3.4xlarge	12	96	4	128 TB	2–32[5]	8192 TB[5]	
ra3.16xlarge	48	384	16	128 TB	2–128	16384 TB	

[1] Amazon Redshift 托管存储的存储限制。这是一个硬性限制。

[2] 总托管式存储限制是每个节点的最大节点数乘以托管式存储限制。

[3] 要将单节点集群的大小调整为多节点，只支持经典大小调整。

[4] 您可以创建一个最多包含 16 个节点的 ra3.xlplus（多节点）节点类型的集群。对于多节点集群，您可以使用弹性调整大小将大小调整为最多 32 个节点。

[5] 您可以使用最多包含 32 个节点的 ra3.4xlarge 节点类型创建一个集群。您可以通过弹性调整大小将大小调整为最多 64 个节点。

密集存储节点类型

节点类型	vCPU	RAM (GiB)	每个节点的默认切片数	每个节点的存储	节点范围	总容量	
ds2.xlarge	4	31	2	2TB HDD	1–32	64 TB	

节点类型	vCPU	RAM (GiB)	每个节点的默认切片数	每个节点的存储	节点范围	总容量	
ds2.8xlarge	36	244	16	16TB HDD	2–128	2PB	

密集计算节点类型

节点类型	vCPU	RAM (GiB)	每个节点的默认切片数	每个节点的存储	节点范围	总容量	
dc2.large	2	15	2	160 GB NVMe-SSD	1–32	5.12 TB	
dc2.8xlarge	32	244	16	2.56 TB NVMe-SSD	2–128	326 TB	
dc1.large[1]	2	15	2	160GB SSD	1–32	5.12 TB	
dc1.8xlarge[1]	32	244	32	2.56TB SSD	2–128	326 TB	

[1] 我们建议使用 DC2 节点类型，而不是 DC1 节点类型。有关如何升级的更多信息，请参阅从 DC1 节点类型升级到 DC2 节点类型 (p. 59)。

以前的节点类型名称

在先前的 Amazon Redshift 版本中，某些节点类型的名称不同。您可以在 Amazon Redshift API 和 Amazon CLI 中使用以前的名称。但是，我们建议您更新引用这些名称的所有脚本，以改用当前名称。当前名称和之前的名称如下所示。

当前名称	以前的名称
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

确定节点数

由于 Amazon Redshift 在集群的所有计算节点间并行分配和运行查询，因此您可以通过向集群添加节点来提高查询性能。在运行具有至少两个计算节点的集群时，每个节点上的数据将镜像到其他节点的磁盘上，从而降低数据丢失的风险。

您可以在 Amazon Redshift 控制台中使用 Amazon CloudWatch 指标监控查询性能。您还可以根据需要添加或删除节点，以便在集群的价格和性能之间达到平衡。当您请求额外节点时，Amazon Redshift 会处理部署、负载均衡和数据维护方面的所有详细信息。有关集群性能的更多信息，请参阅监控 Amazon Redshift 集群性能 (p. 472)。

预留节点适合状态稳定的生产工作负载，可以提供比按需节点大得多的折扣。在运行试验和概念验证以验证生产配置后，您可以购买预留节点。有关更多信息，请参阅购买 Amazon Redshift 预留节点 (p. 337)。

在暂停集群时，您可以在集群暂停期间暂停按需计费。在该暂停时间内，您仅需为备份存储付费。这可避免规划和购买超出需求的数据仓库容量，并使您能够经济高效地管理环境以进行开发或测试。

有关按需和预留节点定价的信息，请参阅 Amazon Redshift 定价。

在创建集群时使用 EC2-VPC

Amazon Redshift 集群在已针对您选择的 Amazon Redshift 节点类型和大小配置的 Amazon EC2 实例中运行。使用 EC2-VPC 创建集群。如果您仍在使用 EC2-Classic，我们建议您使用 EC2-VPC 以提高性能和安全性。有关这些联网平台的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的支持的平台。您的 Amazon 账户设置决定了您可以使用 EC2-VPC 还是 EC2-Classic。

Note

为了防止 SQL 客户端工具与 Amazon Redshift 数据库之间出现连接问题，建议执行下列两项操作之一。您可以配置一个允许主机协商数据包大小的入站规则。或者，您可以通过在 Amazon EC2 实例的网络接口 (NIC) 上将最大传输单位 (MTU) 设置为 1500 来禁用 TCP/IP 巨型帧。有关这些方法的更多信息，请参阅查询似乎挂起，有时无法连接到集群 (p. 266)。

EC2-VPC

在使用 EC2-VPC 时，集群在逻辑上与您的 Amazon 账户隔离的 Virtual Private Cloud (VPC) 中运行。如果您在 EC2-VPC 中预置集群，则可以将一个或多个 VPC 安全组与集群关联以控制对集群的访问。有关更多信息，请参阅 Amazon VPC 用户指南 中的您的 VPC 的安全组。

要在 VPC 中创建集群，您必须先通过提供 VPC 的子网信息来创建一个 Amazon Redshift 集群子网组，然后在启动集群时提供该子网组。有关更多信息，请参阅Amazon Redshift 集群子网组 (p. 95)。

有关 Amazon Virtual Private Cloud (Amazon VPC) 的更多信息，请参阅 Amazon VPC 产品详细信息页面。

EC2-Classic

EC2-Classic 平台将于 2022 年 8 月 15 日停用。我们建议您将集群从 EC2-Classic 平台移动到 EC2-VPC 平台。有关更多信息，请参阅 将 EC2-Classic 上的 DS2 集群升级为 EC2-VPC (p. 60) 和 EC2-Classic Networking is Retiring – Here's How to Prepare。

在 EC2-Classic 中，集群在一个与其他 Amazon 客户共享的扁平化网络中运行。如果您在 EC2-Classic 中预置集群，则可以将一个或多个 Amazon Redshift 集群安全组与集群关联以控制对集群的访问。有关更多信息，请参阅Amazon Redshift 集群安全组 (p. 458)。

启动集群

您的 Amazon 账户可以按区域启动 EC2-VPC 和 EC2-Classic 实例，或者仅启动 EC2-VPC 实例。要确定您的账户支持哪种网络平台并随后启动集群，请执行以下操作：

1. 确定要部署集群的 Amazon 区域。有关提供了 Amazon Redshift 的 Amazon 区域的列表，请参阅 Amazon Web Services 一般参考中的 Amazon Redshift 端点。
2. 找出您的账户在所选 Amazon 区域中支持的 Amazon EC2 平台。您可以在 Amazon EC2 控制台中找到这些信息。有关分步指导，请参阅 适用于 Linux 实例的 Amazon EC2 用户指南中的支持的平台。
3. 如果您的账户支持这两种平台，我们建议使用 EC2-VPC。如果您的账户仅支持 EC2-VPC，则必须在 VPC 中部署集群。

4. 启动 Amazon Redshift 集群。您可以使用 Amazon Redshift 控制台或使用 Amazon Redshift API、Amazon CLI 或开发工具包库创建集群。有关这些选项的更多信息以及相关文档的链接，请参阅什么是 Amazon Redshift？ (p. 1)。

RA3 节点类型概述

我们建议您将 DS2 节点类型集群上运行的现有工作负载升级到 RA3 节点类型，以利用提升的性能并获得更多的存储容量。RA3 节点具有以下优点：

- 它们可以灵活地增加计算容量，而不增加存储成本。此外，它们可以扩展存储，而不会超额预置计算容量。
- 它们使用高性能 SSD 存储热数据，并使用 Simple Storage Service（Amazon S3）存储冷数据。因此，它们提供了易用性、经济高效的存储以及较高的查询性能。
- 它们使用在 Amazon Nitro 系统上构建的高带宽联网，以进一步减少将数据卸载到 Simple Storage Service（Amazon S3）以及从中检索数据所花的时间。

在以下情况下，请考虑选择 RA3 节点类型：

- 您需要将计算与存储分开，以灵活地扩展和支付费用。
- 您查询的数据占总数据的一小部分。
- 数据量正在迅速增长，或者预计会迅速增长。
- 您希望仅根据性能需求灵活地调整集群大小。

要使用 RA3 节点类型，您的 Amazon 区域必须支持 RA3。有关更多信息，请参阅Amazon 区域中的 RA3 节点类型可用性 (p. 56)。

> Important
>
> 只能对集群版本 1.0.21262 或更高版本使用 ra3.xlplus 节点类型。您可以使用 Amazon Redshift 控制台查看现有集群的版本。有关更多信息，请参阅确定集群维护版本 (p. 63)。
> 请确保在使用 RA3 节点类型时使用新的 Amazon Redshift 控制台。
> 此外，要将 RA3 节点类型与使用维护跟踪的 Amazon Redshift 操作结合使用，必须将维护跟踪值设置为支持 RA3 的集群版本。有关维护跟踪的更多信息，请参阅选择集群维护跟踪 (p. 62)。

使用单节点 RA3 节点类型时，请考虑以下几点。

- 支持 AQUA。
- 支持数据共享创建者和使用者。
- 只支持经典调整大小来更改节点类型。不支持使用弹性调整大小或快照恢复来更改节点类型。以下方案均可支持：
  - 将 1 节点 ds2.xlarge 经典调整为 1 节点 ra3.xlplus，反之亦然。
  - 将 1 节点 ds2.xlarge 经典调整为多节点 ra3.xlplus，反之亦然。
  - 将多节点 ds2.xlarge 经典调整为 1 节点 ra3.xlplus，反之亦然。
  - 将 1 节点 dc2.xlarge 经典调整为 1 节点 ra3.xlplus，反之亦然。
  - 将 1 节点 dc2.xlarge 经典调整为多节点 ra3.xlplus，反之亦然。
  - 将多节点 dc2.xlarge 经典调整为 1 节点 ra3.xlplus，反之亦然。

使用 Amazon Redshift 托管存储

借助 Amazon Redshift 托管存储，您可以在 Amazon Redshift 中存储和处理所有数据，同时可以更灵活地分别扩展计算容量和存储容量。您继续使用 COPY 或 INSERT 命令接收数据。为了优化性能并管理跨各存储

层的自动数据放置，Amazon Redshift 利用诸如数据块温度、数据块使用期限和工作负载模式之类的优化功能。需要时，Amazon Redshift 自动将存储扩展到 Simple Storage Service（Amazon S3），而无需任何手动操作。

有关存储成本的信息，请参阅 Amazon Redshift 定价。

管理 RA3 节点类型

要利用将计算与存储分开的优势，您可以使用 RA3 节点类型创建或升级集群。要使用 RA3 节点类型，请在 Virtual Private Cloud (EC2-VPC) 中创建集群。

要更改具有 RA3 节点类型的 Amazon Redshift 集群的节点数，请执行以下操作之一：

- 使用弹性调整大小操作添加或删除节点。在某些情况下，不允许使用弹性调整大小从 RA3 集群中删除节点。例如，在 2:1 节点计数升级将每个节点的切片数设置为 32 时。有关更多信息，请参阅调整集群大小 (p. 65)。如果弹性调整大小不可用，请使用经典调整大小。
- 使用经典调整大小操作添加或删除节点。当您将大小调整为无法通过弹性调整大小实现的配置时，请选择此选项。弹性调整大小比经典调整大小更快。有关更多信息，请参阅调整集群大小 (p. 65)。

Amazon 区域中的 RA3 节点类型可用性

RA3 节点类型仅在以下 Amazon 区域中可用：

- 美国东部（弗吉尼亚北部）区域 (us-east-1)
- 美国东部（俄亥俄）区域 (us-east-2)
- 美国西部（加利福尼亚北部）区域 (us-west-1)
- 美国西部（俄勒冈）区域 (us-west-2)
- 非洲（开普敦）区域 (af-south-1)
- 亚太地区（香港）区域 (ap-east-1)
- 亚太地区（雅加达）区域（ap-southeast-3）– 仅支持 ra3.4xlarge 和 ra3.16xlarge 节点类型
- 亚太地区（孟买）区域 (ap-south-1)
- 亚太地区（大阪）区域 (ap-northeast-3)
- 亚太地区（首尔）区域 (ap-northeast-2)
- 亚太地区（新加坡）区域 (ap-southeast-1)
- 亚太地区（悉尼）区域 (ap-southeast-2)
- 亚太地区（东京）区域 (ap-northeast-1)
- 加拿大（中部）区域 (ca-central-1)
- 中国（北京）区域 (cn-north-1)
- 中国（宁夏）区域 (cn-northwest-1)
- 欧洲（法兰克福）区域 (eu-central-1)
- 欧洲（爱尔兰）区域 (eu-west-1)
- 欧洲（伦敦）区域 (eu-west-2)
- 欧洲（米兰）区域 (eu-south-1)
- 欧洲（巴黎）区域 (eu-west-3)
- 欧洲（斯德哥尔摩）区域 (eu-north-1)
- 中东（巴林）区域 (me-south-1)
- 中东（阿联酋）区域（me-central-1）– 仅支持 ra3.4xlarge 和 ra3.16xlarge 节点类型
- 南美洲（圣保罗）区域 (sa-east-1)
- Amazon GovCloud（美国东部）(us-gov-east-1)

- Amazon GovCloud（美国西部）(us-gov-west-1)

升级到 RA3 节点类型

要将现有节点类型升级到 RA3，您可以使用以下方法更改节点类型：

- 从快照中还原 – Amazon Redshift 使用 DS2 或 DC2 集群的最新快照，并还原该快照以创建新的 RA3 集群。在集群创建完成后（通常在几分钟内），RA3 节点可以立即运行全部生产工作负载。由于计算与存储分开并具有较大的网络带宽，因此，可以快速地将热数据存储到本地缓存中。如果从最新的 DS2 或 DC2 快照中还原，则 RA3 保留 DS2 或 DC2 工作负载的热块信息，并使用最热的块填充其本地缓存。有关更多信息，请参阅从快照还原集群 (p. 322)。

  要为应用程序和用户保持相同的端点，可以使用与原始 DS2 或 DC2 集群相同的名称重命名新的 RA3 集群。要重命名集群，请在 Amazon Redshift 控制台或 `ModifyCluster` API 操作中修改集群。有关更多信息，请参阅 Amazon Redshift API 参考中的 重命名集群 (p. 74) 或 `ModifyCluster` API 操作。
- 弹性调整大小 – 使用弹性调整大小调整集群大小。在使用弹性调整大小更改节点类型时，Amazon Redshift 自动创建快照，创建新的集群，删除旧集群并重命名新集群。可以按需运行弹性调整大小操作，也可以计划在将来的时间运行。您可以使用弹性调整大小将现有的 DS2 或 DC2 节点类型集群快速升级到 RA3。有关更多信息，请参阅弹性调整大小 (p. 66)。

下表显示了在升级到 RA3 节点类型时的建议。（这些建议也适用于预留节点。）

现有的节点类型	现有节点数	建议的新节点类型	升级操作	
ds2.xlarge	1	ra3.xlplus	创建 1 节点 ra3.xlplus 集群[1]。	
ds2.xlarge	2	ra3.xlplus	创建 2 节点 ra3.xlplus 集群[1]。	
ds2.xlarge	3	ra3.xlplus	创建 2 节点 ra3.xlplus 集群[1]。	
ds2.xlarge	4	ra3.xlplus	创建 3 节点 ra3.xlplus 集群[1]。	
ds2.xlarge	5	ra3.xlplus	创建 4 节点 ra3.xlplus 集群[1]。	
ds2.xlarge	6	ra3.xlplus	创建 4 节点 ra3.xlplus 集群[1]。	
ds2.xlarge	7	ra3.xlplus	创建 5 节点 ra3.xlplus 集群[1]。	
ds2.xlarge	8	ra3.4xlarge	创建 2 节点 ra3.4xlarge 集群[1]。	
ds2.xlarge	9	ra3.4xlarge	创建 3 节点 ra3.4xlarge 集群[1]。	
ds2.xlarge	10	ra3.4xlarge	创建 3 节点 ra3.4xlarge 集群[1]。	

现有的节点类型	现有节点数	建议的新节点类型	升级操作	
ds2.xlarge	11-128	ra3.4xlarge	为每 4 个 ds2.xlarge[1] 节点创建 1 个 ra3.4xlarge 节点。	
ds2.8xlarge	2–15	ra3.4xlarge	为每 1 个 ds2.8xlarge[1] 节点创建 2 个 ra3.4xlarge 节点。	
ds2.8xlarge	16–128	ra3.16xlarge	为每 2 个 ds2.8xlarge[1] 节点创建 1 个 ra3.16xlarge 节点。	
dc2.8xlarge	2–15	ra3.4xlarge	为每 1 个 dc2.8xlarge[1] 节点创建 2 个 ra3.4xlarge 节点。	
dc2.8xlarge	16–128	ra3.16xlarge	为每 2 个 dc2.8xlarge[1] 节点创建 1 个 ra3.16xlarge 节点。	
dc2.large	1–4	无	保留现有的 dc2.large 集群。	
dc2.large	5–15	ra3.xlplus	为每 8 个 dc2.large 节点创建 3 个 ra3.xlplus 节点[1]。	
dc2.large	16 – 32	ra3.4xlarge	为每 8 个 dc2.large1[1、2] 节点创建 1 个 ra3.4xlarge 节点。	

[1]根据工作负载要求，可能需要使用额外的节点。请根据所需的查询性能的计算要求添加或删除节点。

[2] 具有 dc2.large 节点类型的集群仅限 32 个节点。

某些 RA3 节点类型的最小节点数为 2 节点。在创建 RA3 集群时，请考虑到这一点。

在弹性调整大小或快照恢复期间将 DS2 保留节点升级为 RA3 保留节点

如果您有 DS2 预留节点，则可以使用 Amazon Redshift 控制台或 Amazon CLI，然后通过 RA3 预留节点升级功能将其进行升级。在控制台上，您可以通过多种方式执行此操作。

一种方法是在弹性调整大小期间将 DS2 保留节点升级为 RA3。如果您有预留节点并选择 RA3 节点，则控制台会引导您完成预留节点升级过程。从技术角度来看，弹性调整大小对于预留节点和非预留节点的工作方式相同。

如果您更改推荐的集群大小，则配置弹性调整大小时，RA3 预留节点升级将不可用，也不会出现在控制台上。（您仍然可以将 DS2 预留节点升级到 RA3，但调整大小并不会将 RA3 预留节点升级作为过程的一部分。另请注意，由于弹性调整大小的集群大小限制，您可能无法获得所需的集群大小。例如，如果您具有 4 节点 DS2 预留节点集群，则可能无法选择 3 节点 RA3 集群。在这种情况下，您可以执行经典调整大小以获得所需的集群大小。

在集群调整大小后，需要执行这些步骤。首先，将数据迁移到 RA3 集群。然后，DS2 预留节点租约将转换为 RA3 预留节点租约。请注意，数据迁移的时间可能会有所不同，具体取决于集群的大小以及调整大小是弹性调整还是经典调整。在经典调整大小的情况下，数据迁移通常需要几个小时。

开始调整大小后，通过在 Events（事件）[在 Amazon Redshift dashboard（Amazon Redshift 控制面板）中可用] 中查看消息，来跟踪进度。此处会有调整大小的事件通知，以及另一个关于预留节点升级的事件通知。有关使用事件的信息，请参阅Amazon Redshift 事件 (p. 501)。调整大小后，处于活动状态的调整大小集群将显示在 Amazon Web Services Management Console 中。您还可以查看转换后的 RA3 预留节点租约。源 DS2 预留节点可能仍会在控制台上出现大约一天。您无需为此付费。在验证 RA3 集群是否处于活动状态并生成转换后的预留节点租约之前，不要删除源 DS2 预留节点。

使用 RA3 保留节点升级功能的另一种方法是从快照还原。如果选择 RA3 节点类型，并且拥有 DS2 预留节点，则可以在此时选择 RA3 预留节点升级功能。从快照还原时，它将恢复到 RA3 预留节点集群中。如前所述，如果您选择的集群大小不是推荐的大小，则控制台上将不提供 RA3 保留节点升级选项。

有关调整集群大小和升级节点的更多信息，请参阅获取领导节点 IP 地址 (p. 72)。在那里，您可以找到过程的详细描述，还可以了解当您调整大小时，集群和数据发生什么变化。有关弹性调整大小过程中步骤的更多详细信息，请参阅弹性调整大小 (p. 66)。有关从快照还原的更多信息，请参阅从快照还原集群 (p. 322)。

如果您有更多关于将预留节点升级到 RA3 的问题，例如将 DC2 预留节点升级到 RA3，请联系 Amazon Support。有关按需和预留节点定价的信息，请参阅 Amazon Redshift 定价。

如果您已购买 DS2 预留节点，请与 Amazon 联系以获得将 DS2 预留节点转换为 RA3 预留节点的帮助。要与 Amazon 联系以获取更多信息，请参阅具有托管存储的 Amazon Redshift RA3 实例。

从 DC1 节点类型升级到 DC2 节点类型

为了利用提升的性能，您可以将 DC1 集群升级到 DC2 节点类型。

使用 DC2 节点类型的集群必须在 Virtual Private Cloud (EC2-VPC) 中启动。

如果您的 DC1 集群不在 VPC 中：

1. 创建 DC1 集群的快照。有关更多信息，请参阅Amazon Redshift 快照 (p. 318)。
2. 创建 VPC，或选择您账户中的现有 VPC。有关更多信息，请参阅在 VPC 中管理集群 (p. 92)。
3. 将快照还原到 VPC 中的新 DC2 集群。有关更多信息，请参阅从快照还原集群 (p. 322)。

如果您的 DC1 集群已在 VPC 中，请选择以下方法之一：

- 作为操作的一部分，调整 DC1 集群的大小并将节点类型更改为 DC2。在调整大小操作期间，您的集群在一段时间内不可用。有关更多信息，请参阅在 Amazon Redshift 中调整集群大小 (p. 65)。
- 创建 DC1 集群的快照，然后将快照还原到 VPC 中的 DC2 集群。有关更多信息，请参阅从快照还原集群 (p. 322)。

从 DC1 升级到 DC2 节点类型时，请考虑以下事项。

- 100% 满的 DC1 集群可能不会升级到相同数量的 DC2 节点。如果需要更多磁盘空间，您可以：
  - 调整配置的大小，使其具有更多可用磁盘空间。

  - 通过截断表或删除行来清理不需要的数据。
- DC2 集群不支持 EC2-Classic 网络。如果您的 DC1 集群未在 VPC 中运行，请为 DC2 迁移创建一个。有关更多信息，请参阅在 VPC 中管理集群 (p. 92)。
- 如果您调整集群的大小，在操作期间它可能会进入只读模式。有关更多信息，请参阅在 Amazon Redshift 中调整集群大小 (p. 65)。
- 如果您购买了 DC1 预留节点，您可以在剩余期限内将 DC1 预留节点升级到 DC2 节点。有关如何使用 Amazon CLI 更改预留的更多信息，请参阅使用 Amazon CLI 升级预留节点 (p. 340)。
- 如果使用还原从 dc1.large 升级到 dc2.large，并更改节点数量，则必须在集群版本 1.0.10013 或更高版本创建快照。
- 如果使用还原从 dc1.8xlarge 升级到 dc2.8xlarge，则必须在集群版本 1.0.10013 或更高版本创建快照。
- 如果使用弹性调整大小从 DC1 升级到 DC2，并更改节点数量，则集群必须为 1.0.10013 或更高版本。
- 如果要升级的 dc1.8xlarge 集群的快照来自 1.0.10013 版本之前的集群，则首先将快照从 dc1.8xlarge 集群还原到具有相同节点数的新 dc1.8xlarge 集群中。然后使用以下方法之一升级新的 dc1.8xlarge：
  - 使用新还原的集群中的快照升级到 dc2.8xlarge。
  - 使用弹性调整大小将新还原的集群升级到 dc2.8xlarge。

将 EC2-Classic 上的 DS2 集群升级为 EC2-VPC

Amazon Redshift 集群在 Amazon EC2 实例中运行，这些实例针对您选择的 Amazon Redshift 节点类型和大小进行配置。我们建议您在 EC2-Classic 上升级集群以使用 EC2-VPC 在 VPC 中启动，从而提高性能和安全性。

要将 EC2-Classic 上的 DS2 集群升级为 EC2-VPC

1. 创建 DS2 集群的快照。有关更多信息，请参阅Amazon Redshift 快照 (p. 318)。
2. 创建 VPC，或选择您账户中的现有 VPC。有关更多信息，请参阅在 VPC 中管理集群 (p. 92)。
3. 将快照还原到 VPC 中的新 DS2 集群。有关更多信息，请参阅从快照还原集群 (p. 322)。

区域和可用区注意事项

Amazon Redshift 在多个 Amazon 区域可用。预设情况下，Amazon Redshift 在所选的 Amazon 区域内随机选择的可用区 (AZ) 中预置集群。所有集群节点是在同一可用区中预置的。

您可以选择请求特定的可用区（如果 Amazon Redshift 在该区域中可用）。例如，如果您已在某个可用区中运行 Amazon EC2 实例，您可能希望在同一可用区中创建 Amazon Redshift 集群以减少延迟。另一方面，您可能希望选择另一个可用区以获得更高的可用性。Amazon Redshift 可能无法在 Amazon 区域内的所有可用区中使用。

有关可以预置 Amazon Redshift 集群的支持 Amazon 区域的列表，请参阅 Amazon Web Services 一般参考中的 Amazon Redshift 端点。

集群维护

Amazon Redshift 定期执行维护以升级您的集群。在此类更新期间，无法对 Amazon Redshift 集群执行常规操作。您可以通过多种方式控制维护集群的方法。例如，您可以控制将更新部署到集群的时间。您还可以选择集群是运行最近发行的版本，还是运行以前发行的版本并升级到最近发行的版本。最后，您可以选择将非强制性维护更新推迟一段时间。

主题

- 维护时段 (p. 61)
- 推迟维护 (p. 62)
- 选择集群维护跟踪 (p. 62)
- 管理集群版本 (p. 63)
- 回滚集群版本 (p. 63)
- 确定集群维护版本 (p. 63)

维护时段

Amazon Redshift 针对每个 Amazon 区域从 8 小时时间段中随机分配 30 分钟的维护时段，维护可能发生在包括周一至周日在内的一周中随机的一天。

默认维护时段

下方列表显示了为每个 Amazon 区域分配默认维护时段的时间段。

- 美国东部（弗吉尼亚北部）区域：03:00–11:00 UTC
- 美国东部（俄亥俄）区域：03:00-11:00 UTC
- 美国西部（加利福尼亚北部）区域：06:00 -14:00 UTC
- 美国西部（俄勒冈）区域：06:00-14:00 UTC
- 非洲（开普敦）区域：20:00-04:00 UTC
- 亚太地区（香港）区域：13:00-21:00 UTC
- 亚太地区（雅加达）区域：15:00–23:00 UTC
- 亚太地区（孟买）区域：16:30–00:30 UTC
- 亚太地区（大阪）区域：13:00–21:00 UTC
- 亚太地区（首尔）区域：13:00–21:00 UTC
- 亚太地区（新加坡）区域：14:00-22:00 UTC
- 亚太地区（悉尼）区域：12:00–20:00 UTC
- 亚太地区（东京）区域：13:00–21:00 UTC
- 加拿大（中部）区域：03:00–11:00 UTC
- 中国（北京）区域：13:00–21:00 UTC
- 中国（宁夏）区域：13:00–21:00 UTC
- 欧洲（法兰克福）区域：06:00–14:00 UTC
- 欧洲（爱尔兰）区域：22:00-06:00 UTC
- 欧洲（伦敦）区域：22:00-06:00 UTC
- 欧洲（米兰）区域：21:00-05:00 UTC
- 欧洲（巴黎）区域：23:00-07:00 UTC
- 欧洲（斯德哥尔摩）区域：23:00–07:00 UTC
- 中东（巴林）区域：13:00-21:00 UTC
- 中东（阿联酋）区域：18:00–02:00 UTC
- 南美洲（圣保罗）区域：19:00–03:00 UTC

如果在指定周内安排了维护事件，则维护将在分配的 30 分钟维护时段内启动。当 Amazon Redshift 执行维护时，它会终止正在进行的任何查询或其他操作。大多数维护都将在 30 分钟的维护时段内完成，但某些维护任务可能在此时段结束后继续运行。如果在计划的维护时段没有要执行的维护任务，您的集群会在下个计划维护时段到来之前继续正常运行。

您可以通过编程方式或使用 Amazon Redshift 控制台对集群进行修改来更改计划的维护时段。该时段必须至少为 30 分钟，但不得超过 24 小时。有关更多信息，请参阅使用控制台管理集群 (p. 83)。

推迟维护

如果需要重新计划集群的维护时段，您可以选择将维护最多延迟 45 天。例如，如果集群的维护时段设置为星期三 8:30 – 9:00 UTC，并且您需要在该时间访问集群，则可以将维护推迟到以后的时间段。除非我们需要更新硬件，否则在您指定推迟时，我们不会对您的集群执行任何维护。

如果我们需要在您推迟期间更新硬件或进行其他强制更新，我们会通知您并进行必要的更改。在这些更新期间，您的集群不可用。

如果您推迟了集群的维护，则推迟时段后的维护时段是强制实施的。不能将它推迟。

Note

维护一旦开始便无法推迟。

有关更多信息，请参阅修改集群 (p. 86)。

选择集群维护跟踪

当 Amazon Redshift 发布新的集群版本时，您的集群将在其维护时段内更新。您可以控制集群是更新为最新的经审批版本还是先前版本。

维护跟踪控制将在维护时段内应用的集群版本。当 Amazon Redshift 发布新的集群版本时，该版本将分配给最新跟踪，上一个版本将分配给尾随跟踪。要为集群设置维护跟踪，请指定下列值之一：

- 最新 – 使用最新的经批准的集群版本。
- 尾随 – 使用最新版本之前的集群版本。
- 预览 – 使用包含可用于预览的新功能的集群版本。

例如，假设您的集群当前正在运行版本 1.0.2762，而 Amazon Redshift 的最新版本为 1.0.3072。如果将维护跟踪值设置为 Current (当前)，则您的集群在下一个维护时段内将更新为版本 1.0.3072 (下一个经审批的版本) 。如果您将维护跟踪值设置成 Trailing (尾随)，则在 1.0.3072 后面的新版本出现之前，您的集群不会更新。

预览跟踪

Preview (预览) 跟踪可能并非总是可以选择。在选择 Preview (预览) 跟踪时，还必须选择跟踪名称。预览跟踪及其相关资源是临时的，具有功能限制，并且可能不包含其他跟踪中可用的所有当前 Amazon Redshift 功能。在使用预览跟踪时：

- 使用预览跟踪时，使用新的 Amazon Redshift 控制台。例如，当您创建要与预览功能一起使用的集群时。
- 无法将集群从一个预览跟踪切换到另一个预览跟踪。
- 无法将集群从当前跟踪或尾随跟踪切换到预览跟踪。
- 无法从通过其他预览跟踪创建的快照中还原。
- 只能在创建新集群或从快照还原时使用预览跟踪。
- 您不能从通过其他预览跟踪创建的快照中进行还原，也不能使用晚于预览跟踪集群版本的集群维护版本进行还原。例如，在将集群还原到预览跟踪时，您只能使用通过早于预览跟踪的集群维护版本创建的快照。

在维护跟踪之间切换

更改集群的跟踪通常是一个一次性的决定。更改跟踪时要慎重。如果您将维护跟踪从 Trailing (尾随) 更改为 Current (最新)，我们将在下一个维护时段内将集群更新为 Current (最新) 跟踪发布版。不过，如果您将集群

的维护跟踪更改为 Trailing (尾随)，则在 Current (最新) 跟踪发布版之后的新版本出现之前，我们不会更新您的集群。

维护跟踪和还原

快照将继承源集群的维护跟踪。如果您在制作快照后更改源集群的维护跟踪，则快照和源集群将位于不同的跟踪上。当您从快照进行还原时，新集群将位于从源集群继承的维护跟踪上。在还原操作完成后，您可以更改维护跟踪。调整集群的大小不会影响集群的维护跟踪。

管理集群版本

维护跟踪是一系列的版本。您可以决定您的集群是在最新跟踪还是尾随跟踪上。如果您将集群放在最新跟踪上，则它在维护时段内将始终升级到最新的集群发布版。如果您将集群放在尾随跟踪上，则它将始终运行在最近发布的版本之前发布的集群发布版。

集群的 Amazon Redshift 控制台列表中的发布状态列指示您的其中一个集群是否可用于升级。

回滚集群版本

如果您的集群为最新版本，则您可以选择将其回滚到之前的版本。

有关每个集群版本包含的功能和改进的详细信息，请参阅 集群版本历史记录 (p. 98)。

回滚回早期集群版本

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 选择要回滚的集群。
4. 对于 Actions (操作)，选择 Roll back cluster version (回滚集群版本)。这将显示 Roll back cluster version (回滚集群版本) 页面。
5. 如果有可用于回滚的版本，请按照该页面上的说明进行操作。
6. 选择 Roll back now (立即回滚)。

确定集群维护版本

您可以使用 Amazon Redshift 控制台确定 Amazon Redshift 引擎和数据库版本。

查找集群的版本

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后从列表中选择集群名称以打开其详细信息。此时将显示集群的详细信息，其中包括 Cluster performance（集群性能）、Query monitoring（查询监控）、Databases（数据库）、Datashares（数据共享）、Schedules（计划）、Maintenance（维护）和 Properties（属性）选项卡。
3. 选择 Maintenance（维护）选项卡以查看更多详细信息。
4. 在 Maintenance (维护) 部分中，找到 Current cluster version (当前集群版本)。

   Note

   虽然这些信息在控制台的一个字段中显示，但在 Amazon Redshift API 中由两个参数来表示：`ClusterVersion` 和 `ClusterRevisionNumber`。有关更多信息，请参阅 Amazon Redshift API 参考中的集群。

默认磁盘空间警报

创建 Amazon Redshift 集群时，您可以选择配置一个 Amazon CloudWatch 告警来监控在集群的所有节点中已用磁盘空间所占的平均百分比。我们将此警报称为默认磁盘空间警报。

默认磁盘空间警报的目的是帮助您监控集群的存储容量。您可以根据数据仓库的需要配置此警报。例如，您可以使用警告作为可能需要调整集群大小的指示器。您可以将大小调整为不同的节点类型或添加节点，或者购买预留节点以供将来扩展。

当磁盘的使用率在指定持续时间达到或超出指定百分比一定次数，则会触发默认磁盘空间警报。默认情况下，当磁盘的使用率达到您指定的百分比并保持或超出这一百分比五分钟或更长时间，则会触发此警报。启动集群后，您可以编辑默认值。

当触发 CloudWatch 告警时，Amazon Simple Notification Service (Amazon SNS) 会向指定收件人发送通知，以提醒他们已达到百分比阈值。Amazon SNS 使用主题来指定接收方，并以通知的形式发送消息。您可以使用现有 Amazon SNS 主题；如果不使用的话，系统会根据您启动集群时指定的设置创建一个主题。启动集群后，您可以编辑此警报的主题。有关创建 Amazon SNS 主题的更多信息，请参阅开始使用 Amazon Simple Notification Service。

启动集群后，您可以从该集群 Status 窗口的 CloudWatch Alarms 下方查看和编辑警报。其名称为 percentage-disk-space-used-default-<*string*>。您可以打开该告警，以查看与其相关联的 Amazon SNS 主题以及编辑告警设置。如果您未选择使用现有的 Amazon SNS 主题，则系统为您创建的主题名为 <*clustername*>-default-alarms (<*recipient*>)，例如 examplecluster-default-alarms (notify@example.com)。

有关配置和编辑默认磁盘空间警报的更多信息，请参阅创建集群 (p. 84)和创建或编辑磁盘空间警报 (p. 89)。

Note

如果您将集群删除，与该集群相关联的警报不会被删除，但也不会触发。如果您不再需要该警报，可以从 CloudWatch 控制台中将其删除。

集群状态

集群状态显示了集群的当前状态。下表提供了对每个集群状态的说明。

状态	描述
available	集群正在运行且可供使用。
available, prep-for-resize	该集群正在为弹性调整大小操作做准备。集群正在运行且可用于读取和写入查询，但集群操作（例如，创建快照）不可用。
available, resize-cleanup	弹性调整大小操作正在完成到新集群节点的数据传输。集群正在运行且可用于读取和写入查询，但集群操作（例如，创建快照）不可用。
cancelling-resize	正在取消调整大小操作。
creating	Amazon Redshift 正在创建集群。有关更多信息，请参阅创建集群 (p. 84)。
deleting	Amazon Redshift 正在删除集群。有关更多信息，请参阅删除集群 (p. 86)。
final-snapshot	Amazon Redshift 正在删除集群前对其拍摄最终快照。有关更多信息，请参阅删除集群 (p. 86)。

状态	描述
hardware-failure	集群发生了硬件故障。 如果您的集群为单节点集群，则该节点无法替换。要恢复您的集群，请还原快照。有关更多信息，请参阅Amazon Redshift 快照 (p. 318)。
incompatible-hsm	Amazon Redshift 无法连接到硬件安全模块 (HSM)。检查集群和 HSM 之间的 HSM 配置。有关更多信息，请参阅使用硬件安全模块的 Amazon Redshift 加密 (p. 349)。
incompatible-network	基本网络配置出现问题。确保您在其中启动集群的 VPC 及其设置正确无误。有关更多信息，请参阅在 VPC 中管理集群 (p. 92)。
incompatible-parameters	相关联的参数组中的一个或多个参数值出现问题，此时无法应用这些参数值。修改参数组并更新所有无效值。有关更多信息，请参阅Amazon Redshift 参数组 (p. 299)。
incompatible-restore	从快照中还原集群时出现问题。使用其他快照再次尝试还原集群。有关更多信息，请参阅Amazon Redshift 快照 (p. 318)。
modifying	Amazon Redshift 正在将更改应用于集群。有关更多信息，请参阅修改集群 (p. 86)。
paused	集群已暂停。有关更多信息，请参阅暂停和恢复集群 (p. 73)。
rebooting	Amazon Redshift 正在重启集群。有关更多信息，请参阅重新引导集群 (p. 87)。
renaming	Amazon Redshift 正在将新名称应用于集群。有关更多信息，请参阅重命名集群 (p. 74)。
resizing	Amazon Redshift 正在调整集群的大小。有关更多信息，请参阅调整集群大小 (p. 87)。
rotating-keys	Amazon Redshift 正在轮换集群的加密密钥。有关更多信息，请参阅Amazon Redshift 中的加密密钥轮换 (p. 350)。
storage-full	集群已达到其存储容量。调整集群的大小以添加节点或选择其他节点大小。有关更多信息，请参阅调整集群大小 (p. 87)。
updating-hsm	Amazon Redshift 正在更新 HSM 配置。

Amazon Redshift 中的集群管理概览

创建集群后，您可以对其执行多个操作。操作包括调整大小、暂停、恢复、重命名和删除。

在 Amazon Redshift 中调整集群大小

随着您的数据仓库容量和性能需求的变化，您可以调整集群大小，以便充分利用 Amazon Redshift 的计算和存储选项。

调整大小操作有两种类型：

- 弹性调整大小：您可以向集群添加节点，或从集群中移除节点。您还可以更改节点类型，如从 DS2 节点更改为 RA3 节点。弹性调整大小是一项快速操作，通常可在数分钟内完成。因此，我们建议将其作为首选项。当您执行弹性调整大小时，它会重新分发数据切片，这些数据切片是在每个节点中分配内存和磁盘空间的分区。弹性调整大小适用于以下情况：

  - 增加或减少现有集群中的节点，但不更改节点类型：这通常被称为就地调整大小。当您执行这种调整大小时，一些正在运行的查询会成功完成，但其他查询可能会作为该操作的组成部分而被删除。弹性调整大小可在数分钟内完成。
  - 更改集群的节点类型：当您更改节点类型时，将创建快照，并将数据从原始集群重新分发到由新节点类型组成的集群。完成后，将删除正在运行的查询。与就地调整大小一样，它很快即可完成。
- 经典调整大小：您可以更改节点类型、节点数量或此两者，其方式与弹性调整大小相似。经典调整大小需要更多时间才能完成，但在节点计数发生变化或要迁移到的节点类型不在弹性调整大小范围内的情况下，它会很有用。例如，当节点计数的变化非常大时，此调整大小类型可能适用。您还可以使用经典调整大小来更改集群加密。例如，您可以使用它将未加密的集群修改为使用 Amazon KMS 加密。

计划调整大小：您可以为集群制定调整大小操作计划，使其纵向扩展以满足预期高使用率的要求，或者缩减其规模以节约成本。计划适用于弹性调整大小和经典调整大小。您可以在 Amazon Redshift 控制台上设置计划。有关更多信息，请参阅 Managing clusters using the console（使用控制台管理集群）下的 调整集群大小 (p. 87)。还可以使用 Amazon CLI 或 Amazon Redshift API 操作来设置调整大小计划。有关更多信息，请参阅 Amazon CLI 命令参考中的 create-scheduled-action 和 Amazon Redshift API 参考中的 CreateScheduledAction。

主题

- 弹性调整大小 (p. 66)
- 经典调整大小 (p. 68)

弹性调整大小

当您添加或移除相同类型的节点时，弹性调整大小操作包括以下阶段：

1. 弹性调整大小操作将为集群制作快照。此快照始终包括节点的无备份表 (p. 321)（如果适用）。（某些节点类型（如 RA3）没有无备份表。）如果您的集群因禁用了自动快照而没有最近的快照，则备份操作可能会花费更长时间。（要最大程度地减少调整大小操作开始前的时间，我们建议您在开始调整大小操作之前启用自动快照或创建手动快照。）如果在您启动弹性调整大小时，系统正在执行快照操作，若该快照操作未能在数分钟内完成，则调整大小可能会失败。有关更多信息，请参阅Amazon Redshift 快照 (p. 318)。
2. 该操作将迁移集群元数据。集群将在数分钟内不可用。大多数查询将暂停，并且连接将保持打开状态。但是，某些查询可能会被删除。此阶段很短。
3. 会话连接将恢复，并且查询将继续。
4. 弹性调整大小操作会在后台将数据重新分发到节点切片。集群可用于读取和写入操作，但是某些查询可能需要更长的时间来运行。
5. 在该操作完成后，Amazon Redshift 会发送一个事件通知。

当您使用弹性调整大小来更改节点类型时，它的工作方式与您增加或减少相同类型的节点时相似。首先，创建一个快照。使用该快照中的最新数据预调配新的目标集群，并在后台将数据传输到新集群。在此期间，数据是只读的。在大小调整接近完成时，Amazon Redshift 会将端点更新为指向新集群，并断开与原始集群的所有连接。

如果您有预留节点，例如 DS2 预留节点，则您可以在执行调整大小时升级到 RA3 预留节点。您可以在执行弹性调整大小或者使用控制台从快照还原时执行此操作。控制台将引导您完成此过程。有关升级到 RA3 节点的更多信息，请参阅升级到 RA3 节点类型。

新控制台

要使用 Amazon Redshift 控制台监控调整大小操作的进度，请选择 CLUSTERS（集群），然后选择要调整大小的集群以查看详细信息。

弹性调整大小操作不会对表进行排序或回收磁盘空间，因此，它不能替代 vacuum 操作。有关更多信息，请参阅对表执行 vacuum 操作。

弹性调整大小操作具有以下限制：

- 弹性大小调整和数据共享集群 - 如果您在作为数据共享创建者的集群上添加或缩减节点，则当 Amazon Redshift 迁移集群元数据时，您无法从使用者连接到该集群。同样，如果您执行弹性大小调整并选择新的节点类型，则当连接断开并转移到新的目标集群时，数据共享将不可用。在这两种类型的弹性大小调整中，创建者会有几分钟时间不可用。
- 单节点集群：您不能将弹性调整大小用于从单节点集群调整大小，也不能将其用于调整大小到单节点集群。
- 从共享快照传输数据：要在从共享快照传输数据的集群上运行弹性调整大小，必须至少有一个备份可供该集群使用。您可以在 Amazon Redshift 控制台快照列表中或通过 `describe-cluster-snapshots` CLI 命令或 `DescribeClusterSnapshots` API 操作查看备份。
- 平台限制：弹性调整大小仅可用于使用 EC2-VPC 平台的集群。有关更多信息，请参阅在创建集群时使用 EC2-VPC (p. 54)。
- 存储注意事项：确保新的节点配置有足够的存储空间来存储现有数据。您可能需要添加其他节点或更改配置。
- 源与目标集群大小：可以使用弹性调整大小将大小调整到的节点数量和类型的可能配置，取决于原始集群中的节点数量，和已调整大小的集群的目标节点类型。可以使用控制台确定可能的配置。您也可以运行带 `action-type resize-cluster` 选项的 `describe-node-configuration-options` Amazon CLI 命令。有关使用 Amazon Redshift 控制台进行大小调整的更多信息，请参阅调整集群大小 (p. 87)。

  以下示例 CLI 命令描述了可用的配置选项。在此示例中，名为 `mycluster` 的集群是一个 8 节点的 `dc2.large` 集群。

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

  此命令会返回一个选项列表，包括每个选项的建议节点类型、节点数和磁盘利用率。返回的配置根据特定的输入集群而不同。指定 `resize-cluster` CLI 命令的选项时，可以选择其中一种返回的配置。
- 其他节点的上限：弹性调整大小对您可以添加到集群的节点有限制。例如，dc2 集群支持弹性调整大小，最大可将节点数量增加一倍。为了说明，您可以将一个节点添加到 4 节点 dc2.8xlarge 集群中，使其成为 5 节点集群，或者添加更多节点，直到达到 8 个为止。

  使用某些 ra3 节点类型，您最多可以将节点数增加到现有计数的四倍。具体来说，假设您的集群由 ra3.4xlarge 或 ra3.16xlarge 节点组成。然后，您可以使用弹性调整大小将 8 节点集群中的节点数增加到 32。或者，您可以选择低于限制的值。（在这种情况下，请记住，集群增长 4 倍的能力取决于原始集群的大小。）如果您的集群有 ra3.xlplus 节点，则限制为两倍。

  所有 ra3 节点类型都支持将节点数减少到现有计数的四分之一。例如，您可以将包含 ra3.4xlarge 节点的集群的大小从 12 个节点减少到 3 个节点，或者减少到高于最小值的数字。

  下表列出了支持弹性调整大小的每个节点类型的增长和减少限制。

节点类型	增长限制	减少限制
ra3.16xlarge	4 倍（例如，从 4 个节点到 16 个节点）	到数量的四分之一（例如，从 16 个节点到 4 个节点）
ra3.4xlarge	4 倍	到数量的四分之一
ra3.xlplus	2 倍（例如，从 4 个节点到 8 个节点）	到数量的一半
dc2.8xlarge	2 倍	到数量的一半（例如，从 16 个节点到 8 个节点）
dc2.large	2 倍	到数量的一半

节点类型	增长限制	减少限制
ds2.8xlarge	2 倍	到数量的一半
ds2.xlarge	2 倍	到数量的一半

经典调整大小

经典调整大小用于处理集群大小或节点类型的更改不在弹性调整大小支持的规范范围内的情况。经典调整大小已经进行了性能改进，以便更快地完成大量数据的迁移（过去可能需要数小时或数天时间）。它通过在源集群与目标集群之间使用备份和还原操作来实现这一目标。它还使用更高效的分配，将数据合并到目标集群。

经典调整大小包含以下阶段：

1. 从源集群到目标集群的初始迁移。当预调配新的目标集群时，Amazon Redshift 发送一个事件通知，告知大小调整已开始。它会重新启动现有集群，这会关闭所有连接。如果集群是数据共享的创建者，则这包括来自使用者的连接。重新启动后，该集群处于只读模式，数据共享将恢复。这些操作需要几分钟时间。接下来，将数据迁移到目标集群，并且读取和写入都可用。

2. 使用后台工件将作为 Distribution Even（分配 Even）迁移的 Distribution Key（分配键）表重新转换为其原始分配方式。此阶段的持续时间取决于数据集的大小。有关更多信息，请参阅分配方式。

   在此过程中，可对数据库进行读取和写入。查询性能可能会有所下降。
3. 在调整大小过程即将完成时，Amazon Redshift 会将端点更新到目标集群，并将删除与源集群的所有连接。目标集群承担数据共享的创建者角色。
4. 在调整大小操作完成后，Amazon Redshift 会发送一个事件通知。

您可以在 Amazon Redshift 控制台上查看调整大小的进度。调整集群大小所用的时间取决于数据量。

> Note
>
> 如果您在具有大量数据的集群上执行经典调整大小，并且节点不是 RA3，则数据迁移可能会非常缓慢。迁移包含多 TB 数据的集群可能需要数天时间。完成 RA3 节点的数据传输速度会快得多。

弹性调整大小与经典调整大小的对比

下表对比了两种调整大小类型之间的行为。

弹性调整大小与经典调整大小的对比

行为	弹性调整大小	经典调整大小	注释				
系统数据留存	弹性调整大小将保留系统日志数据。	经典调整大小不会保留系统表和数据。	如果您在源集群中启用了审计日志记录，则您可以在调整大小后继续访问 Amazon S3 或				

行为	弹性调整大小	经典调整大小	注释				
			CloudWatch 中的日志。您可以根据数据策略的规定保留或删除这些日志。				
更改节点类型	当节点类型不变时弹性调整大小：就地调整大小，并将保留大多数查询。 在选择新节点类型的情况下弹性调整大小：将创建新集群。在调整大小过程完成后，将删除查询。	经典调整大小：将创建新集群。在调整大小过程中将删除查询。					
会话和查询留存	当源集群和目标集群中的节点类型相同时，弹性调整大小将保留会话和查询。如果您选择新的节点类型，则将删除查询。	经典调整大小不会保留会话和查询。将删除查询。	在删除查询后，预计会出现一些性能下降的情况。最好是在轻度使用期间执行调整大小操作。				

行为	弹性调整大小	经典调整大小	注释				
表排序	表格不会作为调整大小操作的组成部分进行排序。	表格不会作为调整大小操作的组成部分进行排序。	Amazon Redshift 在执行调整操作时不会对表进行排序，因此现有的排列顺序将保持不变。在您调整集群大小时，Amazon Redshift 会将数据库表分配至新的节点，然后运行 ANALYZE 命令来更新统计数据。该服务不会传输标记为删除的行，因此，如果您需要重新对表进行排序，则只需运行 VACUUM 命令即可。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的对表				

行为	弹性调整大小	经典调整大小	注释				
			执行 vacuum 操作。				
取消调整大小操作	您无法取消弹性调整大小。	您可以在经典调整大小操作完成之前取消该操作，方法是在 Amazon Redshift 控制台中从集群详细信息中选择 Cancel resize（取消调整大小）。	取消调整大小操作所需的时间取决于取消时调整大小操作所处的阶段。在取消操作完成前，如果您这样做，集群将不可用。如果调整大小操作处于最后阶段，您将无法取消。				

快照、还原和调整大小

弹性调整大小 (p. 66)是调整 Amazon Redshift 集群大小的最快方法。如果弹性调整大小操作不适合您，并且您需要对集群进行近乎恒定的写入访问，则可以使用下一部分中所述的快照和还原操作以及经典调整大小。如果采用此方法，在切换后，您必须手动将在制作快照后写入源集群的所有数据都复制到目标集群中。根据复制用时，您可能需要重复执行此操作多次，直到两个集群中的数据相同。然后，您可以切换到目标集群。在目标集群拥有完整数据集之前，此过程可能会对现有查询产生负面影响。不过，它能最大程度地缩短您无法写入数据库的时间。

快照、还原和调整大小方法使用以下流程：

1. 为您的现有集群制作快照。现有集群就是源集群。
2. 记下制作快照的时间。这样做意味着，您稍后可确定需要重新运行提取、事务处理和加载 (ETL) 流程的时间点，从而将制作快照后写入的所有数据都加载到目标数据库中。
3. 将快照还原到新集群中。这个新集群就是目标集群。验证目标集群中包含示例数据。
4. 调整目标集群的大小。为目标集群选择新的节点类型、节点数和其他设置。
5. 查看为源集群制作快照后通过 ETL 流程加载的数据。请确保按相同顺序将相同的数据重新加载到目标集群中。如果您的数据正在不断加载，请重复执行此流程多次，直到源集群和目标集群中的数据相同为止。
6. 停止在源集群上运行的所有查询。为此，您可以重启集群，或以超级用户的身份登录并使用 PG_CANCEL_BACKEND 和 PG_TERMINATE_BACKEND 命令。重启集群是确保集群不可用的最简单方法。
7. 重命名源集群。例如，将其从 `examplecluster` 重命名为 `examplecluster-source`。

8. 重命名目标集群，使用源集群在重命名之前的名称。例如，将目标集群从之前的名称重命名为 `examplecluster`。此后，使用包含 `examplecluster` 的端点的所有应用程序都会连接到目标集群。
9. 在切换到目标集群后删除源集群，并验证所有流程均可按预期正常工作。

或者，您可以在将数据重新加载到目标集群之前重命名源集群和目标集群。如果您不要求任何关联系统和报告立即与目标集群中的相应内容保持同步，则此方法将有效。在这种情况下，步骤 6 将移至前述流程的最后。

仅当您希望应用程序继续使用相同的端点连接到集群时，才需要执行重命名流程。如果您没有此要求，则可以更新连接到集群的任何应用程序，以使用目标集群的端点，而无需重命名集群。

重新使用集群名称具有诸多优势。首先，您无需更新应用程序的连接字符串，因为端点始终保持不变，即使基础集群发生改变也是如此。其次，相关项（例如 Amazon CloudWatch 警报和 Amazon Simple Notification Service (Amazon SNS) 通知）与集群名称相关联。这种关联意味着，您可以继续使用已为集群设置的相同警报和通知。在您希望灵活调整集群大小而无需重新配置相关项目（如警报和通知）的生产环境中，继续使用集群名称关系重大。

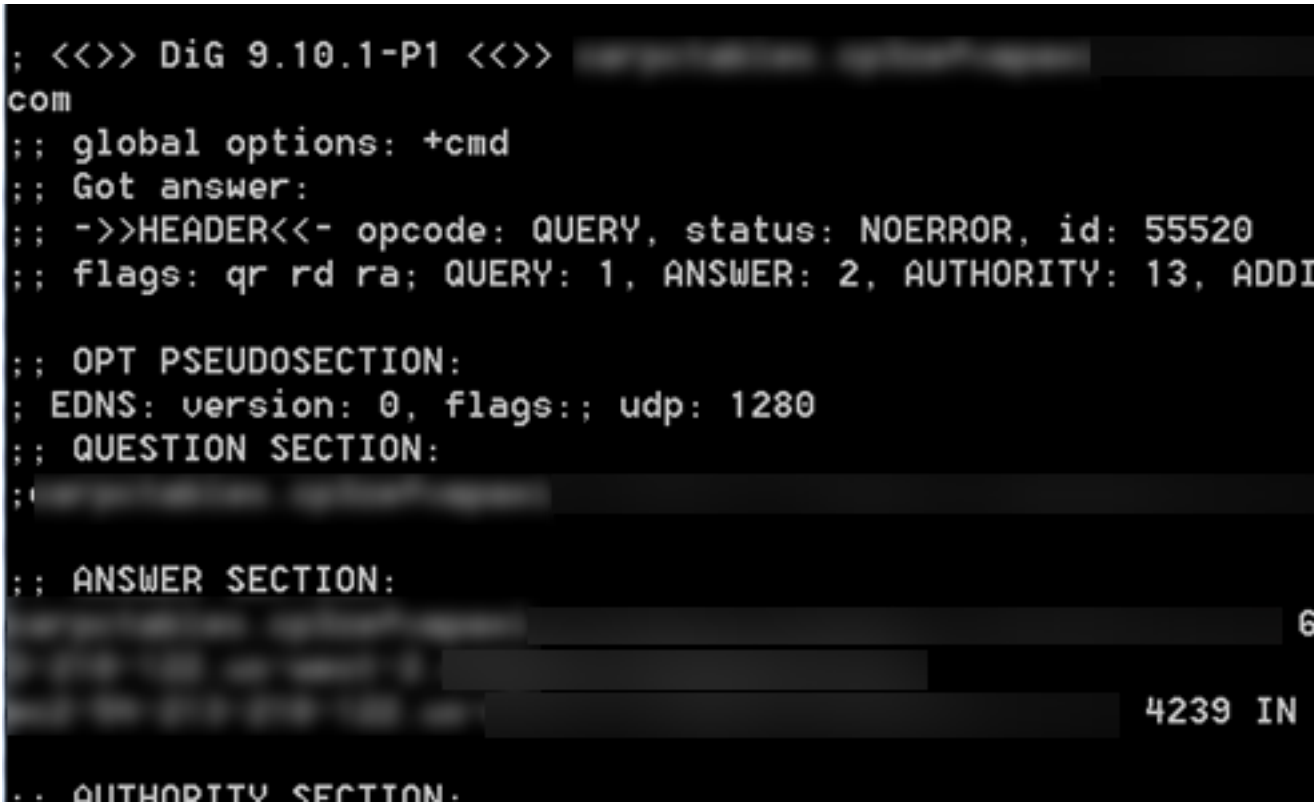
获取领导节点 IP 地址

如果您的集群是公有的且位于 VPC 中，则在调整大小后，该集群将保留领导节点的弹性 IP 地址 (EIP)。如果您的集群是私有的且位于 VPC 中，则在调整大小后，该集群将保留领导节点的私有 IP 地址。如果您的集群没有位于 VPC 中，则在调整大小操作过程中，系统将针对领导节点分配新的公有 IP 地址。

要获取集群的领导节点 IP 地址，请使用 dig 实用工具，如下所示。

```
dig mycluster.abcd1234.us-west-2.redshift.amazonaws.com
```

领导节点 IP 地址位于结果中的 ANSWER SECTION 末尾，如下所示。



暂停和恢复集群

如果您的集群只需在特定时间可用，则可以暂停该集群，然后再恢复它。当集群暂停时，按需计费将暂停。仅集群的存储会产生费用。有关定价的更多信息，请参阅 Amazon Redshift 定价页面。

如果您暂停集群，Amazon Redshift 将创建快照、开始终止查询并将集群置于暂停状态。如果您删除已暂停的集群而未请求最终快照，则无法还原该集群。在暂停或恢复操作启动后，无法取消或回滚该操作。

您可以在新的 Amazon Redshift 控制台上暂停和恢复集群，也可以使用 Amazon CLI 或 Amazon Redshift API 操作暂停和恢复集群。

可以计划用于暂停和恢复集群的操作。在使用新的 Amazon Redshift 控制台创建暂停和恢复的定期计划时，将为您选择的日期范围创建两个计划操作。计划操作名称的后缀为 `-pause` 和 `-resume`。名称的总长度必须在计划操作名称的最大大小范围内。

无法暂停以下类型的集群：

- EC2-Classic 集群。
- 不活动的集群，例如，当前正在修改的集群。
- 硬件安全模块 (HSM) 集群。
- 已禁用自动快照的集群。

在决定暂停集群时，请考虑以下事项：

- 与集群的连接或针对集群的查询不可用。
- 在 Amazon Redshift 控制台上看不到已暂停集群的查询监控信息。
- 无法修改已暂停的集群。未对集群执行任何计划操作。其中包括创建快照、调整集群大小和集群维护操作。
- 未创建硬件指标。如果已设置指标缺失警报，请更新 CloudWatch 警报。
- 无法将已暂停集群的最新自动快照复制到手动快照。
- 当正在暂停集群时，无法恢复集群，直至暂停操作完成。
- 如果您暂停集群，则计费将暂停。不过，暂停操作通常在 15 分钟内完成，具体取决于集群的大小。
- 审计日志已存档，无法在恢复时进行还原。
- 暂停集群后，跟踪和日志可能无法用于对暂停之前出现的问题进行故障排除。
- 恢复时不会还原集群上的无备份表。有关无备份表的更多信息，请参阅从快照中排除表 (p. 321)。

在恢复集群时，请考虑以下事项：

- 已恢复集群的集群版本将根据集群的维护时段更新为维护版本。
- 如果删除与已暂停集群关联的子网，则您的网络可能会不兼容。在此情况下，将从最新的快照还原您的集群。
- 如果您在集群暂停时删除弹性 IP 地址，则会请求新的弹性 IP 地址。
- 如果 Amazon Redshift 无法使用集群之前的弹性网络接口恢复集群，Amazon Redshift 会尝试分配一个新的弹性网络接口。
- 在恢复集群时，您的节点 IP 地址可能会发生更改。对于从 Secure Shell (SSH) 执行 COPY 或从 Amazon EMR 执行 COPY 等功能，您可能需要更新 VPC 设置以支持这些新的 IP 地址。
- 如果您尝试恢复未暂停的集群，恢复操作将返回错误。如果恢复操作是计划操作的一部分，请修改或删除计划操作以防止将来出现错误。
- 根据集群的大小，可能需要几分钟来恢复集群，然后才能处理查询。此外，在恢复完成后重新补充集群时，查询性能可能会在一段时间内受到影响。

重命名集群

如果您希望集群使用其他名称，则可以对其进行重命名。由于连接到集群的端点包含集群名称（也称集群标识符），因此重命名集群之后，端点也会改为使用新名称。例如，如果您的集群名为 `examplecluster`，您将其重命名为 `newcluster`，则端点会改为使用 `newcluster` 标识符。连接至集群的所有应用程序都必须使用新的端点进行更新。

如果您希望更改应用程序所连接到的集群，但又不想更改这些应用程序中的端点，则您可以对集群进行重命名。在此情况下，您必须先重命名原始集群，然后更改第二个集群，以重新使用原始集群重命名之前的名称。之所以这样做，是因为集群标识符在您的账户和区域中必须是独一无二的，因此原始集群和第二个集群的名称不能相同。如果从快照中还原集群，并且不希望更改任何从属应用程序的连接属性，则可能会这样做。

Note

如果您删除原始集群，则还需删除任何不需要的集群快照。

当您重命名集群时，在该过程结束之前，集群的状态会变为 `renaming`。该集群使用的旧 DNS 名称会被立即删除，但可能会在缓存中保留几分钟。重命名后的集群的新 DNS 名称在大约 10 分钟内生效。重命名后的集群在新名称生效之前不可用。系统会重新启动集群，且集群的所有现有连接都会被删掉。此过程完成后，端点会改为使用新名称。因此，您应该在开始重命名之前停止运行查询，并在重命名完成后恢复运行。

系统将会保留集群快照，而且与集群相关联的所有快照在集群重命名之后仍与该集群相关联。例如，假设您的一个集群服务于生产数据库且该集群有若干个快照。如果重命名该集群，然后在生产环境中将其替换为一个快照，则这些现有快照仍与重命名后的集群相关联。

Amazon CloudWatch 警报和 Amazon Simple Notification Service (Amazon SNS) 事件通知与集群的名称相关联。如果您重命名该集群，则需要相应地对这些内容进行更新。您可以在 CloudWatch 控制台中更新 CloudWatch 警报，也可以在 Amazon Redshift 控制台中的 Events（事件）窗格上更新 Amazon SNS 事件通知。集群的加载和查询数据在重命名前后都会继续显示数据。但是，性能数据则在重命名过程完成后重置。

有关更多信息，请参阅修改集群 (p. 86)。

关闭和删除集群

如果您希望集群停止运行且不再产生费用，则可以将其关闭。在关闭集群时，您可以选择创建一个最终快照。如果您创建最终快照，则 Amazon Redshift 会在您将集群关闭之前为其创建一个手动快照。如果您希望恢复运行集群和查询数据，则可以在之后还原该快照。

如果您不再需要集群及其数据，则可以将其关闭，而不创建最终快照。在这种情况下，会永久删除该集群及其数据。有关关闭和删除集群的更多信息，请参阅删除集群 (p. 86)。

无论在您关闭集群时是否有最终手动快照，与该集群相关联的所有自动快照都会在您关闭集群后删除。与该集群相关联的所有手动快照都会保留下来。如果您在关闭集群时没有其他正在运行的集群，或者正在运行的 Amazon Redshift 集群超出了向您提供的免费可用存储，则您需要针对保留下来的所有手动快照（包括可选的最终快照）按 Amazon Simple Storage Service 存储费率支付相应的费用。有关快照存储费用的更多信息，请参阅 Amazon Redshift 定价页面。

使用 AQUA（高级查询加速器）

AQUA（高级查询加速器）是一款面向 Amazon Redshift 的分析查询加速器，它使用自定义设计的硬件来加快扫描大型数据集的查询速度。

AQUA 是对 Amazon RedShift 托管存储的经济高效的补充，针对安全、事务性、多租户访问和高吞吐量分析查询进行了优化。它采用高速非易失性存储器标准 (NVMe) 固态存储元件和基于 Nitro 的加速来进行压缩和

加密。它使用基于现场可编程门阵列 (FPGA) 的加速度，将尽可能多的计算推送到存储层。这些组件以独特的方式连接在一起，无需使用传统 CPU 即可进行数据扫描。同时，这些组件允许在高速存储器中聚合中间结果。AQUA 是一个数据缓存，可以保持与 Redshift 托管存储的高速连接。

您无需更改数据库或应用程序即可使用 AQUA。Amazon Redshift 可识别查询中可以从加速中获益的扫描部分，并将其推送到 AQUA 进行处理。AQUA 会自动优化需要大量扫描、筛选器和聚合的数据子集的查询性能。使用此方法，您可以使用 AQUA 运行扫描、筛选和聚合大型数据集的查询。AQUA 擅长处理需要处理密集型扫描、筛选器和聚合的查询，例如那些包含 LIKE 和 SIMILAR TO 谓词的查询。

AQUA 支持身份验证、加密、隔离和合规性，以确保静态数据和传输中的数据安全。有关数据安全性和 AQUA 的更多信息，请参阅以下内容：

- Amazon Redshift 中的数据保护 (p. 346)
- 静态加密 (p. 346)
- 传输中加密 (p. 354)

有关 AQUA 的更多信息，请参阅Amazon Redshift 何时使用 AQUA 来运行查询？ (p. 75)。

AQUA 适用于具有 ra3.xlplus、ra3.4xlarge 和 ra3.16xlarge 节点类型的集群。

Aqua 在以下 Amazon 区域适用于发布版本 1.0.24421 或更高版本：

- 美国东部（弗吉尼亚北部）区域 (us-east-1)
- 美国东部（俄亥俄）区域 (us-east-2)
- 美国西部（加利福尼亚北部）区域 (us-west-1)
- 美国西部（俄勒冈）区域 (us-west-2)
- 亚太地区（孟买）区域 (ap-south-1)
- 亚太地区（首尔）区域 (ap-northeast-2)
- 亚太地区（新加坡）区域 (ap-southeast-1)
- 亚太地区（悉尼）区域 (ap-southeast-2)
- 亚太地区（东京）区域 (ap-northeast-1)
- 欧洲（法兰克福）区域 (eu-central-1)
- 欧洲（爱尔兰）区域 (eu-west-1)
- 欧洲（伦敦）区域 (eu-west-2)
- 欧洲（斯德哥尔摩）区域 (eu-north-1)

Amazon Redshift 会自动确定您的集群的 AQUA 是否处于活动状态。

Amazon Redshift 何时使用 AQUA 来运行查询？

对于扫描表的每个查询，Amazon Redshift 将确定扫描操作是发送到 AQUA 还是在 Amazon Redshift 集群本地运行。当扫描和聚合操作至少包含一个包含 AQUA 支持的 LIKE 或 SIMILAR TO 表达式的谓词时，它们将被发送到 AQUA。如果将扫描操作发送到 AQUA，则整个操作在 AQUA 上运行（不仅仅是 LIKE 或 SIMILAR TO 处理）。

例如，以下查询包含发送到 AQUA 的谓词 `str1 LIKE 'a%'` 和 `num1 > 10`。

```
select num2 from tbl where str1 LIKE 'a%' and num1 > 10 GROUP BY num2;
```

在此示例中，AQUA 将扫描表 `tbl`，按谓词进行筛选，按 `num2` 对结果进行分组，然后将结果返回至 Amazon Redshift。

在以下示例中，Amazon Redshift 确定查询的哪些部分最好在 AQUA 中运行，哪些部分在 Amazon Redshift 集群本地运行。在这种情况下，customer_name 列上有用于筛选返回的行的 LIKE 谓词。扫描操作被发送到 AQUA 以运行该部分查询。Amazon Redshift 仅接收扫描的结果，然后 Amazon Redshift 将使用该结果在本地执行联接并完成查询。

```
select  c.customer_name, p.prod_name, sum(revenue)
from orders o
  join customers c ON c.id = o.customer_id
  join products p ON p.id = o.product_id
where c.customer_name LIKE '%Amazon%Web%'
order by sum(revenue);
```

有关 LIKE 和 SIMILAR TO 的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 LIKE 和 SIMILAR TO。

AQUA 的注意事项

AQUA 目前不支持以下类型的 SQL 查询。包含这些查询的查询会在您的 Amazon Redshift 集群本地运行。

- 执行写入操作的查询，如 INSERT、UPDATE、DELETE、CREATE TABLE AS、COPY 和 UNLOAD。有关更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 SQL 命令。
- 没有谓词的 SELECT 查询，例如以下内容。

```
select * from tbl1
```

- 扫描中 Python 用户定义的函数 (UDF)，包括对 Python UDF 定义的复杂视图进行扫描。
- 在 LIKE 和 SIMILAR TO 谓词中使用以下元字符的查询：
  - LIKE 表达式中的非常量正则表达式文本。
  - 两种备选方案之一，例如以下内容。

```
SIMILAR TO '%(cat|dog)%'
```

  - VARCHAR 列中单字符通配符的多个实例，例如以下内容。

```
SIMILAR TO 'ab.cd.ef'
```

  - 匹配字符串中的 Unicode 转义序列、十六进制字符和八进制字符，例如以下内容。

```
SIMILAR TO '%ab\uc382'
```

```
SIMILAR TO '%ab\U0000c382'
```

```
SIMILAR TO '%ab\x88'
```

```
SIMILAR TO '%ab\127'
```

  - 重复元字符，如“*”、“+”、“?”、{m, n} 应用于 () 内的模式和多字节字符上，例如以下内容。

```
SIMILAR TO 'abc(def)*'
```

```
SIMILAR TO 'abc#+'
```

  - 括号表达式中的多字节字符 [...]，例如以下内容。

```
SIMILAR TO 'abc[#de]'.
```

- 字符串函数（如 LOWER、UPPER、LEFT、RIGHT）应用于 LIKE 或 SIMILAR TO 扫描的输出所处的查询。例如，以下摘录显示了 LOWER 函数。

```
LOWER(a) LIKE "%cat%"
```

相反，请尝试重写查询以使用不区分大小写的 ILIKE 而不带 LOWER。

```
ILIKE "%cat%"
```

如何确定是否使用了 AQUA

下面的 SQL 显示了在 AQUA 上运行的 SVL_QUERY_SUMMARY 的查询执行分段。

```
select * from svl_query_summary where label ~ 'Aqua' limit 100;
```

如果您拥有超级用户访问权限，还可以联接 STL_QUERY 和 STL_QUERYTEXT 视图以查看与 AQUA 运行的查询相对应的 SQL 语句。由 EXPLAIN 语句生成的解释计划不会显示查询是否使用了 AQUA。

管理 Amazon Redshift 中的使用限制

您可以定义限制来监控和管理某些 Amazon Redshift 功能的使用和相关成本。您可以创建每日、每周和每月使用限制，并定义 Amazon Redshift 在达到这些限制时自动采取的操作。操作包括将事件记录到系统表，以记录超出定义的限制的使用。其他可能的操作包括使用 Amazon SNS 和 Amazon CloudWatch 发出提醒以通知管理员，并禁用进一步的使用以控制成本。

可以为每个集群定义使用限制。在创建集群后，您可以为以下功能定义使用限制：

- Amazon Redshift Spectrum
- Amazon Redshift 并发扩展
- Amazon Redshift 跨区域数据共享

使用限制适用于提供了 Amazon Redshift Spectrum 和 Amazon Redshift 并发扩展的 Amazon 区域中的 1.0.14677 发布版本或更高版本。

Redshift Spectrum 限制指定以 1 TB 为增量扫描的数据总量的阈值。并发扩展限制指定并发扩展所用总时间的阈值（以 1 分钟为增量）。跨区域数据共享限制指定了扫描的数据总量阈值（以 1TB 为单位递增）。

可以为每日、每周或每月期间指定限制（使用 UTC 确定期间的开始和结束时间）。如果您在期间的中间时间点创建限制，则测量的限制为从该时间点到期间结束。例如，如果您在 3 月 15 日创建月度限制，则测量的第一个月度期间为 3 月 15 日到 3 月 31 日。

可以为每项功能定义多个使用限制。每个限制可具有不同的操作。可能的操作包括：

- 登录到系统表 – 这是默认操作。信息将记录到 STL_USAGE_CONTROL 表中。在评估过去的使用情况以及决定将来的使用限制时，日志记录非常有用。有关记录内容的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 STL_USAGE_CONTROL。
- 提示 – Amazon Redshift 会针对可用和已用的用量发出 CloudWatch 指标。可以为每项功能定义最多三个使用限制。如果您使用 Amazon Redshift 控制台启用提示操作，则将自动基于这些指标创建 CloudWatch

告警。您可以选择将 Amazon SNS 订阅附加到该告警。如果您使用的是 Amazon CLI 或 API 操作，请确保手动创建 CloudWatch 告警。在达到阈值时，也会将事件记录到系统表中。

- 禁用功能 – 在达到阈值时，Amazon Redshift 会禁用该功能，直到为下一个时间段（每天、每周或每月）刷新配额。对于每项功能，只能对一个限制执行禁用操作。事件也将记录到系统表中，并且会发出提醒。

使用限制将保留，直到使用限制定义本身或集群被删除为止。

可以使用新的 Amazon Redshift 控制台、Amazon CLI 或 Amazon Redshift API 操作来定义和管理使用限制。要在 Amazon Redshift 控制台上定义限制，请导航到您的集群，然后为 Actions（操作）选择 Configure usage limit（配置使用限制）。要查看之前为您的集群定义的使用限制，请导航到您的集群，然后选择 Maintenance（维护）选项卡、Usage limits（使用限制）部分。要查看集群的可用和已用的用量，请导航到您的集群。选择 Cluster performance（集群性能）选项卡，然后查看此功能已用的用量的图表。

您可以通过以下 Amazon Redshift CLI 操作来管理使用限制。有关更多信息，请参阅 Amazon CLI 命令参考。

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

您可以通过以下 Amazon Redshift API 操作来管理使用限制。有关更多信息，请参阅 Amazon Redshift API 参考。

- CreateUsageLimit
- DescribeUsageLimits
- ModifyUsageLimit
- DeleteUsageLimit

观看以下视频，了解如何使用 Amazon Redshift 控制台创建和监控使用限制：Amazon Redshift Spectrum 的成本控制和并发扩展。

在 Amazon Redshift 中管理集群重新定位

通过在 Amazon Redshift 中使用重新定位，您可以启用 Amazon Redshift 将集群移动到另一个可用区 (AZ)，而不会丢失任何数据或对您的应用程序进行更改。通过重新定位，您可以在集群上出现服务中断时继续操作，而产生的影响最小。

启用集群重新定位后，Amazon Redshift 可能会在某些情况下选择重新定位集群。特别是，当当前可用区中的问题阻碍了最佳集群操作或提高服务可用性时，会发生这种情况。您还可以在给定可用区中的资源限制中断集群操作的情况下调用重新定位功能。例如，恢复集群或调整集群大小的功能。Amazon Redshift 提供重新定位功能，无需额外付费。

当 Amazon Redshift 集群重新定位到新的可用区时，新集群具有与原始集群相同的端点。您的应用程序可以重新连接到端点并继续操作，而不会进行修改或丢失数据。但是，由于给定可用区中的潜在资源限制，重新定位可能并不总是可能的。

仅对 RA3 实例类型支持 Amazon Redshift 集群重新定位，例如 ra3.16xlarge、ra3.4xlarge 和 ra3.xlplus。RA3 实例类型使用 Redshift 托管存储 (RMS) 作为持久存储层。集群数据的最新副本始终提供在 Amazon 区域中的其他可用区中。换句话说，您可以将 Amazon Redshift 集群重新定位到另一个可用区，而不会丢失任何数据。

当您启用集群进行重新定位时，Amazon Redshift 会将您的集群迁移到代理后面。这样做有助于实现对集群计算资源的位置无关访问。迁移会导致重新引导集群。当集群重新定位到另一个可用区时，在新集群在新可

用区中重新联机时，会发生中断。但是，您无需对应用程序进行任何更改，因为即使集群重新定位到新的可用区后，集群端点仍保持不变。

如果您启用了重新定位，并且您当前使用领导节点 IP 地址访问您的集群，请确保更改该访问权限。反之，请使用与集群的 Virtual Private Cloud (VPC) 端点关联的 IP 地址。要查找此集群 IP 地址，在集群详细信息页面的 Network and security（网络和安全）部分中查找和使用 VPC 终端节点。要获取有关 VPC 终端节点的更多详细信息，请登录 Amazon VPC 控制台。

您也可以使用 Amazon Command Line Interface (Amazon CLI) 命令 `describe-vpc-endpoints` 获取与端点关联的弹性网络接口。您可以使用 `describe-network-interfaces` 命令获取关联的 IP 地址。有关 Amazon Redshift Amazon CLI 命令的更多信息，请参阅 Amazon CLI 命令参考中的可用命令

启用集群重新定位

您可以从 Amazon Redshift 控制台、通过 Amazon CLI 和 Amazon Redshift API 启用和管理集群重定位。

要启用集群重新定位，请定义包含多个可用区的子网组。如果 Amazon Redshift 确定了多个可访问的可用区，Amazon Redshift 会自动从可访问的可用区列表中选择以重新定位集群。

重新定位完成后，您可以使用相同的端点访问集群。Amazon Redshift 会删除原始集群的计算资源，并将其返回到资源池。

限制

使用 Amazon Redshift 重新定位时，请注意以下限制：

- 由于给定可用区中的潜在资源限制，可能无法在所有情况下进行集群重新定位。如果发生这种情况，Amazon Redshift 不会更改原始集群。
- DC1、DC2 或 DS2 产品实例系列不支持重新定位。
- 对于可公开访问的 Amazon Redshift 集群，重新定位不可用。
- 您不能跨 Amazon 区域执行重新定位。
- 您只能为使用默认端口设置 (5439) 的集群启用重新定位。否则，启用重新定位失败。
- 如果您已成功启用重定位并在稍后尝试修改默认端口设置，则修改操作将失败。

使用控制台管理重新定位

您可以使用 Amazon Redshift 控制台管理集群重新定位的设置。

在创建新集群时启用重新定位

在创建新集群时，可以使用以下过程启用重新定位。

要启用新集群的重新定位

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 选择 Create cluster（创建集群）以创建新集群。有关如何创建集群的更多信息，请参阅《Amazon Redshift 入门指南》中的创建示例 Amazon Redshift 集群。
4. 在 Backup（备份）下，为 Cluster relocation（集群重新定位）选择 Enable（启用）。重新定位预设情况下禁用。
5. 在 Network and security（网络和安全性）下，对于 Publicly accessible（可公开访问），请接受默认的 Disable（禁用）。如果选择 Enable（启用），Amazon Redshift 将返回错误。
6. 选择创建集群。

修改现有集群的重新定位

使用以下过程更改现有集群的重新定位设置。

要修改现有集群的重新定位设置

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。这将列出您的账户在当前 Amazon 区域中的集群。列表中的各个列中显示了每个集群的一部分属性。
3. 从列表中选择您要修改的集群的名称。此时将会显示集群详细信息页面。
4. 选择 Maintenance（维护）选项卡，然后在 Backup details（备份详细信息）部分中选择 Edit（编辑）。
5. 在 Backup（备份）下，选择 Enable（启用）。重新定位预设情况下禁用。
6. 选择 Properties（属性）选项卡，然后在 Network and security（网络和安全性）部分中确保为 Publicly accessible（可公开访问）选项选择 Disable（禁用）。
7. 选择修改集群。

重新定位集群

使用以下过程手动将集群重新定位到其他可用区。当您希望在辅助可用区中测试网络设置或当您在当前可用区中遇到资源限制时，这一点尤其有用。

要将集群重新定位到其他可用区

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。这将列出您的账户在当前 Amazon 区域中的集群。列表中的各个列中显示了每个集群的一部分属性。
3. 从列表中选择您要移动的集群的名称。此时将会显示集群详细信息页面。
4. 对于 Actions（操作），选择 Relocate（重新定位）。此时将显示 Relocate cluster（重新定位集群）页面。
5. （可选）选择一个可用区。如果您没有选择可用区，Amazon Redshift 会为您选择一个可用区。

Amazon Redshift 开始重新定位并将集群显示为重新定位。重新定位完成后，集群状态将更改为可用。

使用 Amazon Redshift CLI 管理重新定位

您可以使用 Amazon 命令行界面 (CLI) 管理集群重新定位的设置。

使用 Amazon CLI，以下示例命令会创建一个启用了重新定位且名为 **`mycluster`** 的 Amazon Redshift 集群。

```
aws redshift create-cluster --cluster-identifier mycluster --number-of-nodes 2 --master-
username adminuser --master-user-password TopSecret1 --node-type ra3.4xlarge --port 5439 --
no-publicly-accessible --availability-zone-relocation
```

如果您的当前集群使用不同的端口，您必须在修改它以启用重新定位之前将其修改为使用 5439。以下示例命令在您的集群不使用 5439 时修改端口。

```
aws redshift modify-cluster --cluster-identifier mycluster --port 5439
```

以下示例命令在 Amazon Redshift 集群上启用 availability-zone-relocation 参数。

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

以下示例命令在 Amazon Redshift 集群上禁用 availability-zone-relocation 参数。

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

以下示例命令将在 Amazon Redshift 集群上调用重新定位。

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

在 Amazon Redshift 中使用 Redshift 托管的 VPC 终端节点

预设情况下，Amazon Redshift 集群在 Virtual Private Cloud (VPC) 中进行预置。当您允许公共访问或设置互联网网关、NAT 设备或 Amazon Direct Connect 连接将流量路由到集群时，可从另一个 VPC 或子网中访问它。或者，您可以通过设置 Redshift 托管的 VPC 终端节点（由 Amazon PrivateLink 支持）来访问集群。

您可以将 Redshift 托管的 VPC 终端节点设置为包含集群的 VPC 与运行客户端工具的 VPC 之间的私有连接。如果集群位于另一个账户中，则账户拥有者（授予者）需要授予对要建立连接的账户（被授予者）的访问权限。通过这种方法，您可以访问数据仓库，而无需使用公有 IP 地址或通过 Internet 路由流量。

以下场景描述了允许使用 Redshift 托管的 VPC 终端节点访问集群的常见原因：

- Amazon 账户 A 希望允许 Amazon 账户 B 中的 VPC 对集群具有访问权限。
- Amazon 账户 A 希望允许同样位于 Amazon 账户 B 中的 VPC 对集群具有访问权限。
- Amazon 账户 A 希望允许 Amazon 账户 A 中的集群 VPC 中的另一个子网对集群具有访问权限。

设置 Redshift 托管的 VPC 终端节点以访问其他账户中的集群的常规工作流程如下所示：

1. 集群的拥有者账户和向其他账户授予访问权限，并指定被授权者的 Amazon 账户 ID 和 VPC 标识符（或所有 VPC）。
2. 被授权者账户收到通知，告知他们有权创建 Redshift 托管的 VPC 终端节点。
3. 被授权者账户创建一个 Redshift 托管的 VPC 终端节点。
4. 被授权者账户现在可以使用 Redshift 托管的 VPC 终端节点访问拥有者账户的集群。

您可以使用 Amazon Redshift 控制台、Amazon CLI 或 Amazon Redshift API 管理此过程。

使用 Redshift 托管的 VPC 终端节点时的注意事项

使用 Redshift 托管的 VPC 终端节点时，请牢记以下内容：

- 请确保要访问的集群是 RA3 节点类型。
- 确保要访问的集群已打开集群重新定位。有关启用集群重新定位的要求的信息，请参阅在 Amazon Redshift 中管理集群重新定位 (p. 78)。
- 确保要访问的集群可通过端口 5439 访问。
- 您可以修改与现有 Redshift 托管的 VPC 终端节点关联的 VPC 安全组。要修改其他设置，请删除当前 Redshift 托管 VPC 终端节点并创建一个新的端点。

- 您可以创建的 Redshift 托管 VPC 终端节点的数量限制为您的 VPC 终端节点配额。
- 无法从互联网访问 Redshift 托管的 VPC 终端节点。Redshift 托管的 VPC 终端节点只能在预置了端点的 VPC 中访问，或者在路由表和安全组允许的情况下与预置端点的 VPC 对等连接的任何 VPC 中访问。
- 您不能使用 Amazon VPC 控制台管理 Redshift 托管的 VPC 终端节点。

有关配额和命名约束的信息，请参阅Amazon Redshift 资源中的配额和限制 (p. 514)。

有关定价的信息，请参阅 Amazon PrivateLink 定价。

使用 Amazon Redshift 控制台管理 Redshift 托管的 VPC 终端节点

您可以使用 Amazon Redshift 控制台配置 Redshift 托管 VPC 终端节点的使用。

授予对集群的访问权限

如果您要访问集群的 VPC 位于另一个 Amazon 账户中，请确保从拥有者（授予者）账户授权它。

允许另一个 Amazon 账户中的 VPC 访问您的集群

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 对于您要允许访问的集群，请通过选择集群名称查看集群详细信息。选择集群的 Properties（属性）选项卡。

   Granted accounts（授予的账户）部分显示有权访问集群的账户和相应的 VPC。
4. 选择 Grant access（授予访问权限）以显示要输入 Grantee information（被授权者信息）的表单以添加账户。
5. 对于 Amazon account ID（Amazon 账户 ID），输入您授予访问权限的账户 ID。您可以授予对指定账户中特定 VPC 或所有 VPC 的访问权限。
6. 选择 Grant access（授予访问权限）以授予访问权限。

创建 Redshift 托管的 VPC 终端节点

如果您拥有某个集群，或者您已被授予对集群的访问权限，则可以为该集群创建一个 Redshift 托管的 VPC 终端节点。

要创建 Redshift 托管的 VPC 终端节点

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Configurations（配置）。

   Configurations（配置）页面显示已创建的 Redshift 托管 VPC 终端节点。要查看端点的详细信息，请选择其名称。
3. 选择 Create endpoint（创建端点）以显示一个表单，在其中输入有关要添加的端点的信息。
4. 输入 Endpoint name（端点名称）、Amazon account ID（Amazon 账户 ID）、Cluster identifier（集群标识符）、Virtual Private Cloud (VPC)、Subnet group（子网组）的值，以及端点的其他属性。

   Subnet group（子网组）中的子网组定义了 Amazon Redshift 部署端点所在的子网和 IP 地址。Amazon Redshift 选择具有可用于与端点关联的网络接口的 IP 地址的子网。

Security group（安全组）中的可选安全组定义您为端点授权的入站流量的端口、协议和源。通常，您允许访问工作负载运行所在的安全组或 CIDR 范围的端口 5439。

5. 选择 Create endpoint（创建端点）以创建端点。

创建端点后，您可以通过您的 Redshift 托管 VPC 终端节点的配置设置中的 Endpoint URL（端点 URL）中所示的 URL 来访问集群。

使用 Amazon CLI 管理 Redshift 托管的 VPC 终端节点

您可以使用以下 Amazon Redshift CLI 操作来使用 Redshift 托管的 VPC 终端节点。有关更多信息，请参阅 Amazon CLI 命令参考。

- authorize-endpoint-access
- revoke-endpoint-access
- create-endpoint-access
- modify-endpoint-access
- delete-endpoint-access
- describe-endpoint-access
- describe-endpoint-authorization

使用 Amazon Redshift API 操作管理 Redshift 托管的 VPC 终端节点

您可以使用以下 Amazon Redshift API 操作来使用 Redshift 托管的 VPC 终端节点。有关更多信息，请参阅 Amazon Redshift API 参考。

- AuthorizeEndpointAccess
- RevokeEndpointAccess
- CreateEndpointAccess
- ModifyEndpointAccess
- DeleteEndpointAccess
- DescribeEndpointAccess
- DescribeEndpointAuthorization

使用控制台管理集群

要创建、修改、调整、删除、重启和备份集群，请使用 Amazon Redshift 控制台中的 Clusters（集群）部分。

查看集群

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。这将列出您的账户在当前 Amazon 区域中的集群。列表中的各个列中显示了每个集群的一部分属性。如果您没有集群，请选择 Create cluster (创建集群) 来创建一个集群。
3. 在列表中选择集群名称可查看有关集群的更多详细信息。

主题

- 创建集群 (p. 84)
- 修改集群 (p. 86)
- 删除集群 (p. 86)
- 重新引导集群 (p. 87)
- 调整集群大小 (p. 87)
- 升级集群的发行版本 (p. 88)
- 获取有关集群配置的信息 (p. 88)
- 获取集群状态概述 (p. 88)
- 创建集群快照 (p. 88)
- 创建或编辑磁盘空间警报 (p. 89)
- 使用集群性能数据 (p. 89)

创建集群

在创建集群之前，请参阅Amazon Redshift 集群概览 (p. 50)和Amazon Redshift 中的集群和节点 (p. 50)。

创建集群

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。这将列出您的账户在当前 Amazon 区域中的集群。列表中的各个列中显示了每个集群的一部分属性。
3. 选择 Create cluster（创建集群）以创建集群。
4. 按照控制台页面上的说明进行操作，为 Cluster configuration (集群配置) 输入属性。

   选择以下方法之一以调整集群的大小：

   Note

   以下步骤介绍了 Amazon Redshift 控制台，它在Amazon支持 RA3 节点类型的区域中运行。有关支持 RA3 节点类型的 Amazon 区域的列表，请参阅 Amazon Redshift 集群管理指南中的 RA3 节点类型概览。

   - 如果您的Amazon区域支持 RA3 节点类型，请选择 Production（生产）或 Free trial（免费试用）回答问题您打算将此集群用于什么？

     如果您的组织符合条件，您或许能够在 Amazon Redshift 免费试用计划下创建集群。为此，请选择 Free trial（免费试用）创建具有 dc2.large 节点类型的配置。有关选择免费试用的更多信息，请参阅 Amazon Redshift 免费试用。
   - 如果您不知道要将集群调整到多大，请选择 Help me choose（帮我选择）。执行此操作将启动大小调整计算器，该计算器将询问您有关计划存储在数据仓库中的数据的大小和查询特性的问题。

     如果您知道集群所需的大小（即节点类型和节点数），请选择 I'll choose（我会选择）。然后选择节点类型和节点数量来调整集群的大小以进行概念验证。
5. 按照控制台页面上的说明进行操作，为 Cluster details (集群详细信息) 输入属性。

   Note

   如果您在防火墙的后面，则数据库端口必须是接受入站连接的开放端口。
6. （可选）按照控制台页面上的说明进行操作，为 Cluster permissions (集群权限) 输入属性。如果您的集群需要为您访问其他 Amazon 服务（例如，从 Amazon S3 加载数据），请提供集群权限。

7. 选择 Create cluster (创建集群) 以创建集群。集群可能需要几分钟才可以使用。

其他配置

在创建一个集群时，可以指定其他属性来自定义该集群。您可以在下面的列表中找到有关这些属性中的某些属性的更多详细信息。

Virtual Private Cloud (VPC)

选择具有子网组的 VPC。集群创建之后，无法更改子网组。

参数组

选择一个集群参数组，以便与集群相关联。如果您不选择参数组，集群将使用默认参数组。

加密

选择是否要加密集群内的所有数据及其快照。如果保留默认设置 None，将不会启用加密功能。如果您要启用加密功能，请选择您是使用 Amazon Key Management Service (Amazon KMS)，还是使用硬件安全模块 (HSM)，然后配置相关设置。有关 Amazon Redshift 中的加密功能的更多信息，请参阅Amazon Redshift 数据库加密 (p. 347)。

- KMS

  如果您想启用加密并使用 Amazon KMS 来管理您的加密密钥，请选择 Use Amazon Key Management Service (Amazon KMS) [使用 Amazon Key Management Service（Amazon KMS）]。此外还需选择要使用的密钥。您可以选择原定设置密钥、当前账户中的密钥，或其他账户中的密钥。

  Note

  如果想使用来自其他 Amazon 账户的密钥，则输入要使用的密钥的 Amazon Resource Name（ARN）。您必须拥有使用此密钥的权限。有关在 Amazon KMS 中访问密钥的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的控制对您的密钥的访问。

  有关使用 Amazon Redshift 中的 Amazon KMS 加密密钥的更多信息，请参阅使用 Amazon KMS 为 Amazon Redshift 进行数据库加密 (p. 348)。

- HSM

  如果您要启用加密功能并使用硬件安全模块 (HSM) 来管理加密密钥，请选择 HSM。

  如果选择 HSM，请从 HSM 连接和 HSM 客户端证书中选择相应值。Amazon Redshift 和 HSM 需要使用这些值来构建受信任的连接，以便通过此连接传输集群密钥。必须先在 Amazon Redshift 中设置 HSM 连接和客户端证书，之后再启动集群。有关设置 HSM 连接和客户端证书的更多信息，请参阅使用硬件安全模块的 Amazon Redshift 加密 (p. 349)。

Maintenance track (维护跟踪

您可以选择使用的集群版本为 Current (当前)、Trailing (尾随) 或（有时）Preview (预览) 跟踪。

监控

可以选择是否创建 CloudWatch 警报。

Configure cross-region snapshot (配置跨区域快照

您可以选择是否启用跨区域快照。

Automated Snapshot Retention Period（自动快照保留期）

您可以选择这些快照的保留天数（最多 35 天）。如果节点类型为 DC2 或 DS2，则可以选择零 (0) 天以便不创建自动快照。

Manual snapshot retention period（手动快照保留期）

您可以选择天数或 `Indefinitely` 来保留这些快照。

修改集群

当您修改集群时，对以下选项做出的更改将立即生效：

- VPC 安全组
- 公开访问
- 管理员用户密码
- HSM 连接
- HSM 客户端证书
- 维护详细信息
- Snapshot preferences (快照首选项

对以下选项做出的更改只能在重启集群后才会生效：

- 集群标识符

  当您更改集群标识符时，Amazon Redshift 会自动重新启动集群。
- 增强型 VPC 路由

  当您更改增强型 VPC 路由时，Amazon Redshift 会自动重新启动集群。
- 集群参数组

如果您缩短自动快照的保留期，系统将删除保留期设置超出了新保留期的现有自动快照。有关更多信息，请参阅Amazon Redshift 快照 (p. 318)。

有关集群属性的更多信息，请参阅其他配置 (p. 85)。

修改集群

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 选择要修改的集群。
4. 选择编辑。此时将显示 Edit cluster（编辑集群）页面。
5. 更新集群属性。您可以修改的一些属性包括：

   - 集群标识符
   - 快照保留
   - 集群重新定位

   要编辑 Network and security（网络和安全）、Maintenance（维护）和 Database configurations（数据库配置）的设置，控制台将提供指向相应集群详细信息选项卡的链接。
6. 选择保存更改。

删除集群

如果不再需要您的集群，可将其删除。如果您打算使用与要删除的集群相同的数据和配置来预配置新集群，您将需要使用手动快照。通过使用手动快照，您可以稍后还原快照并恢复使用集群。如果您删除了集群但没有创建最终手动快照，则将删除集群数据。无论采用哪种方式，自动快照都将在删除集群后被删除，但所有

手动快照将保留下来，直到您将它们删除。根据您为集群的 Amazon Redshift 快照所使用的存储的数量，您可能需要为手动快照支付 Amazon Simple Storage Service 存储费。有关更多信息，请参阅关闭和删除集群 (p. 74)。

删除集群

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 选择要删除的集群。
4. 对于 Actions (操作)，选择 Delete (删除)。此时将显示 Delete cluster (删除集群) 页面。
5. 选择 Delete Cluster (删除集群)。

重新引导集群

重启集群后，集群状态将设置为 `rebooting`，并在重启完成后创建一个集群事件。任何待处理的集群修改都将在此次重启时应用。

重启集群

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 选择要重启的集群。
4. 对于 Actions (操作)，选择 Reboot cluster (重启集群)。此时将显示 Reboot cluster (重启集群) 页面。
5. 选择 Reboot cluster (重启集群)。

调整集群大小

调整集群大小时，您可以指定与集群当前配置不同的节点数量或节点类型。当集群处于调整大小过程中时，您将无法在集群上运行任何写入或读取/写入查询；您只可以运行读取查询。

有关调整集群大小的更多信息（包括使用不同方法调整集群大小的过程），请参阅在 Amazon Redshift 中调整集群大小 (p. 65)。

调整集群大小

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 选择要调整大小的集群。
4. 对于 Actions (操作)，选择 Resize (调整大小)。此时将显示 Resize cluster (调整集群大小) 页面。
5. 按照页面上的说明操作。您可以立即调整集群大小，在特定时间调整一次，或者按计划增加和减小集群大小。
6. 根据您的选择，选择 Resize now (立即调整大小) 或 Schedule resize (计划调整大小)。

如果您有预留节点，例如 DS2 预留节点，则可以升级到 RA3 预留节点。使用控制台从快照还原或执行弹性调整大小时，您可以执行此操作。您可以使用控制台引导您完成此过程。有关升级到 RA3 节点的更多信息，请参阅升级到 RA3 节点类型。

升级集群的发行版本

您可以升级 Release Status (版本状态) 值为 New release available (有新版本可用) 的集群的发布维护版本。在升级维护版本时，可以选择是立即升级还是在下一个维护时段升级。

Important

如果选择立即升级，您的集群将处于脱机状态，直到升级完成。

将集群升级到新的发布版本

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 选择要升级的集群。
4. 对于 Actions (操作)，选择 Upgrade cluster version (升级集群版本)。这将显示 Upgrade cluster version (升级集群版本) 页面。
5. 按照页面上的说明操作。
6. 选择 Upgrade cluster version (升级集群版本)。

获取有关集群配置的信息

显示有关集群的信息

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后从列表中选择集群名称以打开其详细信息。此时将显示集群的详细信息，其中包括 Cluster performance（集群性能）、Query monitoring（查询监控）、Databases（数据库）、Datashares（数据共享）、Schedules（计划）、Maintenance（维护）和 Properties（属性）选项卡。
3. 选择每个选项卡可查看更多详细信息。

获取集群状态概述

查看集群的状态

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 在 Status (状态) 列中查看集群的状态。

创建集群快照

创建集群的快照

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 选择要为其创建快照的集群。

4. 对于 Actions (操作)，选择 Create snapshot (创建快照)。此时会显示 Create snapshot (创建快照) 页面。
5. 按照页面上的说明操作。
6. 选择 Create snapshot (创建快照)。

创建或编辑磁盘空间警报

为集群创建磁盘空间用量警报

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Alarms（告警）。
3. 对于 Actions (操作)，选择 Create alarm (创建警报)。此时将显示 Create alarm (创建警报) 页面。
4. 按照页面上的说明操作。
5. 选择创建警报。

使用集群性能数据

在控制台中，您可以使用集群详细信息页面的 Cluster performance（集群性能）选项卡上的集群性能。

使用 Amazon CLI 和 Amazon Redshift API 管理集群

您可以使用以下 Amazon CLI 操作来管理 Amazon Redshift 中的集群。

- 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

您可以使用以下 Amazon Redshift API 操作来管理集群。

- CancelResize
- CreateCluster
- DeleteCluster
- DescribeClusters
- DescribeClusterVersions
- DescribeNodeConfigurationOptions

- DescribeResize
- DescribeOrderableClusterOptions
- ModifyCluster
- PauseCluster
- RebootCluster
- ResizeCluster
- ResumeCluster

使用 Amazon SDK for Java 管理集群

以下 Java 代码示例演示了常见的集群管理操作，其中包括：

- 创建集群。
- 列出与集群有关的元数据。
- 修改配置选项。

提出创建集群的请求之后，您必须等到集群处于 `available` 状态后才能对其进行修改。本示例通过 `describeClusters` 方法，使用循环来定期检查集群的状态。当集群可供使用时，集群的首选维护时段会发生变化。

有关运行以下示例的分步说明，请参阅 使用 Eclipse 运行 Amazon Redshift 的 Java 示例 (p. 464)。您需要更新代码并指定集群标识符。

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
 */

// snippet-sourcedescription:[CreateAndModifyCluster demonstrates how to create and modify
 an Amazon Redshift cluster.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[CreateCluster]
// snippet-keyword:[DescribeClusters]
// snippet-keyword:[ModifyCluster]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-02-01]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.CreateAndModifyCluster.complete]

package com.amazonaws.services.redshift;

import java.io.IOException;
```

```
import com.amazonaws.services.redshift.AmazonRedshift;
import com.amazonaws.services.redshift.AmazonRedshiftClientBuilder;
import com.amazonaws.services.redshift.model.*;

public class CreateAndModifyCluster {

    public static AmazonRedshift client;
    public static String clusterIdentifier = "***provide a cluster identifier***";
    public static long sleepTime = 20;

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
 com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
        client = AmazonRedshiftClientBuilder.defaultClient();

        try {
            createCluster();
            waitForClusterReady();
            describeClusters();
            modifyCluster();
            describeClusters();
        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }

    private static void createCluster() {
        CreateClusterRequest request = new CreateClusterRequest()
                .withClusterIdentifier(clusterIdentifier)
                .withMasterUsername("masteruser")
                .withMasterUserPassword("12345678Aa")
                .withNodeType("ds2.xlarge")
                .withNumberOfNodes(2)
                .withClusterSubnetGroupName("subnetgroup1");


        Cluster createResponse = client.createCluster(request);
        System.out.println("Created cluster " + createResponse.getClusterIdentifier());
    }

    private static void describeClusters() {
        DescribeClustersRequest request = new DescribeClustersRequest()
                .withClusterIdentifier(clusterIdentifier);

        DescribeClustersResult result = client.describeClusters(request);
        printResult(result);
    }

    private static void modifyCluster() {
        ModifyClusterRequest request = new ModifyClusterRequest()
                .withClusterIdentifier(clusterIdentifier)
                .withPreferredMaintenanceWindow("wed:07:30-wed:08:00");

        client.modifyCluster(request);
        System.out.println("Modified cluster " + clusterIdentifier);

    }

    private static void printResult(DescribeClustersResult result)
    {
        if (result == null)
        {
            System.out.println("Describe clusters result is null.");
            return;
```

```
        }

        System.out.println("Cluster property:");
        System.out.format("Preferred Maintenance Window: %s\n",
 result.getClusters().get(0).getPreferredMaintenanceWindow());
    }

    private static void waitForClusterReady() throws InterruptedException {
        Boolean clusterReady = false;
        System.out.println("Wating for cluster to become available.");
        while (!clusterReady) {
            DescribeClustersResult result = client.describeClusters(new
 DescribeClustersRequest()

 .withClusterIdentifier(clusterIdentifier));
            String status = (result.getClusters()).get(0).getClusterStatus();
            if (status.equalsIgnoreCase("available")) {
                clusterReady = true;
            }
            else {
                System.out.print(".");
                Thread.sleep(sleepTime*1000);
            }
        }
    }
}
// snippet-end:[redshift.java.CreateAndModifyCluster.complete]
```

在 VPC 中管理集群

主题

- 概览 (p. 92)
- 在 VPC 中创建集群 (p. 93)
- 管理集群的 VPC 安全组 (p. 94)
- Amazon Redshift 集群子网组 (p. 95)

概览

Amazon Redshift 支持 EC2-VPC 和 EC2-Classic 平台以在 Virtual Private Cloud (VPC) 中基于 Amazon VPC 服务启动集群。有关更多信息，请参阅在创建集群时使用 EC2-VPC (p. 54)。

> Note
>
> Amazon Redshift 支持在专用租赁 VPC 中启动集群。有关更多信息，请参阅 Amazon VPC 用户指南中的专用实例。

在 VPC 中预配置集群时，您需要执行以下操作：

- 提供有关 VPC 的信息。

  在请求 Amazon Redshift 在您的 VPC 中创建集群时，您必须通过创建一个集群子网组来提供您的 VPC 信息。此信息包括 VPC ID 和 VPC 中的子网列表，启动集群时，您需要提供集群子网组，以便 Amazon Redshift 能够在 VPC 内的其中一个子网中预置您的集群。有关在 Amazon Redshift 中创建子网组的更多信息，请参阅Amazon Redshift 集群子网组 (p. 95)。有关设置 VPC 的更多信息，请参阅 Amazon VPC 入门指南中的 Amazon VPC 入门。
- （可选）配置可公开访问的选项。

如果您将集群配置为可公开访问，则还可以选择用于外部 IP 地址的弹性 IP 地址。弹性 IP 地址是与您的 Amazon 账户关联的静态 IP 地址。您可以使用弹性 IP 地址从 VPC 外部连接到您的集群。借助弹性 IP 地址，您可以更改自己的基本配置，而不影响客户端用来连接到您的集群的 IP 地址。在某些情况下（如在故障后进行恢复时），这种方法会很有用。

如果您希望使用与自己的 Amazon 账户相关联的弹性 IP 地址，则必须先在 Amazon EC2 中进行创建，然后再启动 Amazon Redshift 集群。否则，您在启动过程中将无法使用它。您也可以让 Amazon Redshift 配置用于 VPC 的弹性 IP 地址。不过，分配的弹性 IP 地址由 Amazon Redshift 服务托管，并且不与您的 Amazon 账户关联。有关更多信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中的弹性 IP 地址。

在某些情况下，您可能在 VPC 中有可公开访问的集群，并且希望使用该 VPC 内的私有 IP 地址连接到此集群。如果是这样的话，则必须将下列 VPC 参数设置为 `true`：

- `DNS resolution`
- `DNS hostnames`

假设您在 VPC 中有可公开访问的集群，但不在 VPC 中将这些参数设置为 `true`。在这些情况下，从 VPC 内部进行的连接将解析为集群的弹性 IP 地址，而不是私有 IP 地址。建议您将这些参数设置为 `true`，并使用私有 IP 地址从该 VPC 中连接到可公开访问的集群。有关更多信息，请参阅 Amazon VPC 用户指南中的在 VPC 中使用 DNS。

> **Note**
>
> 如果您在 VPC 中有可公开访问的集群，则在您调整该集群的大小之前，从该 VPC 中发出的连接将继续使用弹性 IP 地址连接到集群。即使设置了前面的参数，也会发生此情况。从同一 VPC 中连接到可公开访问的集群时，任何新集群都将遵循使用私有 IP 地址这一新行为。

弹性 IP 地址是用于访问 VPC 外部集群的外部 IP 地址。它与集群节点公有 IP 地址和私有 IP 地址（显示在 Amazon Redshift 控制台中的 Connection details（连接详细信息）下）不相关。无论集群是否可公开访问，公有和私有集群节点 IP 地址都会显示。它们仅在某些情况下用于配置远程主机上的入口规则。在使用安全外壳 (SSH) 连接从 Amazon EC2 实例或其他远程主机加载数据时，会发生这些情况。有关更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的步骤 1：检索集群公有密钥和集群节点 IP 地址。

在您创建集群或从快照还原集群时，将集群与弹性 IP 地址相关联的选项可用。在某些情况下，您可能需要将集群与弹性 IP 地址关联，或更改与集群关联的弹性 IP 地址。要在创建集群后附加弹性 IP 地址，请首先更新集群，使其不可公开访问，然后在同一个操作中使其可公开访问并添加弹性 IP 地址。

- 关联 VPC 安全组。

  然后，您可以使用 VPC 安全组授予入站访问权限。此 VPC 安全组必须允许通过数据库端口访问集群，以便您能够使用 SQL 客户端工具连接到集群。您可以提前配置此安全组，也可以在启动集群后向其添加规则。有关更多信息，请参阅 Amazon VPC 用户指南中的您的 VPC 的安全性。您无法使用 Amazon Redshift 集群安全组来授予针对该集群的入站访问权限。

有关使用 VPC 中的集群的更多信息，请参阅在 VPC 中创建集群 (p. 93)。

还原 VPC 中的集群的快照

只能在 VPC 内部还原 VPC 中的集群快照，而不能在 VPC 外部。您可以在同一 VPC 中或您账户中的其他 VPC 中还原快照。有关 快照的更多信息，请参阅 Amazon Redshift 快照 (p. 318)。

在 VPC 中创建集群

以下是如何在 Virtual Private Cloud (VPC) 中部署集群的一般步骤。

要在 VPC 中创建集群，请执行以下操作：

1. 设置 VPC。

您可以在账户的默认 VPC（如果您的账户有的话）中或您创建的 VPC 中创建集群。有关更多信息，请参阅在创建集群时使用 EC2-VPC (p. 54)。要创建默认 VPC，请参阅《Amazon VPC 用户指南》中的创建 VPC。记下 VPC 标识符、子网和子网的可用区。您在启动集群时需要使用这些信息。

Note

您必须在自己的 VPC 中至少定义一个子网，以便您在下一步中将其添加到集群子网组。有关将子网添加到 VPC 的更多信息，请参阅 Amazon VPC 用户指南中的将子网添加到 VPC 中。

2. 创建 Amazon Redshift 集群子网组，以指定 Amazon Redshift 集群可在 VPC 中使用的子网。

   您可以使用 Amazon Redshift 控制台或以编程方式创建集群子网组。有关更多信息，请参阅Amazon Redshift 集群子网组 (p. 95)。
3. 在您要将其与集群相关联的 VPC 安全组中，授予针对入站连接的访问权限。

   您可以允许 VPC 外部（在公共 Internet 上）的客户端连接到集群。为此，请将集群与一个 VPC 安全组关联，该安全组授予对启动集群时使用的端口的入站访问权限。有关安全组规则的示例，请参阅 Amazon VPC 用户指南中的安全组规则。
4. 按《Amazon Redshift 入门指南》中的开始使用 Amazon Redshift 中的步骤操作，以创建集群。创建集群时进行以下修改：

   - 要显示 Additional configurations (其他配置) 部分，请关闭 Use defaults (使用默认值)。
   - 在 Network and security（网络和安全性）部分中，指定您设置的 Virtual Private Cloud（VPC）、Cluster subnet group（集群子网组）和 VPC security group（VPC 安全组）。

您现在可以使用该集群。您可以按照“入门”步骤操作，通过上传示例数据并尝试示例查询来测试集群。

管理集群的 VPC 安全组

在您预置 Amazon Redshift 集群时，它默认处于锁定状态，因此任何人都无法访问。要为其他用户授予针对 Amazon Redshift 集群的入站访问权限，您可以将该集群与安全组关联起来。如果您处于 EC2-VPC 平台上，则可使用现有的 Amazon VPC 安全组或者定义一个新的安全组。然后将它与集群关联，如下所述。如果您处于 EC2-Classic 平台上，您可以定义一个集群安全组，并将其与集群关联。有关在 EC2-Classic 平台上使用集群安全组的更多信息，请参阅Amazon Redshift 集群安全组 (p. 458)。

VPC 安全组中包含一组规则，用于控制对 VPC 上实例（如您的集群）的访问。各个规则根据 IP 地址范围或其他 VPC 安全组设置访问权限。当您将 VPC 安全组与集群关联后，在 VPC 安全组中定义的规则即可控制对集群的访问。

您在 EC2-VPC 平台上预置的每个集群均拥有一个或多个与其关联的 Amazon VPC 安全组。Amazon VPC 提供一个名为 default 的 VPC 安全组，该安全组是在您创建 VPC 时自动创建的。如果您在创建集群时未指定其他 VPC 安全组，则您在 VPC 内启动的每个集群都会自动与默认 VPC 安全组关联。您可以在创建集群时将 VPC 安全组与之关联，也可以稍后通过修改该集群再将 VPC 安全组与之关联。

下表介绍了默认 VPC 安全组的默认规则。

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

您可以视需要针对您的 Amazon Redshift 集群更改默认 VPC 安全组的规则。

如果默认 VPC 安全组足以满足您的需求，则无需创建更多 VPC 安全组。不过，您可以选择创建其他 VPC 安全组，以便更好地管理针对您的集群的入站访问权限。例如，假设您正在 Amazon Redshift 集群上运行一

项服务，向客户提供多种不同的服务水平。如果您不希望在所有服务级别提供相同的访问权限，则可能需要创建单独的 VPC 安全组，每种服务级别一个。然后，您可以将这些 VPC 安全组与您的集群关联起来。

您可以为一个 VPC 创建最多 100 个 VPC 安全组，并将一个 VPC 安全组与许多集群关联。不过，您最多只能将五个 VPC 安全组与一个给定集群关联。

Amazon Redshift 可将更改即时应用到 VPC 安全组。因此，如果您已将该 VPC 安全组与某个集群关联，则更新后的 VPC 安全组中的入站集群访问规则将立即应用。

您可以在 https://console.aws.amazon.com/vpc/ 上创建和修改 VPC 安全组。您还可以使用 Amazon CLI、Amazon EC2 CLI 和 Amazon Tools for Windows PowerShell 以编程方式管理 VPC 安全组。有关使用 VPC 安全组的更多信息，请参阅 Amazon VPC 用户指南中的您的 VPC 的安全组。

Amazon Redshift 集群子网组

概览

如果您要在 Virtual Private Cloud (VPC) 中配置集群，则可以创建集群子网组。有关 VPC 的更多信息，请参阅 Amazon VPC 产品详细信息页面。

您的 VPC 可以有一个或多个子网，这是您的 VPC 中的一部分 IP 地址，使您能够根据安全和操作需求对资源进行分组。您可以通过集群子网组在 VPC 中指定一组子网。在预置集群时，您可以提供子网组，而 Amazon Redshift 在该子网组内的其中一个子网上创建集群。

有关创建 VPC 的更多信息，请转到 Amazon VPC 用户指南文档。

创建子网组之后，您可以删除之前添加的子网，也可以添加更多子网。Amazon Redshift 提供 API 操作，可用于创建、修改或删除集群子网组。您也可以在控制台中执行这些操作。

使用控制台管理集群子网组

您可以使用 Amazon Redshift 控制台管理您的集群子网组。您可以创建集群子网组，管理现有的集群子网组或者删除集群子网组。所有这些任务都从集群子网组列表开始。您必须选择一个集群子网组才能进行管理。

您可以在您提供子网组的其中一个子网上预置集群。您可以通过集群子网组在 Virtual Private Cloud (VPC) 中指定一组子网。

创建集群子网组

您必须定义至少一个集群子网组，才能在 VPC 中配置集群。

创建集群子网组

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Configurations（配置），然后选择 Subnet groups（子网组）。此时将显示子网组列表。
3. 选择 Create cluster subnet group（创建集群子网组）以显示创建页面。
4. 输入子网组的信息，包括要添加的子网。
5. 选择 Create cluster subnet group（创建集群子网组）创建包含您选择的子网的组。

修改集群子网组

修改集群子网组

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。

2. 在导航菜单上，选择 Configurations（配置），然后选择 Subnet groups（子网组）。此时将显示子网组列表。
3. 选择要修改的子网组。
4. 对于 Actions（操作），选择 Modify（修改）以显示子网组的详细信息。
5. 更新子网组的信息。
6. 选择 Save（保存）以修改组。

删除集群子网组

您无法删除集群正在使用的集群子网组。

删除集群子网组

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Configurations（配置），然后选择 Subnet groups（子网组）。此时将显示子网组列表。
3. 选择要删除的子网组，然后选择 Delete（删除）。

使用 Amazon SDK for Java 管理集群子网组

以下 Java 代码示例演示了常见的集群子网操作，其中包括：

- 创建集群子网组。
- 列出集群子网组的元数据。
- 修改集群子网组。

有关运行以下示例的分步说明，请参阅 使用 Eclipse 运行 Amazon Redshift 的 Java 示例 (p. 464)。您需要更新代码并提供集群子网组的名称和两个子网标识符。

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
*/

// snippet-sourcedescription:[CreateAndModifyClusterSubnetGroup demonstrates how to create
 and modify an Amazon Redshift subnet group.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[CreateClusterSubnetGroup]
// snippet-keyword:[DescribeClusterSubnetGroups]
```

```
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-02-01]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.CreateAndModifyClusterSubnetGroup.complete]
package com.amazonaws.services.redshift;

import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

import com.amazonaws.services.redshift.model.*;

public class CreateAndModifyClusterSubnetGroup {

    public static AmazonRedshift client;
    public static String clusterSubnetGroupName = "subnet-group-name";
    // You can use the VPC console to find subnet IDs to use.
    public static String subnetId1 = "***provide a subnet ID****";
    public static String subnetId2 = "***provide a subnet ID****";

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
 com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
       client = AmazonRedshiftClientBuilder.defaultClient();

        try {
             createClusterSubnetGroup();
             describeClusterSubnetGroups();
             modifyClusterSubnetGroup();
        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }

    private static void createClusterSubnetGroup() {
        CreateClusterSubnetGroupRequest request = new CreateClusterSubnetGroupRequest()
            .withClusterSubnetGroupName(clusterSubnetGroupName)
            .withDescription("my cluster subnet group")
            .withSubnetIds(subnetId1);
        client.createClusterSubnetGroup(request);
        System.out.println("Created cluster subnet group: " + clusterSubnetGroupName);
    }

    private static void modifyClusterSubnetGroup() {
        // Get existing subnet list.
        DescribeClusterSubnetGroupsRequest request1 = new
 DescribeClusterSubnetGroupsRequest()
            .withClusterSubnetGroupName(clusterSubnetGroupName);
        DescribeClusterSubnetGroupsResult result1 =
 client.describeClusterSubnetGroups(request1);
        List<String> subnetNames = new ArrayList<String>();
        // We can work with just the first group returned since we requested info about one
 group.
        for (Subnet subnet : result1.getClusterSubnetGroups().get(0).getSubnets()) {
            subnetNames.add(subnet.getSubnetIdentifier());
        }
        // Add to existing subnet list.
        subnetNames.add(subnetId2);

        ModifyClusterSubnetGroupRequest request = new ModifyClusterSubnetGroupRequest()
            .withClusterSubnetGroupName(clusterSubnetGroupName)
            .withSubnetIds(subnetNames);
        ClusterSubnetGroup result2 = client.modifyClusterSubnetGroup(request);
        System.out.println("\nSubnet group modified.");
        printResultSubnetGroup(result2);
```

```
    }


    private static void describeClusterSubnetGroups() {
        DescribeClusterSubnetGroupsRequest request = new
 DescribeClusterSubnetGroupsRequest()
        .withClusterSubnetGroupName(clusterSubnetGroupName);

    DescribeClusterSubnetGroupsResult result = client.describeClusterSubnetGroups(request);
    printResultSubnetGroups(result);
    }

    private static void printResultSubnetGroups(DescribeClusterSubnetGroupsResult result)
    {
        if (result == null)
        {
            System.out.println("\nDescribe cluster subnet groups result is null.");
            return;
        }

        for (ClusterSubnetGroup group : result.getClusterSubnetGroups())
        {
            printResultSubnetGroup(group);
        }

    }
    private static void printResultSubnetGroup(ClusterSubnetGroup group) {
        System.out.format("Name: %s, Description: %s\n", group.getClusterSubnetGroupName(),
 group.getDescription());
        for (Subnet subnet : group.getSubnets()) {
            System.out.format("  Subnet: %s, %s, %s\n", subnet.getSubnetIdentifier(),
                    subnet.getSubnetAvailabilityZone().getName(),
 subnet.getSubnetStatus());
        }
    }
}
// snippet-end:[redshift.java.CreateAndModifyClusterSubnetGroup.complete]
```

使用 Amazon CLI 和 Amazon Redshift API 管理集群子网组

您可以使用以下 Amazon Redshift CLI 操作来管理集群子网组。

- create-cluster-subnet-group
- delete-cluster-subnet-group
- describe-cluster-subnet-groups
- modify-cluster-subnet-group

您可以使用以下 Amazon Redshift API 操作来管理集群子网组。

- CreateClusterSubnetGroup
- DeleteClusterSubnetGroup
- DescribeClusterSubnetGroups
- ModifyClusterSubnetGroup

集群版本历史记录

Amazon Redshift 会定期发布用于更新集群的新集群版本。

Important

有关可用 Amazon Redshift 集群版本及其功能、改进和修复的信息，请参阅 Amazon Redshift 的集群版本 (p. 523)。

查询数据库

要查询 Amazon Redshift 集群托管的数据库，您有两种选择：

- 连接到您的集群，并使用查询编辑器在 Amazon Web Services Management Console上运行查询。

  如果您在 Amazon Redshift 控制台上使用查询编辑器，则无需下载和设置 SQL 客户端应用程序。
- 通过 SQL 客户端工具（如 SQL Workbench/J）连接到集群。

  Amazon Redshift 支持通过 Java 数据库连接 (JDBC) 和开放式数据库连接 (ODBC) 来连接 SQL 客户端工具。Amazon Redshift 不提供或安装任何 SQL 客户端工具或库，因此您必须将其安装到您的客户端计算机或 Amazon EC2 实例上才能使用它们。您可以使用支持 JDBC 或 ODBC 驱动程序的大多数 SQL 客户端工具。

  Note

  在编写存储过程时，我们建议使用最佳实践来保护敏感值：
  不要在存储过程逻辑中对任何敏感信息进行硬编码。例如，不要在存储过程主体的 CREATE USER 语句中分配用户密码。这会带来安全风险，因为硬编码值可以作为架构元数据记录在目录表中。而是应通过参数将诸如密码之类的敏感值作为参量传递给存储过程。
  有关存储过程的更多信息，请参阅 CREATE PROCEDURE 和在 Amazon Redshift 中创建存储过程。有关目录表的更多信息，请参阅系统目录表。

主题

- 使用 Amazon Redshift 查询编辑器 v2 查询数据库 (p. 100)
- 使用查询编辑器查询数据库 (p. 128)
- 使用 SQL 客户端工具连接到 Amazon Redshift 集群 (p. 135)
- 使用 Amazon Redshift 数据 API (p. 267)

使用 Amazon Redshift 查询编辑器 v2 查询数据库

查询编辑器 v2 是一个单独的基于 Web 的 SQL 客户端应用程序，用于在 Amazon Redshift 数据仓库上创作和运行查询。您可以在图表中可视化结果，并通过与团队中的其它人共享查询来进行协作。查询编辑器 v2 是以前的查询编辑器的替代品。

Note

查询编辑器 v2 已在 Amazon Redshift 可用的商业 Amazon Web Services 区域中推出，但中东（阿联酋）（me-central-1）除外。它也已在中国 Amazon Web Services 区域推出。

要了解查询编辑器 v2 的演示，请观看以下视频。Amazon Redshift 查询编辑器 v2。

要了解数据分析的演示，请观看以下视频。使用 Amazon Redshift 查询编辑器 v2 进行数据分析。

有关使用查询编辑器 v2 通过隔离或共享连接运行多个查询的演示，请观看以下视频。使用查询编辑器 v2 执行并发查询。

查询编辑器 v2 具有一组丰富的功能来管理和运行 SQL 语句。以下各部分中的主题可让您使用其中的许多功能。请亲自浏览查询编辑器 v2 以熟悉其功能。

主题

- 配置您的 Amazon Web Services 账户 (p. 101)
- 使用查询编辑器 v2 (p. 106)
- 编写和运行查询 (p. 115)
- 查询数据湖 (p. 118)
- 使用数据共享 (p. 121)
- 可视化查询结果 (p. 123)
- 以团队形式协作和共享 (p. 127)

配置您的 Amazon Web Services 账户

当您从 Amazon Redshift 控制台中选择查询编辑器 v2 时，浏览器将打开新选项卡，其中包含查询编辑器 v2 界面。使用适当的权限，您可以访问当前 Amazon Web Services 区域中您的 Amazon Web Services 账户拥有的 Amazon Redshift 集群或工作组中的数据。

管理员第一次为您的 Amazon Web Services 账户配置查询编辑器 v2 时，他们会选择用于加密查询编辑器 v2 资源的 Amazon KMS key。默认情况下，Amazon 拥有的密钥用于加密资源。或者，管理员可在配置页面中为密钥选择 Amazon Resource Name（ARN）来使用客户托管式密钥。配置账户后，Amazon KMS 无法更改加密设置。

有关通过查询编辑器 v2 创建和使用客户托管式密钥的更多信息，请参阅创建用于查询编辑器 v2 的 Amazon KMS 客户托管式密钥 (p. 101)。

Amazon Redshift 查询编辑器 v2 支持身份验证、加密、隔离和合规性，以确保静态数据和传输中的数据安全。有关数据安全性和查询编辑器 v2 的更多信息，请参阅以下内容：

- 静态加密 (p. 346)
- 传输中加密 (p. 354)
- Amazon Redshift 中的配置和漏洞分析 (p. 461)

查询编辑器 v2 对其部分资源具有可调配额。有关更多信息，请参阅Amazon Redshift 对象的配额 (p. 514)。

使用查询编辑器 v2 创建的资源

在查询编辑器 v2 中，您可以创建资源，例如保存的查询和图表。查询编辑器 v2 中的所有资源都与 IAM 角色或 IAM 用户关联。

在查询编辑器 v2 中，您可以添加和删除已保存查询和图表的标签。您可以在设置自定义 IAM policy 或搜索资源时使用这些标签。您还可以使用 Amazon Resource Groups 标签编辑器来管理标签。

您可以使用 IAM policy 设置 IAM 角色和 IAM 用户，以便与 Amazon Web Services 区域中相同 Amazon Web Services 账户 中的其它人共享查询。

创建用于查询编辑器 v2 的 Amazon KMS 客户托管式密钥

创建对称加密客户托管式密钥：

使用 Amazon KMS 控制台或 Amazon KMS API 操作，您可以创建对称加密客户托管式密钥来加密查询编辑器 v2 资源。有关创建密钥的说明，请参阅《Amazon Key Management Service 开发人员指南》中的创建对称加密 Amazon KMS 密钥。

密钥策略

密钥策略控制对客户托管式密钥的访问。每个客户托管式密钥必须只有一个密钥策略，其中包含确定谁可以使用密钥以及如何使用密钥的声明。创建客户托管式密钥时，可以指定密钥策略。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的管理对 Amazon KMS 密钥的访问。

要将您的客户托管式密钥与 Amazon Redshift 查询编辑器 v2 一起使用，密钥策略中必须允许以下 API 操作：

- `kms:GenerateDataKey` – 生成唯一的对称数据密钥以加密您的数据。
- `kms:Decrypt` – 解密客户托管式密钥加密的数据。
- `kms:DescribeKey` – 提供客户托管式密钥详细信息以允许验证密钥服务。

以下是 Amazon Web Services 账户 `111122223333` 的示例 Amazon KMS 策略。在第一部分中，`kms:ViaService` 限制对查询编辑器 v2 服务的密钥使用（在策略中名为 `sqlworkbench.region.amazonaws.com`）。使用密钥的 Amazon Web Services 账户 必须为 `111122223333`。在第二部分中，Amazon Web Services 账户 `111122223333`的根用户和主要管理员可以访问密钥。

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

以下资源提供有关 Amazon KMS 密钥的更多信息：

- 有关 Amazon KMS 策略的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的在策略中指定权限。

- 有关 Amazon KMS 策略故障排除的信息，请参阅《Amazon Key Management Service 开发人员指南》中的密钥访问故障排除。
- 有关密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Amazon KMS 密钥。

访问查询编辑器 v2

如要访问查询编辑器 v2，您需要相应权限。管理员可以将下面的任何一种 Amazon 托管式策略附加到该 IAM 用户或角色以授予权限。这些 Amazon 托管式策略使用不同的选项编写，可控制标记资源允许共享查询的方式。您可以使用 IAM 控制台 (https://console.aws.amazon.com/iam/) 附加 IAM policy。

- AmazonRedshiftQueryEditorV2FullAccess – 授予 Amazon Redshift 查询编辑器 v2 操作和资源的完全访问权限。此策略还授予访问其它所需服务的权限。
- AmazonRedshiftQueryEditorV2NoSharing – 授予在不共享资源的情况下使用 Amazon Redshift 查询编辑器 v2 的权限。此策略还授予访问其它所需服务的权限。
- AmazonRedshiftQueryEditorV2ReadSharing – 授予在共享有限制资源的情况下使用 Amazon Redshift 查询编辑器 v2 的权限。授予主体可以阅读与其团队共享的资源，但无法更新它们。此策略还授予访问其它所需服务的权限。
- AmazonRedshiftQueryEditorV2ReadWriteSharing – 授予在共享资源的情况下使用 Amazon Redshift 查询编辑器 v2 的权限。授予主体可以读取和更新与其团队共享的资源。此策略还授予访问其它所需服务的权限。

您还可以根据提供的托管式策略中允许和拒绝的权限创建您自己的策略。如果您使用 IAM 控制台策略编辑器创建自己的策略，请选择 SQL Workbench 作为您在可视化编辑器中创建策略的服务。查询编辑器 v2 使用可视化编辑器和 IAM policy simulator 中的服务名称 Amazon SQL Workbench。

如使主体（IAM 用户或 IAM 角色）连接到 Amazon Redshift 集群，他们需要一个查询编辑器 v2 托管式策略中的权限。他们还需要对集群的 `redshift:GetClusterCredentials` 权限。要获得此权限，具有管理权限的人员可以使用临时证书将策略附上到需要连接到集群的 IAM 用户或 IAM 角色。您可以将策略范围限定为特定集群，也可以设为常规范围。有关使用临时证书权限的更多信息，请参阅创建有权调用 GetClusterCredentials 的 IAM 角色或用户 (p. 395)。

为了让主体（IAM 用户或 IAM 角色）能够在 Account settings（账户设置）页面中为账户中的其他人启用 Export result set（导出结果集）的功能，他们需要 `sqlworkbench:UpdateAcountExportSettings` 权限。此权限包含在 `AmazonRedshiftQueryEditorV2FullAccess` Amazon 托管式策略中。

要使主体（IAM 用户或 IAM 角色）使用 SQL Notebook（预览版）功能，您必须将以下策略添加到委托人的现有查询编辑器 v2 托管式策略之中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
            "Effect": "Allow",
            "Action": [
                "sqlworkbench:ListNotebooks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
            "Effect": "Allow",
            "Action": [
                "sqlworkbench:CreateNotebook"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/sqlworkbench-resource-owner": "${aws:userid}"
                }
            }
        },
        {
            "Sid": "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
            "Effect": "Allow",
            "Action": [
                "sqlworkbench:GetNotebook",
                "sqlworkbench:UpdateNotebook",
                "sqlworkbench:DeleteNotebook",
                "sqlworkbench:CreateNotebookCell",
                "sqlworkbench:DeleteNotebookCell",
                "sqlworkbench:UpdateNotebookCellContent",
                "sqlworkbench:UpdateNotebookCellLayout",
                "sqlworkbench:BatchGetNotebookCell",
                "sqlworkbench:AssociateNotebookWithTab"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/sqlworkbench-resource-owner": "${aws:userid}"
                }
            }
        },
        {
            "Sid": "AmazonRedshiftQueryEditorV2TeamReadAccessPermissions",
            "Effect": "Allow",
            "Action": [
                "sqlworkbench:GetNotebook",
                "sqlworkbench:BatchGetNotebookCell",
                "sqlworkbench:AssociateNotebookWithTab"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/sqlworkbench-team": "${aws:PrincipalTag/sqlworkbench-
team}"
                }
            }
        }
    ]
}
```

有关 Amazon Redshift 托管式策略的更多信息，请参阅Amazon适用于 Amazon Redshift 的 托管（预定义）策略 (p. 364)。

您可以使用 IAM 控制台将 IAM policy 附到 IAM 用户或 IAM 角色上。您将策略附加到角色后，您可以将该角色附到 IAM 用户上。

将策略附到 IAM 用户上

1. 登录Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 选择 Users（用户）。
3. 选择需要访问查询编辑器 v2 的用户。
4. 选择 Add permissions（添加权限）。
5. 选择 Attach existing policies directly（直接附上现有策略）。
6. 如前所述，选择适当的策略作为 Policy names（策略名称）。

7. 选择 Next: Review（下一步：审核）。
8. 选择 Add permissions (添加权限)。

将 IAM policy 附到 IAM 角色上

1. 登录Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 选择 Roles（角色）。
3. 选择需要访问查询编辑器 v2 的角色。
4. 选择 Attach policies（附上策略）。
5. 如前所述，选择适当的策略作为 Policy names（策略名称）。
6. 选择 Attach policy（附上策略）。

有关使用 IAM 管理用户和角色的更多信息，请参阅《IAM 用户指南》中的更改 IAM 用户的权限。

设置主体标签以作为联合用户连接到查询编辑器 v2

要以联合用户身份访问查询编辑器 v2，请使用主体标签设置 IAM 角色或 IAM 用户。或者，设置身份提供者 (IdP) 以传入 `RedshiftDbUser` 和（可选）`RedshiftDbGroups`。有关使用 IAM 管理标签的更多信息，请参阅《IAM 用户指南》中的在 Amazon Security Token Service 中传递会话标签。要使用 Amazon Identity and Access Management 设置访问权限，管理员可以使用 IAM 控制台 (https://console.aws.amazon.com/iam/) 添加标签。

将主体标签添加到 IAM 角色中

1. 登录Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中选择 Roles。
3. 使用联合用户选择需要访问查询编辑器 v2 的角色。
4. 选择标签选项卡。
5. 选择 Manage tags（管理标签）。
6. 选择 Add tag（添加标签），然后在 Key（键）中输入 `RedshiftDbUser`，并输入联合用户名的 Value（值）。
7. （可选）选择 Add tag（添加标签），然后在 Key（键）中输入 `RedshiftDbGroups`，并且输入要与用户关联的组名称的 Value（值）。
8. 选择 Save changes（保存更改）以查看与您选择的 IAM 角色关联的标签列表。传播更改可能需要几秒时间。
9. 要使用联合用户，请在传播更改后刷新查询编辑器 v2 页面。

同样，您可以向 IAM 用户添加主体标签。

设置身份提供者 (IdP) 以传递主体标签

使用身份提供者 (IdP) 设置标签的过程因 IdP 而异。有关如何将用户和组信息传递给 SAML 属性的说明，请参阅 IdP 文档。正确进行配置后，以下属性将显示在 SAML 响应中，Amazon Security Token Service 使用此响应填充 `RedshiftDbUser` 和 `RedshiftDbGroups` 的主体标签。

```
<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>
```

可选的 *db_groups* 必须是以冒号分隔的列表，例如 `group1:group2:group3`。

此外，您还可以设置 `TransitiveTagKeys` 属性以在角色链接过程中保留标签。

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
  <AttributeValue>RedshiftDbUser</AttributeValue>
  <AttributeValue>RedshiftDbGroups</AttributeValue>
</Attribute>
```

有关设置查询编辑器 v2 的更多信息，请参阅使用查询编辑器 v2 所需的权限 (p. 369)。

使用查询编辑器 v2

查询编辑器 v2 主要用于编辑和运行查询、可视化结果以及与团队共享您的工作。使用查询编辑器 v2，您可以创建数据库、架构、表和用户定义的函数（UDF）。在树视图面板中，对于每个数据库，您都可以查看其架构。对于每个架构，您都可以查看其表、视图、UDF 和存储过程。

主题

- 打开查询编辑器 v2 (p. 106)
- 连接到 Amazon Redshift 数据库 (p. 108)
- 浏览 Amazon Redshift 数据库 (p. 108)
- 创建数据库对象 (p. 111)
- 加载示例数据 (p. 112)
- 从 Simple Storage Service（Amazon S3）加载数据 (p. 113)
- 更改账户设置 (p. 114)
- 使用 SQL 笔记本（预览版）。 (p. 114)

打开查询编辑器 v2

如要打开查询编辑器 v2

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航器菜单中，选择 Editor（编辑器），然后选择 Query editor V2（查询编辑器 V2）。此时将在新的浏览器标签页中打开查询编辑器 v2。

查询编辑器页面有一个导航器菜单，您可以在其中选择视图，如下所示：

数据库

您可以管理和查询以表形式组织并包含在数据库中的数据。数据库可以包含存储的数据，也可以包含对存储在其他位置（如 Amazon S3）的数据的引用。连接到包含在集群或无服务器工作组中的数据库。

在 Database（数据库）视图中工作时，您有以下控件：

- Cluster（集群）或 Workgroup（工作组）字段显示您当前连接到的集群或工作组的名称。Database（数据库）字段显示集群或工作组内的数据库。您在 Database（数据库）视图原定设置中执行的操作会对您选择的数据库执行操作。
- 集群或工作组、数据库和架构的树视图层次结构视图。在架构下，您可以使用表、视图、函数和存储过程。树视图中的每个对象都支持上下文菜单来执行相关操作，例如对对象进行 Refresh（刷新）或 Drop（删除）。
- 通过 + Create（创建）操作来创建数据库、架构、表和函数。
- 通过 Load data（加载数据）操作将数据从 Simple Storage Service（Amazon S3）加载到数据库。
- 通过 Save（保存）图标来保存您的查询。
- 通过 Shortcuts（快捷方式）图标来显示编辑器的键盘快捷键。
- 可以在 + Editor（编辑器）区域中输入和运行查询。

  运行查询后，Result（结果）选项卡随即显示结果。您可以打开此处的 Chart（图表）来可视化您的结果。还可以 Export（导出）结果。
- + Notebook（笔记本）区域，您可以在其中添加各部分，以输入和运行 SQL 或添加 Markdown。

  运行查询后，Result（结果）选项卡随即显示结果。您可以在此处 Export（导出）结果。

查询

查询包含用于管理和查询数据库中数据的 SQL 命令。当您使用查询编辑器 v2 加载示例数据时，它还会为您创建和保存示例查询。您可以与您的团队共享保存的查询。

笔记本

SQL 笔记本包含 SQL 和 Markdown 单元格。使用笔记本可在单个文档中组织、注释及共享多个 SQL 命令。您可以与团队共享笔记本。有关更多信息，请参阅使用 SQL 笔记本（预览版）。 (p. 114)。

图表

图表是您的数据的可视化表示。查询编辑器 v2 提供了用于创建多种图表并保存它们的工具。您可以与团队共享图表。有关更多信息，请参阅可视化查询结果 (p. 123)。

所有查询编辑器 v2 视图都有以下图标：

- Visual mode（可视化模式）图标，可在亮模式和暗模式之间切换。
- Settings（设置）图标，可显示不同设置屏幕的菜单。
- Editor preferences（编辑器首选项）图标，可在使用查询编辑器 v2 时编辑首选项。

- Connections（连接）图标，可查看编辑器选项卡使用的连接。

  连接用于检索数据库中的数据。连接是针对特定数据库创建的。使用隔离连接时，在一个编辑器选项卡中更改数据库的 SQL 命令（例如创建临时表）的结果在另一个编辑器选项卡中不可见。在查询编辑器 v2 中打开编辑器选项卡时，原定设置为隔离连接。创建共享连接时，即关闭 Isolated session（隔离会话）开关，同一数据库的其他共享连接的结果对彼此可见。但是，使用数据库的共享连接的各编辑器选项卡不会并行运行。使用相同连接的查询必须等到连接可用。与一个数据库的连接不能与另一个数据库共享，因此 SQL 结果在不同的数据库连接之间不可见。

  账户中的任何用户可以激活的连接数由查询编辑器 v2 管理员控制。

- Account settings（账户设置）图标，管理员用于更改账户中所有用户的某些设置。有关更多信息，请参阅更改账户设置 (p. 114)。

连接到 Amazon Redshift 数据库

要连接到数据库，请在树视图面板中选择集群或工作组名称。如果出现提示，请输入连接参数。

当您连接到集群或工作组及其数据库时，需要提供 Database（数据库）名称。您还提供以下身份验证方法之一所需的参数：

联合身份用户

使用此方法，您的 IAM 角色或 IAM 用户的主体标签必须提供连接详细信息。您可以在 Amazon Identity and Access Management 或您的身份提供者 (IdP) 中配置这些标签。查询编辑器 v2 依赖以下标签。

- `RedshiftDbUser` – 此标签定义查询编辑器 v2 使用的数据库用户。此标签为必填项。
- `RedshiftDbGroups` – 此标签定义当连接到查询编辑器 v2 时加入的数据库组。此标签是可选的，其值必须是以冒号分隔的列表，例如 `group1:group2:group3`。空值将被忽略，也就是说，`group1::::group2` 被解释为 `group1:group2`。

这些标签将转发到 `redshift:GetClusterCredentials` API 以获取集群的凭证。有关更多信息，请参阅设置主体标签以作为联合用户连接到查询编辑器 v2 (p. 105)。

数据库用户名和密码

使用这种方法，还需要为要连接的数据库提供 User name（用户名）和 Password（密码）。查询编辑器 v2 代表您创建秘钥并存储在 Amazon Secrets Manager 中。此密钥包含用于连接到数据库的凭证。

临时凭证

使用此方法，查询编辑器 v2 会为数据库提供 User name（用户名），并生成用于连接到数据库的临时密码。

当您选择具有查询编辑器 v2 的集群或工作组时，根据上下文，您可以使用上下文（右键单击）菜单创建、编辑和删除连接。

浏览 Amazon Redshift 数据库

在数据库中，您可以在树视图面板中管理架构、表、视图、函数和存储过程。在视图中的每个对象都在上下文（右键单击）菜单中都有与之关联的操作。

选择表后，您可以执行以下操作：

- 如要在编辑器中开启查询表中所有列的 SELECT 语句启动查询，请使用 Select table（选择表）。

- 要查看属性或表格，请使用 Show table definition（显示表定义）。使用此选项可查看列名、列类型、编码、分配键、排序键以及列是否可以包含空值。有关语法的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》https://docs.amazonaws.cn/redshift/latest/dg/r_CREATE_TABLE_NEW.html中的 CREATE TABLE。
- 要删除表，请使用 Delete（删除）。您可以使用 Truncate table（截断表）从表中删除所有行。或使用 Drop table（删除表）从数据库中删除表。更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 TRUNCATE 和 DROP TABLE。

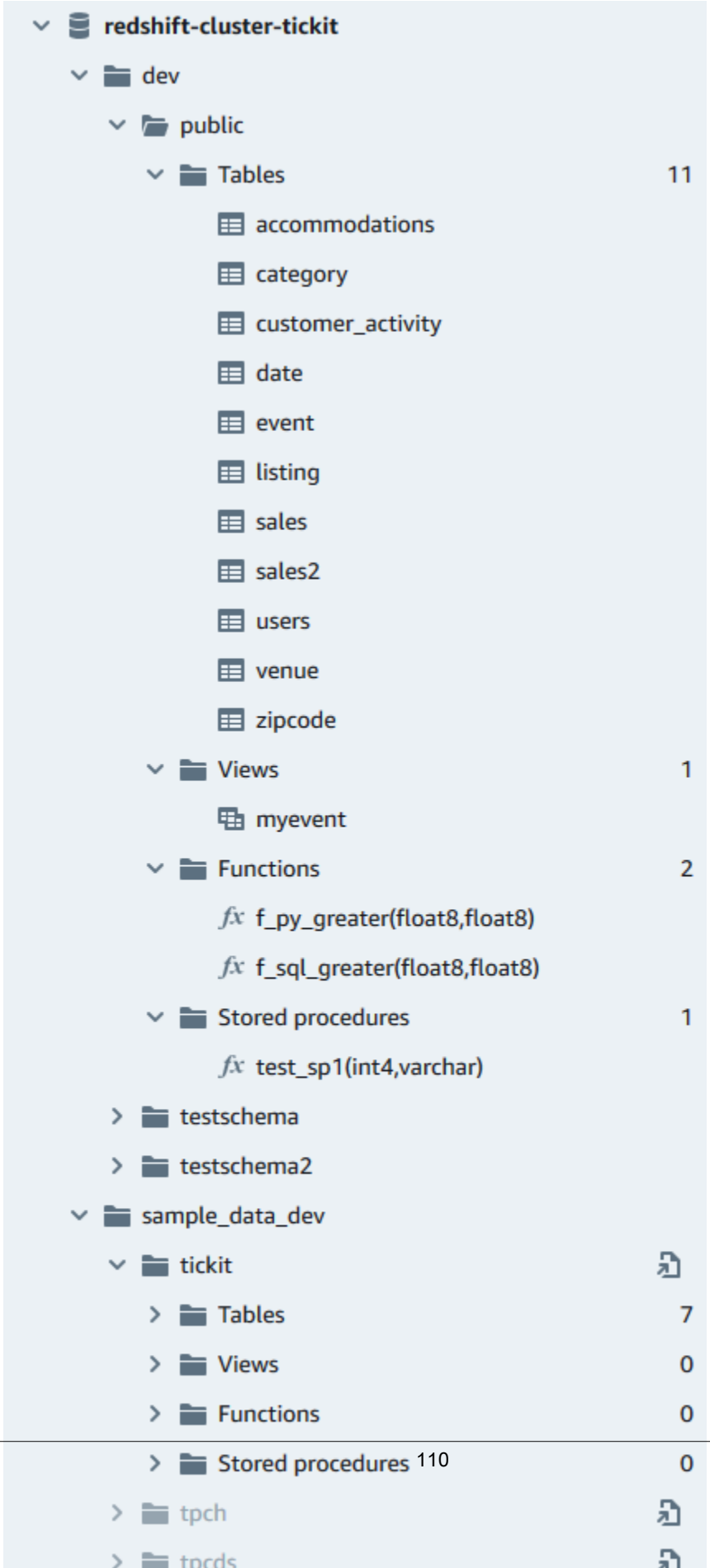
选择架构以 Refresh（刷新）或 Drop schema（删除架构）。

选择视图以 Show view definition（显示视图定义）或 Drop view（删除视图）。

选择函数以 Show function definition（显示函数定义）或 Drop function（删除函数）。

选择存储过程以 Show procedure definition（显示过程定义）或 Drop procedure（删除过程）。

层次结构树状图面板类似于以下内容。打开图标的上下文（右键单击）菜单，以查看您可以执行哪些操作。


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
tpch
tpcds

创建数据库对象

您可以创建数据库对象，包括数据库、架构、表和用户定义的函数（UDF）。您必须连接到集群或工作组以及数据库才能创建数据库对象。

创建数据库

有关数据库的信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 CREATE DATABASE。

1. 选择 Create（创建），然后选择 Database（数据库）。
2. 输入 Database name（数据库名称）。
3. （可选）选择 Users and groups（用户和组），然后选择 Database user（数据库用户）。
4. 选择 Create database（创建数据库）。

   新数据库将在树状视图面板中显示。

创建架构

有关架构的信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 Schemas。

1. 选择 Create（创建），然后选择 Schema（架构）。
2. 输入 Schema name（架构名称）。
3. 选择 Local（本地）或 External（外部）作为 Schema type（架构类型）。

   有关本地架构的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 CREATE SCHEMA。有关外部架构的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 CREATE EXTERNAL SCHEMA。
4. 如果选择 External（外部），则可以选择以下外部架构。

   - Glue Data Catalog（Glue 数据目录）– 在 Amazon Redshift 中创建引用 Amazon Glue 中的表的外部架构。除了选择 Amazon Glue 数据库，还可选择与集群关联的 IAM 角色以及与数据目录关联的 IAM 角色。
   - PostgreSQL – 在 Amazon Redshift 中创建外部架构，此架构引用 Amazon RDS for PostgreSQL 或 Amazon Aurora PostgreSQL 兼容版本的数据库。还提供数据库的连接信息。有关联合查询的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的通过联合查询来查询数据。
   - MySQL – 在 Amazon Redshift 中创建外部架构，该架构引用 Amazon RDS for MySQL 和/或 Amazon Aurora MySQL 兼容版本的数据库。还提供数据库的连接信息。有关联合查询的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的通过联合查询来查询数据。
5. 选择 Create schema（创建架构）。

   新 Schema 将在树状视图面板中显示。

创建表

您可以根据您指定或定义表中每列的逗号分隔值（CSV）文件创建表。有关表的信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 Designing tables 和 CREATE TABLE。

选择 Open query in editor（在编辑器中打开查询）在运行查询以创建表之前查看和编辑 CREATE TABLE 语句。

1. 选择 + Create（创建），然后选择 Table（表）。
2. 选择架构。
3. 输入表名称。

4. 选择 + Add field（添加字段）以添加列。
5. 使用 CSV 文件作为表定义模板：

   a. 选择 Load from CSV（从 CSV 加载）。
   b. 浏览到文件位置。

      如果您使用 CSV 文件，请确保该文件的第一行包含列标题。
   c. 选择文件，然后选择 Open（打开）。确认列名和数据类型符合您的要求。
6. 对于每一列，选择该列并选择所需的选项：

   - 为 Encoding（编码）选择一个值。
   - 选择 Default value（原定设置值）。
   - 如果您想增加列值，启用 Automatically increment（自动增量）。然后为 Auto increment seed（自动增加种子）和 Auto increment step（自动增量步骤）指定值。
   - 如果该列应始终包含值，启用 Not NULL（非 NULL）。
   - 输入列的 Size（大小）值。
   - 如您希望该列成为主密钥，启用 Primary key（主密钥）。
   - 如您希望该列成为唯一密钥，启用 Unique key（唯一密钥）。
7. （可选）选择 Table details（表详细信息）然后选择以下任何选项：

   - 分配密钥列和样式。
   - 对密钥列进行排序和排序类型。
   - 启用 Backup（备份）将表包含在快照中。
   - 启用 Temporary table（临时表）将表创建为临时表。
8. 选择 Open query in editor（在编辑器中打开查询）继续指定用于定义表的选项，或选择 Create table（创建表）来创建表。

创建函数

1. 选择 + Create（创建），然后选择 Function（函数）。
2. 对于 Type（类型），选择 SQL 或 Python。
3. 为 Schema（架构）选择一个值。
4. 为函数 Name（名称）输入一个值。
5. 为函数 Volatility（波动性）输入一个值。
6. 按输入参数的顺序排列的数据类型选择 Parameters（参数）。
7. 为 Returns（返回值）选择一种数据类型。
8. 输入函数的 SQL program（SQL 计划）代码。
9. 选择 Create (创建) 。

有关用户定义的函数（UDF）的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的创建用户定义的函数。

加载示例数据

查询编辑器 v2 附带可加载到示例数据库和相应架构中的示例数据和查询。

要加载示例数据，请选择与要加载的示例数据相关联的 图标。然后，查询编辑器 v2 将数据加载到数据库 `sample_data_dev` 的架构中，并在您的 Queries（查询）文件夹中创建一个存放所保存查询的文件夹。

提供了以下示例数据集。

tickit

Amazon Redshift 文档中的大多数示例使用称为 `tickit` 的示例数据。此数据包含七个表：两个事实表和五个维度。当您加载这些数据时，将使用示例数据更新架构 `tickit`。有关 `tickit` 数据的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的示例数据库。

tpch

此数据用于决策支持基准。当您加载这些数据时，将使用示例数据更新架构 `tpch`。有关 `tpch` 数据类型的更多信息，请参阅 TPC-H。

tpcds

此数据用于决策支持基准。当您加载这些数据时，将使用示例数据更新架构 `tpcds`。有关 `tpcds` 数据的更多信息，请参阅 TPC-DS。

从 Simple Storage Service（Amazon S3）加载数据

将数据从 Simple Storage Service（Amazon S3）加载到现有表中。

将数据加载到现有表中

查询编辑器 v2 使用 COPY 命令从 Simple Storage Service（Amazon S3）加载数据。在查询编辑器 v2 加载数据向导中生成和使用的 COPY 命令支持从 Amazon S3 复制的 COPY 命令语法可用的所有参数。有关 COPY 命令及其用于从 Simple Storage Service（Amazon S3）加载数据选项的信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 Amazon Simple Storage Service 中的 COPY 命令。

1. 确认表已在要加载数据的数据库中创建。查询编辑器 v2 只能将数据加载到现有表中。
2. 选择 Load data（加载数据）
3. 在 S3 URI中，选择 Browse S3（浏览 S3）以查找包含要加载数据的 Simple Storage Service（Amazon S3）桶。
4. 如果指定的 Amazon S3 桶与目标表不在同一个 Amazon Web Services 区域 中，则选择数据所在的 Amazon Web Services 区域 的 S3 file location（S3 文件位置）。
5. 如果 Simple Storage Service（Amazon S3）文件实际上包含多个 Simple Storage Service（Amazon S3）桶 URI 清单，选择This file is a manifest file（此文件是清单文件）。
6. 选择具有从 Simple Storage Service（Amazon S3）加载数据所需的权限的 IAM role（IAM 角色）。
7. 为要上载的文件选择 File format（文件格式）。支持的数据格式有 CSV、JSON、DELIMITER、FIXEDWIDH、SHAPEFILE、AVRO、PARQUET 和 ORC。根据指定的文件格式，您可以选择相应的 File options（文件选项）。如果数据已加密，您还可以选择 Data is encrypted（数据已加密），并输入用于加密数据的 KMS 密钥 Amazon Resource Name（ARN）。

   对于 PLATION 和 ORC，没有任何文件选项可以配置。
8. 选择压缩方法来压缩文件。原定设置为无压缩。
9. （可选）Advanced settings（高级设置）支持各种 Data conversion parameters（数据转换参数）和 Load operations（加载操作）。根据文件的需要输入此信息。

   有关数据转换和数据加载参数的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的数据转换参数和数据加载操作。
10. 确认或选择 Target table（目标表）的位置，包括加载数据的数据库、架构和表名称。
11. 选择 Load data（加载数据）开启数据加载。

    加载完成后，查询编辑器将显示用于加载数据的生成 COPY 命令。将显示 COPY 的 Result（结果）。如果成功，您现在可以使用 SQL 从加载的表中选择数据。当出现错误时，请查询系统视图

STL_LOAD_ERRORS 以获取更多详细信息。有关 COPY 命令错误的信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 STL_LOAD_ERRORS。

更改账户设置

拥有正确 IAM 权限的用户可以查看和更改同一 Amazon Web Services 账户中其他用户的 Account settings（账户设置）。该管理员可以查看或设置以下内容：

- 账户中每个用户的最大并发数据库连接数。这包括用于 Isolated sessions（隔离会话）的连接。更改此值时，更改可能需要 10 分钟才能生效。
- 允许账户中的用户将整个结果集从 SQL 命令导出到文件中。
- 加载和显示示例数据库以及一些关联的已保存查询。
- 查看用于加密查询编辑器 v2 资源的 KMS 密钥 ARN。

使用 SQL 笔记本（预览版）。

以下是针对预览版查询编辑器 v2 笔记本的预发行文档。文档和功能都可能会更改。我们建议您仅在测试环境中使用此功能，不要在生产环境中使用。有关预览条款和条件，请参阅 Amazon 服务条款中的测试版服务参与。

您可以使用 SQL 笔记本在单个文档中组织、注释及共享多个 SQL 查询。您可以将多个 SQL 查询和 Markdown 单元格添加到 SQL 笔记本中。SQL 笔记本提供了一种方法：通过使用多个查询和 Markdown 单元格，将与数据分析相关的查询和解释分组到单个文档中。您可以使用 Markdown 语法添加文本并设置外观格式，以便为数据分析任务提供上下文和其它信息。您可以与团队成员共享您的 SQL 笔记本。

如要使用 SQL notebook 功能，您必须向已具有一个查询编辑器 v2 托管式策略的主体（IAM 用户或 IAM 角色）添加 SQL 笔记本（预览版）功能的策略。有关更多信息，请参阅访问查询编辑器 v2 (p. 103)。

要了解笔记本的演示，请观看以下视频。SQL Notebooks 简介。

创建 SQL 笔记本

1. 选择 + 然后选择 Notebook（笔记本）。

   原定设置情况下，新的 SQL 笔记本中会出现一个 SQL 查询单元格。
2. （可选）选择 Rename（重命名）然后输入 SQL 笔记本的名称。
3. 在 SQL 查询单元格中，执行以下任一操作：

   - 输入查询。
   - 粘贴您复制的查询。
4. （可选）选择 Add markdown（添加标记）添加 Markdown 单元格，在其中可以使用标准 Markdown 语法提供描述性或解释性文本。
5. （可选）选择 Add SQL（添加 SQL）及 Add markdown（添加标记）以插入额外的 SQL 和 Markdown 文本单元格。

打开笔记本

1. 在导航器菜单中，选择 Notebooks（笔记本）。
2. 选择要打开的 SQL 笔记本并双击。

与团队共享 SQL 笔记本

- 选择 Share toteam-name（共享到团队名称）。

编写和运行查询

您可以在编辑器中输入查询，也可以从 Queries（查询）中列出并选择 Run（运行）以选择已保存的查询。

默认情况下，设置 Limit 100（限制 100），将结果限制为 100 行。您可以禁用此选项来返回较大的结果集。禁用此选项时，如要避免非常大型结果集，则可以在 SQL 语句中包含 LIMIT 选项。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 ORDER BY 子句。

要在结果区域中显示查询计划，请打开 Explase（解释）。对结果开启 Explain graph（解释图），也可显示解释计划的图形表示。

选择 Save（保存），将查询保存到 Queries（查询）文件夹。

查询成功，将显示成功消息。如果查询返回信息，则结果将显示在 Results（结果）部分。如果结果数超过显示区域，则数字将显示在结果区域的顶部。您可以选择数字来显示连续的结果页面。

您可以筛选和排序每一列的 Result（结果）。如要在结果列标题中输入筛选条件，请将鼠标悬停在该列上以查看惨淡（ ），您可以在其中输入筛选列的条件。

如果查询包含错误，则查询编辑器 v2 将在结果区域中显示错误消息。此消息提供有关如何更正查询的信息。

您可以使用结果区域中的上下文（右键单击）菜单导出或复制查询结果，如下所示：

- 选择 Export result set（导出结果集）和 JSON 或 CSV，以将整组行结果下载到文件中。结果集中的行数可能受到查询中 Limit（限制）选项或 SQL `limit` 子句限制。下载结果集的最大大小为 5 MB。
- 如果没有选择行，则选择 Export current page（导出当前页面）和 JSON 或 CSV，以将当前页面中的行下载到文件中。
- 如果选择了行，则选择 Export selected rows（导出选定的行）和 JSON 或 CSV，以将选定的行下载到文件中。
- 如果选择了行，则选择 Copy rows（复制行）将选定行复制到剪贴板。
- 如果选择了行，则选择 Copy rows with headers（复制带标题的行），以将带有列标题的选定行复制到剪贴板。

也可以使用快捷方式（Windows 上的 Ctrl+C 或 MacOS 上的 Cmd+C）将数据从当前结果页面复制到剪贴板。如果未选择任何行，则具有焦点的单元格将复制到剪贴板。如果选择了行，则选定的行将复制到剪贴板。

要添加新的查询选项卡，请选择 图标，然后选择 Editor（编辑器），此编辑器将显示在查询选项卡所在行中。查询选项卡可以使用，也可以不使用 `Isolated session`。对于隔离会话，SQL 命令的结果（例如，在一个编辑器选项卡中创建临时表）在另一个编辑器选项卡中不可见。在查询编辑器 v2 中打开编辑器选项卡时，原定设置为隔离会话。

运行查询

1. 在查询区域中，执行以下任一操作：
   - 输入查询。
   - 粘贴您复制的查询。

- 选择 Queries（查询）文件夹中，打开上下文菜单（右键单击）中的保存查询，然后选择 Open query（打开查询）。

2. 确认您为计划运行的 SQL 选择了正确的 Cluster（集群）或 Workgroup（工作组）以及 Database（数据库）值。

   最初，您可以在树视图中选择您的 Cluster（集群）或 Workgroup（工作组）。还可以在树视图中选择您的 Database（数据库）。

   您可以使用位于每个编辑器选项卡的 Isolated session（隔离会话）标题附近的下拉控件，来更改每个编辑器选项卡中的 Cluster（集群）或 Workgroup（工作组）以及 Database（数据库）。

   对于每个编辑器选项卡，您可以选择是否以 Isolated session（隔离会话）运行 SQL。隔离会话与数据库有自己的连接。使用它来运行与其他查询编辑器会话隔离的 SQL。有关连接的更多信息，请参阅打开查询编辑器 v2 (p. 106)。

3. 选择 Run（运行）。

   将打开 Result（结果）区域并显示查询结果。

显示查询的解释计划

1. 选择查询。
2. 启用 Explase（解释）。

   默认情况下，Explain graph（解释图）也将启动。

3. 选择 Run（运行）。

   运行查询，并在查询的 Result（结果）区域中显示解释计划。

查询编辑器 v2 支持以下功能。

- 您可以在一个查询选项卡中使用多个 SQL 语句创作查询。这些查询以连续方式运行，并为每个查询打开多个结果选项卡。
- 您可以使用会话变量和临时表创作查询。
- 您可以使用由 `${parameter}` 指定的可替换参数创作查询。您可以使用多个可替换参数创作 SQL 查询，并在 SQL 语句的多个位置使用相同的参数。

  当查询运行时，会显示一个用来输入参数值的窗口。每次运行查询时，都会显示窗口以输入参数值。

  有关示例，请参阅示例：销售额大于特定参数 (p. 117)。
- 自动对查询进行版本控制。您可以选择要运行的查询的早期版本。
- 在继续工作流程之前，您无需等待查询完成。即使关闭查询编辑器，查询仍会继续运行。
- 创作查询时，支持使用快捷方式自动完成架构、表和列名称。

  选择 Shortcuts（快捷方式）图标来查找 Auto complete（自动完成）快捷方式。

以下示例演示了其中的一些功能。

查询示例

在下方您可以找到可以运行的各种查询类型的描述。

许多此类查询中使用的数据来自 `tickit` 示例架构。有关 `tickit` 数据的更多信息，请参阅加载示例数据 (p. 112)。

运行这些示例查询时，请确认在编辑器中选择了正确的数据库，例如 sample_data_dev。

主题

- 示例：设置会话变量 (p. 117)
- 示例：按总销售额排列的顶事件 (p. 117)
- 示例：销售额大于特定参数 (p. 117)
- 示例：创建一个临时表 (p. 118)
- 示例：从临时表中选择 (p. 118)

示例：设置会话变量

以下命令将 search_path 服务器配置参数设置为会话的 public（公有）参数。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 SET 和 search_path。

```
set search_path to public;
```

示例：按总销售额排列的顶事件

以下查询查找销售额最多的事件。

```
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname
order by 3;
```

以下是结果的部分清单。

```
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
...
```

示例：销售额大于特定参数

以下查询查找销售数量大于 ${numberoforders} 指定参数的销售额。当参数值为 7 时，结果是 60 行。运行查询时，查询编辑器 v2 会显示 Run query form（运行查询表）窗口来收集 SQL 语句中参数值。

```
select salesid, qtysold
from sales
where qtysold > ${numberoforders}
order by 2;
```

以下是结果的部分清单。

```
salesid qtysold
20005 8
21279 8
130232 8
42737 8
```

```
74681 8
67103 8
105533 8
91620 8
121552 8
...
```

示例：创建一个临时表

通过 sales（销售）和 event（事件）表，以下语句创建临时表 eventsalestemp。

```
create temporary table eventsalestemp as
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname;
```

示例：从临时表中选择

按总订单排序，以下语句从临时表 eventsalestemp 中选择事件、订单总数和总销售额。

```
select eventname,  totalorders,  totalsales
from eventsalestemp
order by 2;
```

以下是部分结果列表。

```
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
...
```

查询注意事项

请考虑下列有关使用查询编辑器时处理查询的事项：

- 最大查询结果大小为 5MB 或 100,000 行中的较小者。
- 您可以运行最长为 300,000 个字符的查询。
- 您可以保存最长为 30,000 个字符的查询。
- 不能在查询编辑器中使用事务。有关事务的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 BEGIN。

查询数据湖

您可以在 Simple Storage Service（Amazon S3）数据湖中查询数据。首先，您可以创建一个外部架构来引用在 Amazon Glue Data Catalog 中的外部数据库。然后，您可以在 Simple Storage Service（Amazon S3）数据湖中查询数据。

演示：查询数据湖

要了解如何查询数据湖的演示，请观看以下视频。使用 Amazon Redshift 查询编辑器 v2 查询数据湖。

先决条件

创建 IAM 角色

您创建 IAM 角色以访问为 Amazon Lake Formation 启用的 Amazon Glue Data Catalog。

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Policies (策略)。

   如果这是您首次选择 Policies，则会显示 Welcome to Managed Policies 页面。选择开始使用。
3. 选择 Create policy (创建策略)。
4. 选择以在 JSON 选项卡上创建策略。
5. 粘贴在以下 JSON 策略文档中，该策略授予对 Data Catalog 的访问权限，但拒绝对 Lake Formation 的管理员权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RedshiftPolicyForLF",
            "Effect": "Allow",
            "Action": [
                "glue:*",
                "lakeformation:GetDataAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

6. 完成后，选择审核对策略进行审核。策略验证程序将报告任何语法错误。
7. 在 Review policy（查看策略）页面上，输入您正在创建的策略的 Name（名称）（例如，mydatalake_policy）。输入描述（可选）。查看策略摘要以查看您的策略授予的权限。然后，选择创建策略以保存您的工作。

   创建策略之后，您可以创建一个角色并应用该策略。
8. 在 IAM 控制台的导航窗格中，选择 Roles，然后选择 Create role。
9. 对于选择受信任实体的类型，选择 Amazon 服务。
10. 选择 Amazon Redshift 服务来代入此角色。
11. 为您的服务选择 Redshift Customizable (Redshift 可自定义)。然后选择 Next: Permissions (下一步：权限)。
12. 选择您创建的 `mydatalake_policy` 权限策略以附加到该角色。
13. 选择 Next: Tagging (下一步: 标记)。
14. 选择 Next: Review (下一步：审核)。
15. 对于 Role name（角色名称），请输入角色的名称（例如，mydatalake_role）。
16. （可选）对于 Role description (角色描述)，输入新角色的描述。
17. 检查该角色，然后选择创建角色。

授予权限

您授予对表的 SELECT 权限以在 Lake Formation 数据库中进行查询。

1. 通过 https://console.aws.amazon.com/lakeformation/ 中打开 Lake Formation 控制台。
2. 在导航窗格中，选择权限，然后选择 Grant (授予)。
3. 提供以下信息：
   - 对于 IAM 角色，选择您创建的 IAM 角色 `myspectrum_role`。运行 Amazon Redshift 查询编辑器时，它使用此 IAM 角色来获取数据权限。

     Note

     要授予对启用了 Lake Formation 的 Data Catalog 中的表的 SELECT 权限以进行查询，请执行以下操作：
     - 在 Lake Formation 中注册数据的路径。
     - 在 Lake Formation 中授予用户对该路径的权限。
     - 创建的表可在 Lake Formation 中注册的路径中找到。
   - 对于数据库，请选择您的 Lake Formation 数据库。
   - 对于表，选择数据库中要查询的表。
   - 对于列，选择 All Columns (所有列)。
   - 选择 Select (选择) 权限。
4. 选择保存。

   Important

   作为最佳实践，仅允许通过 Lake Formation 权限访问底层 Simple Storage Service（Amazon S3）对象。要防止未经批准的访问，请删除授予针对 Lake Formation 以外的 Simple Storage Service（Amazon S3）对象的任何权限。如果您在设置 Lake Formation 之前曾访问了 Simple Storage Service（Amazon S3）对象，请删除之前设置的任何 IAM policy 或桶权限。有关更多信息，请参阅将 Amazon Glue 数据权限升级到 Amazon Lake Formation 模型和 Lake Formation 权限。

创建外部架构

要查询 Simple Storage Service（Amazon S3）数据湖中的数据，请创建外部架构。外部架构引用了 Amazon Glue Data Catalog 中的外部数据库。

1. 选择 Create（创建），然后选择 Schema（架构）。
2. 输入 Schema name（架构名称）。
3. 要将数据库的所有权授予用户，请选择 Authorize user（授权用户）然后选择用户。
4. 选择 External（外部）。
5. 在 Amazon Glue Data Catalog（Amazon Glue 数据目录）详细信息下，区域原定设置为 Redshift 数据库所在的区域。
6. 选择外部架构将映射到的 Amazon Glue database（ 数据库）。
7. 选择具有从 Simple Storage Service（Amazon S3）查询数据所需的权限的 IAM role（IAM 角色）。
8. 选择 Create schema（创建架构）。

   架构将显示在数据库浏览器中。

在 Simple Storage Service（Amazon S3）数据湖中查询数据

您可以使用在前一个过程中创建的架构。

1. 在数据库浏览器中，选择架构。

2. 请选择一个表来查看表定义。

   此时系统将显示表列和数据类型。
3. 要查询表，请选择表并使用上下文菜单（右键单击）选择 Select table（选择表）。

使用数据共享

您可以创建数据共享，以便其他集群上的用户可以查询数据。包含您要共享的数据的集群称为创建者集群。您可以在创建者集群上为要共享的数据库对象创建数据共享。您可以共享 Schema、表、视图和 SQL 用户定义的函数（UDF）。您要与其共享数据的集群称为使用者集群。在使用者集群上，您可以利用数据共享创建数据库。然后，使用者集群上的用户可以查询数据。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的数据共享入门。

创建数据共享

您可以在要用作创建者集群的集群上创建数据共享。要详细了解数据共享的注意事项，请参阅中的《Amazon Redshift 数据库开发人员指南》中的 Amazon Redshift 中的数据共享注意事项。

1. 选择要使用的创建者集群上的数据库。
2. 创建数据共享。例如：

```
create datashare mysource;
```

3. 设置数据共享的权限。例如：

```
grant alter, share on datashare mysource to admin;
```

4. 设置要共享的数据库对象的权限。例如：

```
alter datashare mysource add schema public;
```

```
alter datashare mysource add table public.event;
```

5. 设置使用者集群命名空间的权限以访问数据共享。例如：

```
grant usage on datashare mysource to namespace '2b12345-1234-5678-9012-bb1234567890';
```

显示数据共享

您可以显示您在创建者集群上创建的数据共享。

1. 选择创建者集群。
2. 显示数据共享。例如：

```
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
```

创建使用者数据库

在使用者集群上，您可以利用数据共享创建数据库。这些步骤描述了如何在同一个账户中的两个集群之间共享数据。有关跨 Amazon 账户共享数据的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的跨 Amazon 账户共享数据。

您可以使用 SQL 命令或查询编辑器 v2 树状视图面板来创建数据库。

使用 SQL

1. 利用数据共享为您的账户和创建者集群的命名空间创建一个数据库。例如：

```
create database share_db from datashare mysource of account '123456789012' namespace
 'p1234567-8765-4321-p10987654321';
```

2. 设置权限，以便用户可以访问数据库和 Schema。例如：

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

使用查询编辑器 v2 树状视图面板

1. 选择 Create（创建），然后选择 Database（数据库）。
2. 输入 Database name（数据库名称）。
3. （可选）选择 Users and groups（用户和组），然后选择 Database user（数据库用户）。
4. 选择 Create using a datashare（使用数据共享创建）。
5. 选择数据共享。
6. 选择 Create database（创建数据库）。

   新的数据共享数据库将在查询编辑器 v2 树状视图面板中显示。
7. 设置权限，以便用户可以访问数据库和 Schema。例如：

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

查询数据共享对象

在使用者集群上，您可以使用以三段表示法表示的完全限定对象名来查询数据共享对象名：数据库名称、Schema 和对象的名称。

1. 在查询编辑器 v2 树状视图面板中，选择该 Schema。
2. 请选择一个表来查看表定义。

   此时系统将显示表列和数据类型。
3. 要查询表，请选择表并使用上下文菜单（右键单击）选择 Select table（选择表）。
4. 使用 SELECT 命令查询表。例如：

```
select top 10 * from test_db.public.event;
```

可视化查询结果

运行查询并显示结果后，可以打开 chart（图表）以显示结果的图形可视化。您可以使用以下控件来定义图表的内容、结构和外观：

跟踪

表示图表中的一组相关图形标记。可以在图表中定义多个跟踪。

类型

您可以将跟踪类型定义为以下类型之一来表示数据：

- 适用于散点的散点图或气泡图。
- 用垂直条或水平条表示数据类别的条形图。
- 用于定义填充区域的区域图。
- 使用条形表示频率分布的直方图。
- 使用圆形表示数据的饼图，其中每个切片代表所占整体的百分比。
- 用于表示流程不同阶段的数据的漏斗或漏斗区域图。
- OHLC（开盘、高、低、收盘）图通常用于财务数据，表示沿 x 轴的开盘、高、低和收盘值，这通常表示时间间隔。
- K 线图表示时间线上类别的一系列值。
- 瀑布图，表示初始值如何通过一系列中间值而增加或减少。值可以表示时间间隔或类别。
- 折线图表示值随着时间的推移而变化。

X 轴

您可以指定一个表列，其中包含要沿 X 轴绘制的值。包含描述性值的列通常表示维度数据。包含量化值的列通常表示实际数据。

Y 轴

您可以指定一个表列，其中包含要沿 Y 轴绘制的值。包含描述性值的列通常表示维度数据。包含量化值的列通常表示实际数据。

子图

您可以定义图表数据的其它表示形式。

转换

您可以定义转换以筛选跟踪数据。您可以使用拆分转换以显示来自单个源跟踪的多个跟踪。您可以使用聚合转换以将跟踪显示为平均值或最小值。您可以使用排序转换以对跟踪进行排序。

一般外观

您可以设置背景颜色、边距颜色、设计调色板的色阶、文本样式和大小、标题样式和大小以及模式栏的默认值。您可以定义拖动、单击和悬停的交互。您可以定义元文本。您可以定义跟踪、轴、图例和注释的默认外观。

选择 Traces（跟踪）将结果显示为图表。对于 Type（类型），可将图表样式选择为 Bar（条形图）、Line（折线图）等。对于 Orientation（方向），您可以选择 Vertical（垂直）或 Horizontal（水平）。对于 X，选择要用于水平轴的表列。对于 Y，选择要用于垂直轴的表列。

要更新显示，请选择 Refresh（更新）。选择 Full screen（全屏）以扩大图表显示范围。

创建图表

1. 运行查询并获取结果。
2. 启用 chart（图表）。
3. 选择 Trace（跟踪），然后开启可视化您的数据。
4. 从以下值中选择一种图表样式：
   - 散点图
   - 条形图
   - 区域图
   - 直方图
   - 饼图
   - 漏斗图
   - 漏斗区域图
   - OHLC（高开低关）
   - K 线图
   - 瀑布图
   - 折线图
5. 选择 Style（样式）以自定义外观，包括颜色、轴、图例和注释。您可以添加文本、形状和图像。
6. 选择 Annotations（注释）添加文本、形状和图像。

保存图表

1. 选择 Save Chart（保存图表）。
2. 输入图表名称。
3. 选择保存。

导出图表

1. 选择 Export（导出）。
2. 选择 PNG 或者 JPEG。
3. 设置图表的宽度和高度。
4. 选择 Export（导出）。
5. 选择在原定设置图形应用程序中打开文件，或者使用默认名称保存文件。

浏览并打开保存的图表

1. 选择 Charts（图表）选项卡。
2. 打开您想要的图表。

将图表整理到文件夹中

1. 从导航窗格中，选择 Charts（图表）。
2. 选择 New folder（新建文件夹）并命名文件夹。
3. 选择 Create（创建）以在 Charts 选项卡中创建文件夹。

您可以使用拖放方式将图表移入和移出文件夹。

示例：创建饼图以可视化查询结果

以下示例使用示例数据库中的 Sales（销售）表。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 Sample database（示例数据库）。

以下是为饼图提供数据而运行的查询。

```
select top 5 eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid group by eventname
order by 3;
```

按总销售额作为顶事件创建饼图

1. 运行查询。
2. 在查询结果区域中，打开 chart（图表）。
3. 选择 Trace（跟踪）。
4. 对于 Type（类型），选择 Pie（饼图）。
5. 对于Values（值），选择 totalsales（总销售额）。
6. 对于 Labels（标签），选择 eventname（事件名称）。
7. 选择 Style（样式），然后选择 General（普通）。
8. 在 Colorscales（颜色刻度）下，选择 Categorical（分类），然后选择 Pastel2。

示例：创建用于比较收入和销售额的组合图

执行此示例中的步骤创建一个图表，该图表将收入数据的条形图和销售额数据的折线图组合在一起。以下示例使用 tickit 示例数据库中的 Sales（销售额）表。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 Sample database（示例数据库）。

以下是为图表提供数据而运行的查询。

```
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;
```

创建用于比较收入和销售额的组合图

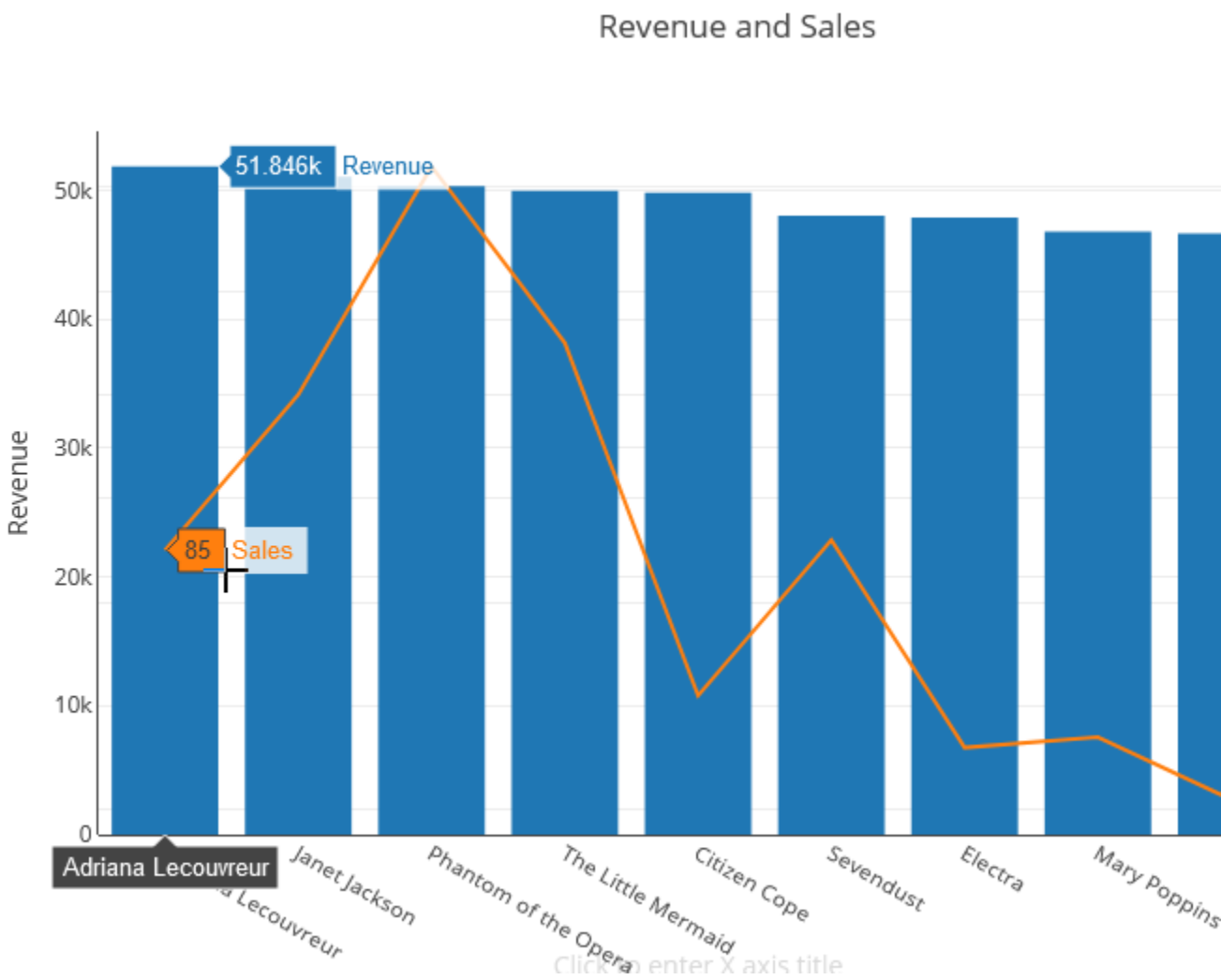
1. 运行查询。
2. 在查询结果区域中，打开 chart（图表）。
3. 在 trace o下，对于 Type（类型），选择 Bar（条形图）。
4. 对于 X，选择 eventname。
5. 对于 Y，选择 total_price。

   条形图将沿 X 轴显示事件名称。
6. 在 Style（样式）下，选择 Traces（跟踪）。
7. 对于 Name（名称），输入 Revenue（收入）。
8. 在 Style（样式）下，选择 Axes（轴）。
9. 对于 Titles（标题），选择 Y 然后输入 Revenue（收入）。

   Revenue（收入）标签将显示在左侧 Y 轴上。
10. 在 Structure（结构）下，选择 Traces（跟踪）。
11. 选择 + Trace（跟踪）。

    系统将显示跟踪 1 选项。
12. 对于 Type（类型），选择 Line（线形图）。
13. 对于 X，选择 eventname。
14. 对于 Y，选择 total_qty_sold。
15. 在 Axes To Use（要使用的轴）下，为 Y Axis（Y 轴）选择 +。

    Y Axis（Y 轴）将显示 Y2。
16. 在 Style（样式）下，选择 Axes（轴）。
17. 在 Titles（标题）下，选择 Y2。
18. 对于 Name（名称），输入 Sales（销售额）。
19. 在 Lines（线形图）下，选择 Y:Sales（Y：销售额）。
20. 在 Axis Line（轴线）下，选择 Show（显示），对于 Position（位置），选择 Right（右侧）。



演示：使用 Amazon Redshift 查询编辑器 v2 构建可视化

要了解如何构建可视化项的演示，请观看以下视频。使用 Amazon Redshift 查询编辑器 v2 构建可视化。

以团队形式协作和共享

您可以与您的团队共享查询。

团队是针对一组协作并共享查询编辑器 v2 资源的用户定义的。管理员可以通过向 IAM 角色添加标签来创建团队。有关更多信息，请参阅使用查询编辑器 v2 所需的权限 (p. 369)。

保存、浏览和删除查询

在与团队共享查询之前，请保存查询。您可以查看和删除已保存的查询。

保存查询

1. 准备查询然后选择 Save（保存）。
2. 输入查询的标题。
3. 选择保存。

浏览保存的查询

1. 从导航窗格中，选择 Queries（查询）。
2. 您可以查看以下查询：My queries（我的查询）、Shared by me（由我分享的查询），或者 Shared to my team（分享给我的团队的查询）。这些查询可以显示为单个查询或存在您创建的文件夹中。

编辑已保存的查询

1. 打开已保存查询的上下文（右键单击）菜单。
2. 选择 Delete（删除）然后确认操作。

将保存的查询整理到文件夹中

1. 从导航窗格中，选择 Queries（查询）。
2. 选择 New folder（新建文件夹）并命名文件夹。
3. 选择 Create（创建）以在 Queries（查询）选项卡中创建文件夹。

   现在，您可以使用拖放方式将查询移入和移出文件夹。

共享查询

您可以与您的团队共享您的查询。您还可以查看已保存查询的历史记录和管理查询版本。

如要与团队共享查询，请确保您将主要标签 `sqlworkbench-team` 设置为与账户中其它团队成员相同的值。例如，管理员可以为会计部门的每个人将该值设置为 `accounting-team`。有关示例，请参阅 使用查询编辑器 v2 所需的权限 (p. 369)。

与团队共享查询

1. 从导航窗格中，选择 Queries（查询）。
2. 打开要共享的查询的上下文（右键单击）菜单，然后选择 Share with my team（与我的团队分享）。
3. 选择要与之共享查询的一个或多个团队，然后选择 Save sharing options（保存共享选项）。

每次保存 SQL 查询时，查询编辑器 v2 都会将其保存为新版本。您可以浏览早期的查询版本、保存查询副本或恢复查询。

管理查询版本

1. 从导航窗格中，选择 Queries（查询）。
2. 打开要处理查询的上下文（右键单击）菜单。
3. 选择 Version history（版本历史记录）以打开查询的版本列表。
4. 在 Version history（版本历史记录）页面上，您可以执行以下操作：

   - Revert to selected（恢复为选定）– 恢复到选定的版本并继续使用此版本。
   - Save selected as（将选定选项另存为）– 在编辑器中创建新的查询。

使用查询编辑器查询数据库

使用查询编辑器是在由 Amazon Redshift 集群托管的数据库上运行查询的简单方法。创建集群后，可以使用 Amazon Redshift 控制台上的查询编辑器立即运行查询。

Note

您无法使用此原始查询编辑器在 Amazon Redshift Serverless 中查询数据。而应使用 Amazon Redshift 查询编辑器 v2。

2021 年 2 月，部署了更新的查询编辑器，并更改了使用查询编辑器的授权权限。新的查询编辑器使用 Amazon Redshift 数据 API 来运行查询。作为 Amazon 托管 Amazon Identity and Access Management (IAM) 策略的 `AmazonRedshiftQueryEditor` 策略已更新为包含必要的权限。如果您有自定义 IAM 策略，请务必更新它。将 `AmazonRedshiftQueryEditor` 用作指南。对 `AmazonRedshiftQueryEditor` 的更改包括以下内容：

- 管理查询编辑器语句结果的权限需要语句拥有者用户。
- 已添加使用 Secrets Manager 连接到数据库的权限。

有关更多信息，请参阅使用 Amazon Redshift 控制台查询编辑器所需的权限 (p. 369)。

从新的查询编辑器连接到集群时，您可以使用两种身份验证方法之一，如使用查询编辑器进行连接 (p. 130)所述。

使用查询编辑器可以执行以下操作：

- 运行单个 SQL 语句查询。
- 将大小为 100 MB 的结果集下载到一个逗号分隔值 (CSV) 文件。
- 保存查询以供重用。您无法在欧洲（巴黎）区域、亚太地区（大阪）区域、亚太地区（香港）区域或中东（巴林）区域中保存查询。
- 查看用户定义表的查询运行时详细信息。
- 安排查询在未来运行。
- 查看您在查询编辑器中创建的查询的历史记录。
- 使用增强型 VPC 路由对集群运行查询。

查询编辑器注意事项

请考虑下列有关使用查询编辑器时处理查询的事项：

- 查询的最长持续时间为 24 小时。
- 查询结果的最大大小为 100 MB。如果调用返回的响应数据超过 100 MB，则调用将终止。
- 查询结果的最长保留时间为 24 小时。
- 最大查询语句大小为 100 KB。
- 集群必须在基于 Amazon VPC 服务的 Virtual Private Cloud (VPC) 中。
- 不能在查询编辑器中使用事务处理。有关事务的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 BEGIN。
- 您可以保存最长为 3000 个字符的查询。

启用对查询编辑器的访问

要访问查询编辑器，您需要相应权限。要启用访问，请将用于 IAM 权限的 `AmazonRedshiftQueryEditor` 和 `AmazonRedshiftReadOnlyAccess` Amazon 托管策略附加到您要用于访问您的集群的 IAM 用户。您可以使用 IAM 控制台 (https://console.aws.amazon.com/iam/) 附加 IAM 策略。

如果您已创建 IAM 用户来访问 Amazon Redshift，则可以将 `AmazonRedshiftQueryEditor` 和 `AmazonRedshiftReadOnlyAccess` Amazon 托管策略附加到该用户。如果您尚未创建 IAM 用户，则可以创建一个，然后将策略附加到 IAM 用户。

Amazon 托管策略 AmazonRedshiftQueryEditor 允许操作 redshift:GetClusterCredentials，预设情况下该操作会为数据库用户提供对数据库的超级用户访问权限。要限制访问，您可以执行下列操作之一：

- 创建自定义策略，该策略允许调用 redshift:GetClusterCredentials 并将资源限制为 DbUser 的给定值。
- 为用户添加一个策略，以拒绝 redshift:GetClusterCredentials 权限，然后要求用户使用临时凭证登录查询编辑器。例如，拒绝策略可能与以下策略相似。

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

有关更多信息，请参阅创建有权调用 GetClusterCredentials 的 IAM 角色或用户 (p. 395)。

如果通过附加 Amazon 托管策略 AmazonRedshiftQueryEditor 为您授予了访问 Amazon Redshift 查询编辑器的权限，则您可以列出所有密钥。但是，您只能创建和检索使用密钥 RedshiftQueryOwner 和值 ${aws:userid} 标记的密钥。如果您从 Amazon Redshift 查询编辑器创建密钥，则会自动标记该密钥。要使用不是通过 Amazon Redshift 查询编辑器创建的密钥，请确认该密钥是否使用键 RedshiftQueryOwner 和您的唯一 IAM 用户标识符的值标记，例如 AIDACKCEVSQ6C2EXAMPLE。

附加查询编辑器所需的 IAM 策略

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 选择 Users（用户）。
3. 选择需要访问查询编辑器的用户。
4. 选择 Add permissions (添加权限)。
5. 选择直接附加现有策略。
6. 对于策略名称，选择 AmazonRedshiftQueryEditor 和 AmazonRedshiftReadOnlyAccess。
7. 选择 Next: Review (下一步：审核)。
8. 选择 Add permissions (添加权限)。

使用查询编辑器进行连接

当您使用查询编辑器连接到集群时，您可以使用下列身份验证方法之一。每种方法都需要来自 Amazon Redshift 控制台的不同输入组合。

Amazon Secrets Manager

使用此方法，为存储在 Amazon Secrets Manager 中的 secret-arn 提供一个密钥值。此密钥包含用于连接到数据库的凭证。

临时凭证

使用此方法，提供 database 和 db-user 值。

在 Amazon Secrets Manager 中存储数据库凭证

调用查询编辑器时，您可以使用 Amazon Secrets Manager 中的密钥传递集群的凭证。要通过此方式传递凭证，您需要指定密钥的名称或 Amazon Resource Name (ARN)。

有关最低权限的更多信息，请参阅 Amazon Secrets Manager 用户指南中的使用 Amazon Secrets Manager 创建和管理密钥。

要将凭证存储在 Amazon Redshift 集群的密钥中

1. 使用 Amazon Secrets Manager 创建包含集群凭证的密钥。当您选择 Store a new secret（存储新密钥）时，选择 Credentials for Redshift cluster（Redshift 集群的凭证）。将 User name（用户名）（数据库用户）、Password（密码）和 DB cluster （数据库集群）（集群标识符）的值存储在您的密钥中。

   有关说明，请参阅 Amazon Secrets Manager 用户指南中的创建基本密钥。
2. 使用 Amazon Secrets Manager 控制台查看您创建的密钥的详细信息，或运行 `aws secretsmanager describe-secret` Amazon CLI 命令。

使用查询编辑器

在以下示例中，您使用查询编辑器执行以下任务：

- 运行 SQL 命令。
- 查看查询执行详细信息。
- 保存查询。
- 下载查询结果集。

要完成以下示例，您需要现有 Amazon Redshift 集群。如果您没有集群，请通过执行创建集群 (p. 84)中所述的过程来创建一个集群。

要在 Amazon Redshift 控制台上使用查询编辑器

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Query editor（查询编辑器），然后连接到集群中的数据库。
3. 对于架构，选择公有以基于该架构创建新表。
4. 在查询编辑器窗口中输入以下内容，然后选择 Run (运行) 以创建新表。

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

5. 选择 Clear (清除)。
6. 在查询编辑器窗口中输入以下命令，然后选择 Run (运行) 以向表中添加行。

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

7. 选择 Clear (清除)。
8. 在查询编辑器窗口中输入以下命令，然后选择 Run (运行) 以查询新表。

```
select * from shoes;
```

Query results (查询结果) 将显示相应结果。

Shoe 类型	颜色
sandals	black
loafers	brown

9. 选择 Execution (执行) 以查看运行详细信息。
10. 选择 Data (数据)，然后选择 Export (导出) 以便以文件形式下载查询结果。

计划查询

要创建运行 SQL 语句的计划，您可以使用 Amazon Redshift 控制台上的查询编辑器。您可以创建一个计划，以便按照与您的业务需求相匹配的时间间隔运行 SQL 语句。当计划查询运行时，Amazon EventBridge 会启动查询。

创建计划以运行 SQL 语句

1. 打开控制台和查询编辑器，如使用查询编辑器 (p. 131)中所述。您只能将此查询编辑器用于预调配集群。
2. 选择 Schedule（计划）以创建运行 SQL 语句的计划。

   在定义计划时，您需要提供以下信息：

   - 用于代入运行查询所需权限的 IAM 角色。有关更多信息，请参阅设置在 Amazon Redshift 控制台上计划查询的权限 (p. 132)。
   - Amazon Secrets Manager 或用于授权访问您的集群的临时凭证的身份验证值。有关更多信息，请参阅对计划查询进行身份验证 (p. 134)。
   - 计划查询的名称和要运行的单个 SQL 语句。
   - 计划频率和重复选项或 cron 格式的值。
   - 或者，您可以启用 Amazon SNS 通知来监控计划查询。如果您的查询正在运行，但您没有看到 SNS 主题中发布的消息，请参阅 Amazon EventBridge 用户指南中的我的规则正被触发，但我没有发现任何消息发布到我的 Amazon SNS 主题。

您还可以使用 Amazon Redshift 控制台管理和更新计划查询。根据控制台版本的不同，计划查询可能会在以下位置列出：

- 在集群的详细信息页面的 Schedules（计划）选项卡上。
- 在查询编辑器的 Scheduled queries（计划查询）选项卡中。

如果您从以下位置之一选择 Schedule name（计划名称），则可以查看和编辑计划查询的定义。

设置在 Amazon Redshift 控制台上计划查询的权限

要计划查询，定义计划的 Amazon Identity and Access Management (IAM) 用户以及与计划关联的 IAM 角色必须按如下方式进行配置。

对于登录 Amazon Redshift 控制台的 IAM 用户，请执行以下操作：

- 附加 `AmazonEventBridgeFullAccess` Amazon 托管策略。
- 附加一个策略，该策略具有您在定义计划 SQL 语句时指定的 IAM 角色的 `sts:AssumeRole` 权限。

以下示例显示了代入指定 IAM 角色的策略。

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

对于您指定的使调度程序能够运行查询的 IAM 角色，请执行以下操作：

- 确保此 IAM 角色指定了 EventBridge 服务委托人 (events.amazonaws.com)。以下是示例信任关系。

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

  有关如何为 EventBridge 事件创建 IAM 角色的更多信息，请参阅使用 Amazon EventBridge 调度程序所需的权限 (p. 371)。
- 将 AmazonRedshiftDataFullAccess Amazon 托管策略附加到 IAM 角色。
- 要允许 IAM 用户查看计划历史记录，请编辑 IAM 角色以添加 sts:AssumeRole 权限。

以下是 IAM 角色中的信任策略示例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Sid": "AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:user/user-name"
            },
```

```
            "Action": "sts:AssumeRole"
        }
    ]
}
```

以下示例代码段允许特定 IAM 用户查看计划历史记录。

```
{
      "Sid": "AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::account-id:user/testRedshiftUser",
          "arn:aws:iam::account-id:user/myusername"
        ]
      },
      "Action": "sts:AssumeRole"
    }
```

对计划查询进行身份验证

当您计划查询时，在查询 SQL 运行时使用下列身份验证方法之一。每种方法都需要来自 Amazon Redshift 控制台的不同输入组合。

Amazon Secrets Manager

使用此方法，为存储在 Amazon Secrets Manager 中的 secret-arn 提供一个密钥值。此密钥包含用于连接到数据库的凭证。密钥必须使用键 `RedshiftDataFullAccess` 进行标记。

有关最低权限的更多信息，请参阅 Amazon Secrets Manager 用户指南中的使用 Amazon Secrets Manager 创建和管理密钥。

临时凭证

使用此方法，提供 database 和 db-user 值。

`AmazonRedshiftDataFullAccess` 策略允许为 `redshift:GetClusterCredentials` 使用名为 `redshift_data_api_user` 权限的数据库用户 如果要使用其他数据库用户运行 SQL 语句，请向 IAM 角色添加策略以允许 `redshift:GetClusterCredentials`。以下示例策略允许数据库用户 `awsuser` 和 `myuser`。

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

创建一个在查询完成时运行的 Amazon EventBridge 规则

您可以创建事件规则，以在查询结束时发送通知。有关使用 Amazon EventBridge 控制台的过程，请参阅《Amazon EventBridge 用户指南》中的创建 Amazon EventBridge 规则以对事件做出反应。有关更多信息，请参阅 Amazon EventBridge 用户指南中 Amazon EventBridge 事件模式。

例如，在查询处于 FINISHED 状态时发送以下示例事件。

```
{
    "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": "awsome query",
        "state": "FINISHED",
        "pages": 5,
        "expireAt": "2020-12-22T18:43:48Z",
        "principal": "arn:aws:sts::123456789012:assumed-role/any",
        "queryId": 123456
    }
}
```

您可以创建事件模式规则来筛选事件。

```
{
    "source": [
        "aws.redshift-data"
    ],
    "detail-type": [
        "Redshift Data Statement Status Change"
    ],
    "detail": {
        "state": [
            "FINISHED"
        ]
    }
}
```

使用 SQL 客户端工具连接到 Amazon Redshift 集群

您可以通过 Java 数据库连接（JDBC）、Python 和开放式数据库连接（ODBC）这几种连接将 SQL 客户端工具连接到 Amazon Redshift 集群。Amazon Redshift 不提供或安装任何 SQL 客户端工具或库。要使用这些工具或库处理集群中的数据，请将它们安装在客户端计算机或 Amazon EC2 实例上。您可以使用支持 JDBC、Python 或 ODBC 驱动程序的大多数 SQL 客户端工具。

可以使用以下部分演练将客户端计算机或 Amazon EC2 实例配置为使用 JDBC、Python 或 ODBC 连接的过程。这些部分还讨论了与服务器的客户端连接的相关安全选项。此外，可在下面找到有关如何设置两种示例第三方 SQL 客户端工具（SQL Workbench/J 和 psql）并从其进行连接的信息。如果您还没有可以使用的商业智能工具，则可以尝试使用这些工具。您还可以通过此部分了解如何以编程方式连接到您的集群。最后，如果您在尝试连接到自己的集群时遇到问题，可以查看此部分中的故障排除信息以确定可行的解决方案。

主题

- 在 Amazon Redshift 中配置连接 (p. 136)
- 配置连接的安全选项 (p. 217)
- 通过客户端工具和代码连接到集群 (p. 221)
- 解决 Amazon Redshift 中的连接问题 (p. 263)

在 Amazon Redshift 中配置连接

在以下部分中，您可以了解如何配置 JDBC、Python 和 ODBC 连接以从 SQL 客户端工具连接到集群。此部分介绍如何设置 JDBC、Python 和 ODBC 连接。它还介绍了如何使用安全套接字层 (SSL) 和服务器证书来加密客户端和服务器之间的通信。

适用于 Amazon Redshift 的 JDBC、Python 和 ODBC 驱动程序

要处理您的集群中的数据，您需要使用 JDBC、Python 或 ODBC 驱动程序将您的客户端计算机或实例连接到该集群。对应用程序进行编码以使用 JDBC、Python 或 ODBC 数据访问 API 操作，并使用支持 JDBC 或 ODBC 的 SQL 客户端工具。

Amazon Redshift 提供 JDBC、Python 和 ODBC 驱动程序以供下载。这些驱动程序受 Amazon Web Services Support 支持。PostgreSQL 驱动程序未经过测试，也不受 Amazon Redshift 团队的支持。连接到 Amazon Redshift 集群时，请使用 Amazon Redshift 特定的驱动程序。Amazon Redshift 驱动程序具有以下优势：

- 支持 IAM、SSO 和联合身份验证。
- 支持新的 Amazon Redshift 数据类型。
- 支持身份验证配置文件。
- 结合 Amazon Redshift 增强功能提升性能。

有关如何下载 JDBC 和 ODBC 驱动程序和配置到集群的连接的更多信息，请参阅 为 Amazon Redshift 配置 JDBC 驱动程序版本 2.1 连接 (p. 136)、配置 Amazon Redshift Python 连接器 (p. 167) 和 配置 ODBC 连接 (p. 207)。

查找集群连接字符串

要将 SQL 客户端工具连接到您的集群，您需要使用集群连接字符串。您可以在 Amazon Redshift 控制台中的集群详细信息页面上查找集群连接字符串。

查找集群的连接字符串

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后从列表中选择集群名称以打开其详细信息。
3. 一般信息部分中提供有 JDBC URL 和 ODBC URL 连接字符串以及其他详细信息。每个字符串均基于运行集群的 Amazon 区域。点击相应连接字符串旁边的图标复制该字符串。

为 Amazon Redshift 配置 JDBC 驱动程序版本 2.1 连接

您可以使用 JDBC 驱动程序版本 2.1 连接将多种第三方 SQL 客户端工具连接到您的 Amazon Redshift 集群。Amazon Redshift Python 连接器提供了一个开源解决方案。您可以浏览源代码、请求增强功能、报告问题和提供文章。

要使用 JDBC 连接，请参阅以下部分。

主题

- 下载 Amazon Redshift JDBC 驱动程序版本 2.1 (p. 137)
- 安装 Amazon Redshift JDBC 驱动程序版本 2.1 (p. 138)
- 获取 JDBC URL (p. 139)
- 构建连接 URL (p. 139)
- 为您的 JDBC 连接配置 TCP Keepalive (p. 140)
- 使用 Apache Maven 配置 JDBC 连接 (p. 140)
- 配置身份验证和 SSL (p. 142)
- 配置 日志记录 (p. 145)
- 转换数据类型 (p. 146)
- 使用预编译的语句支持 (p. 147)
- JDBC 驱动程序 2.1 版本与 1.x 版本之间的差异 (p. 147)
- 为 JDBC 驱动程序版本 2.1 创建初始化（.ini）文件 (p. 148)
- JDBC 驱动程序版本 2.1 配置的选项 (p. 149)
- JDBC 驱动程序版本 2.1 的以前版本 (p. 166)

下载 Amazon Redshift JDBC 驱动程序版本 2.1

Amazon Redshift 向与 JDBC 4.2 API 兼容的工具提供驱动程序。此驱动程序的类名是 `com.amazon.redshift.jdbc42.Driver`。

有关如何安装 JDBC 驱动程序、引用 JDBC 驱动程序库和注册驱动程序类的详细信息，请参阅以下主题。

对于您在其上使用 Amazon Redshift JDBC 驱动程序版本 2.1 的每台计算机，请确保已安装 Java 运行时环境（JRE）8.0。

如果将 Amazon Redshift JDBC 驱动程序用于数据库身份验证，请确保您的 Java 类路径中包含 Amazon SDK for Java 1.11.118 或更高版本。如果您没有安装 Amazon SDK for Java，请下载带有与 JDBC 4.2 兼容的驱动程序和 Amazon SDK 驱动程序相关库的 ZIP 文件：

- 与 JDBC 4.2 兼容的驱动程序版本 2.1 和 Amazon SDK 驱动程序依赖库 在中国（北京）区域，请使用以下链接：与 JDBC 4.2 兼容的驱动程序版本 2.1 和 Amazon SDK 驱动程序依赖库

  此 ZIP 文件包含与 JDBC 4.2 兼容的驱动程序版本 2.1 和 Amazon SDK for Java 1.x 驱动程序相关库文件。将相关 jar 文件解压缩到与 JDBC 驱动程序相同的位置。只有 JDBC 驱动程序需要位于 CLASSPATH 中。

  此 ZIP 文件不包含完整的 Amazon SDK for Java 1.x。但是，它包含适用于 Amazon Identity and Access Management (IAM) 数据库身份验证所需的 Java 1.x 驱动程序相关库的 Amazon 开发工具包。

  将此 Amazon Redshift JDBC 驱动程序与 IAM 数据库身份验证所需的 Amazon SDK 一起使用。

  要安装完整的 Amazon SDK for Java 1.x，请参阅 Amazon SDK for Java 开发人员指南中的 Amazon SDK for Java 1.x。
- 与 JDBC 4.2 兼容的驱动程序版本 2.1（不含 Amazon SDK） 在中国（北京）区域，请使用以下链接：与 JDBC 4.2 兼容的驱动程序版本 2.1（不含 Amazon SDK）

查看 JDBC 驱动程序版本 2.1 软件许可证并更改日志文件：

- JDBC 驱动程序版本 2.1 许可证
- JDBC 驱动程序版本 2.1 更改日志

JDBC 驱动程序版本 1.2.27.1051 及更高版本支持 Amazon Redshift 存储过程。有关更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的在 Amazon Redshift 中创建存储过程。

安装 Amazon Redshift JDBC 驱动程序版本 2.1

要安装与 Amazon Redshift JDBC 4.2 兼容的驱动程序版本 2.1 和 Amazon SDK 的驱动程序相关库，将文件从 ZIP 归档提取到您选择的目录。

要安装与 Amazon Redshift JDBC 4.2 兼容的驱动程序版本 2.1（不含 Amazon SDK），将 JAR 文件复制到您选择的目录。

要使用 Amazon Redshift JDBC 驱动程序访问 Amazon Redshift 数据存储，您需要执行如下配置。

主题

- 引用 JDBC 驱动程序库 (p. 138)
- 注册驱动程序类 (p. 138)

引用 JDBC 驱动程序库

用于连接到数据的 JDBC 应用程序或 Java 代码必须访问驱动程序 JAR 文件。在应用程序或代码中，指定从 ZIP 归档中提取的所有 JAR 文件。

在 JDBC 应用程序中使用驱动程序

JDBC 应用程序通常提供一组用于添加驱动程序库文件列表的配置选项。使用提供的选项将 ZIP 归档中的所有 JAR 文件作为应用程序中的驱动程序配置的一部分。有关更多信息，请参阅您 JDBC 应用程序的文档。

在 Java 代码中使用驱动程序

您必须在类路径中包含所有驱动程序库文件。这是 Java 运行时环境搜索类和其他资源文件的路径。有关更多信息，请参阅相应的 Java SE 文档，以便为操作系统设置类路径。

- Windows：https://docs.oracle.com/javase/7/docs/technotes/tools/windows/classpath.html
- Linux 和 Solaris：https://docs.oracle.com/javase/7/docs/technotes/tools/solaris/classpath.html

注册驱动程序类

请确保您为您的应用程序注册了适当的类。您可以使用以下类将 Amazon Redshift JDBC 驱动程序连接到 Amazon Redshift 数据存储：

- `Driver` 类扩展 `java.sql.Driver`。
- `DataSource` 类扩展 `javax.sql.DataSource` 和 `javax.sql.ConnectionPoolDataSource`。

驱动程序支持以下独立于 JDBC 版本的完全限定类名：

- `com.amazon.redshift.jdbc.Driver`
- `com.amazon.redshift.jdbc.DataSource`

以下示例说明了如何使用 DriverManager 类建立 JDBC 4.2 的连接。

```
            private static Connection connectViaDM() throws Exception
{
Connection connection = null;
connection = DriverManager.getConnection(CONNECTION_URL);
return connection;
}
```

下面的示例展示了如何使用 DataSource 类建立连接。

```
 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;
}
```

获取 JDBC URL

您需要获知您的 Amazon Redshift 集群的 JDBC URL，才能将 SQL 客户端工具连接到该集群。JDBC URL 采用以下格式：jdbc:redshift://*endpoint*:*port*/*database*。

上述格式的字段具有以下值。

字段	值
jdbc	连接协议。
redshift	用于指定使用 Amazon Redshift 驱动程序连接到数据库的子协议。
endpoint	Amazon Redshift 集群的端点。
port	您在启动集群时指定的端口号。如果您启用了防火墙，请确保此端口处于打开状态，可供您使用。
database	您为集群创建的数据库。

以下是一个示例 JDBC URL：jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev

请务必以 URL 编码格式输入 URL 值，例如 SessionToken 值。

有关如何获取 JDBC 连接的信息，请参阅查找集群连接字符串 (p. 136)。

如果客户端计算机无法连接到数据库，您可以进行故障排除，解决可能存在的问题。有关更多信息，请参阅解决 Amazon Redshift 中的连接问题 (p. 263)。

构建连接 URL

使用连接 URL 向您正在访问的数据存储提供连接信息。以下是 Amazon Redshift JDBC 驱动程序 2.1 版本的连接 URL 的格式。此处，[主机] 是 Amazon Redshift 服务器的端点，[端口] 是服务器用于侦听客户端请求的传输控制协议 (TCP) 端口的编号。

```
jdbc:redshift://[Host]:[Port]
```

预设情况下，Amazon Redshift 会使用端口 5439。

以下是指定某些可选设置的连接 URL 的格式。

```
jdbc:redshift://[Host]:[Port]/[Schema];[Property1]=[Value];
[Property2]=[Value];
```

例如，假设您希望在 Amazon 上连接到位于美国西部（加利福尼亚北部）区域的 Amazon Redshift 集群上的端口 9000。您还希望访问名为 Default 的架构，并使用用户名和密码对连接进行身份验证。在此情况下，您使用以下连接 URL。

```
jdbc:redshift://redshift.company.us-west-
                1.redshift.amazonaws.com:9000/Default;UID=amazon;PWD=amazon
```

您可以使用以下字符来分隔 URL 字符串中的配置选项：

- ;
- ?
- &

例如，以下 URL 字符串等效：

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

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

以下 URL 示例指定日志级别 6 和日志的路径。

```
jdbc:redshift://redshift.amazonaws.com:5439/dev;DSILogLevel=6;LogPath=/home/user/logs";
```

不要复制连接 URL 中的属性。

有关可指定的配置选项的完整列表，请参阅 JDBC 驱动程序版本 2.1 配置的选项 (p. 149)。

为您的 JDBC 连接配置 TCP Keepalive

预设情况下，Amazon Redshift JDBC 驱动程序将配置为使用 TCP Keepalive 来防止连接超时。可以指定驱动程序开始发送 Keepalive 包的时间或通过在连接 URL 中设置相关属性来关闭该功能。有关连接 URL 的语法的更多信息，请参阅 构建连接 URL (p. 139)。

属性	描述
`TCPKeepAliveMinutes`	要指定驱动程序何时发送 Keepalive 包，请设置驱动程序开始发送 TCP Keepalive 包之前的非活动分钟数。
`TCPKeepAlive`	要关闭 TCP Keepalive，请将此属性设置为 `FALSE`。

使用 Apache Maven 配置 JDBC 连接

Apache Maven 是一款软件项目管理及理解工具。Amazon SDK for Java 支持 Apache Maven 项目。有关更多信息，请参阅 Amazon SDK for Java 开发人员指南中的将开发工具包与 Apache Maven 一起使用。

如果您使用 Apache Maven，可以配置并构建您的项目，以使用 Amazon Redshift JDBC 驱动程序与 Amazon Redshift 集群连接。为此，在项目的 `pom.xml` 文件中将 JDBC 驱动程序添加为依赖项。如果您使用 Maven 生成项目并希望使用 JDBC 连接，请执行以下部分中的步骤。

将 JDBC 驱动程序配置为 Maven 依赖项

将 JDBC 驱动程序配置为 Maven 依赖项

1. 将 Amazon 存储库或 Maven Central 存储库添加到您的 pom.xml 文件的存储库部分。

   Note

   以下代码示例中的 URL 如果用在浏览器中，将返回错误。仅在 Maven 项目的上下文中使用此 URL。

   对于 Amazon Maven 存储库，请使用以下内容。

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

   要使用安全套接字层 (SSL) 进行连接，请将以下存储库添加到您的 pom.xml 文件。

```
<repositories>
    <repository>
      <id>redshift</id>
      <url>https://s3.amazonaws.com/redshift-maven-repository/release</url>
    </repository>
</repositories>
```

   对于 Maven Central 存储库，请将以下内容添加到您的 pom.xml 文件。

```
<repositories>
    <repository>
      <id>redshift</id>
      <url>https://repo1.maven.org/maven2</url>
    </repository>
</repositories>
```

2. 在 pom.xml 文件的依赖项部分中，声明您要使用的驱动程序版本。

   Amazon Redshift 向与 JDBC 4.2 API 兼容的工具提供驱动程序。有关这些驱动程序支持的功能的信息，请参阅 下载 Amazon Redshift JDBC 驱动程序版本 2.1 (p. 137)。

   如下所示添加驱动程序的依赖项。

   将以下示例中的 *driver-version* 替换为您的驱动程序版本，例如 2.1.0.1。

   对于兼容 JDBC 4.2 的驱动程序，请使用以下内容。

```
<dependency>
   <groupId>com.amazon.redshift</groupId>
   <artifactId>redshift-jdbc42</artifactId>
   <version>driver-version</version>
</dependency>
```

   此驱动程序的类名是 com.amazon.redshift.jdbc42.Driver。

当您使用 IAM 数据库身份验证时，Amazon Redshift Maven 驱动程序需要以下可选依赖项。

```
<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>
```

将驱动程序升级到最新版本

要将 Amazon Redshift JDBC 驱动程序升级或更改到最新版本，请先将依赖项的版本部分修改为驱动程序的最新版本。然后用 Maven Clean Plugin 清除您的项目，如下所示。

```
mvn clean
```

配置身份验证和 SSL

为了防止数据遭到未经授权的访问，Amazon Redshift 数据存储要求所有连接都使用用户凭据进行身份验证。某些数据存储还要求通过安全套接字层 (SSL) 协议建立连接，无论是否使用单向身份验证。

Amazon Redshift JDBC 驱动程序 2.1 版提供了对这些身份验证协议的完全支持。

驱动程序支持的 SSL 版本取决于您使用的 JVM 版本。有关每个 Java 版本支持的 SSL 版本的信息，请参阅 Java 平台组产品管理博客上的诊断 TLS、SSL 和 HTTPS。

用于连接的 SSL 版本是驱动程序和服务器都支持的最高版本，该版本在连接时确定。

配置 Amazon Redshift JDBC 驱动程序版本 2.1，以根据要连接到的 Amazon Redshift 服务器的安全要求对连接进行身份验证。

要对连接进行身份验证，您必须始终提供您的 Amazon Redshift 用户名和密码。根据服务器上是否启用或需要 SSL，您可能还需要将驱动程序配置为通过 SSL 进行连接。或者，您可能要使用单向 SSL 身份验证，以便客户端（驱动程序本身）验证服务器的身份。

在连接 URL 中将配置信息提供给驱动程序。有关连接 URL 的语法的更多信息，请参阅 构建连接 URL (p. 139)。

SSL 表示 TLS/SSL，包括传输层安全性和安全套接字层。驱动程序支持 TLS/SSL 的行业标准版本。

仅使用用户名和密码

如果要连接的服务器不使用 SSL，则只需提供用户名和密码即可对连接进行身份验证。

仅使用您的用户名和密码配置身份验证

1. 将 `UID` 属性设置为您的用户名，以便访问 Amazon Redshift 服务器。
2. 将 PWD 属性设置为与您的用户名相对应的密码。

在不验证身份的情况下使用 SSL

如果要连接的服务器使用 SSL 但不需要身份验证，则可以将驱动程序配置为使用非验证 SSL 出厂设置。

要在不进行身份验证的情况下配置 SSL 连接

1. 将 `UID` 属性设置为您的用户名，以便访问 Amazon Redshift 服务器。
2. 将 `PWD` 属性设置为与您的用户名对应的密码。
3. 将 `SSLFactory` 属性设置为 `com.amazon.redshift.ssl.NonValidatingFactory`。

使用单向 SSL 身份验证

如果要连接的服务器使用 SSL 并且具有证书，则您可以将驱动程序配置为使用单向身份验证来验证服务器的身份。

单向身份验证需要签名、受信任的 SSL 证书来验证服务器的身份。您可以将驱动程序配置为使用特定证书或访问包含相应证书的 TrustStore。如果您未指定证书或 TrustStore，则驱动程序将使用默认的 Java TrustStore（通常为 `jssecacerts` 或 `cacerts`）。

要配置单向 SSL 身份验证

1. 将 UID 属性设置为您的用户名，以便访问 Amazon Redshift 服务器。
2. 将 PWD 属性设置为与您的用户名相对应的密码。
3. 将 SSL 属性设置为 true。
4. 将 SSLRootCert 属性设置为根 CA 证书的位置。
5. 如果您未使用默认的 Java TrustStore 之一，请执行以下操作之一：
   - 要指定服务器证书，请将 SSLRootCert 属性设置为证书的完整路径。
   - 要指定 TrustStore，请执行以下操作：
     a. 使用 keytool 程序将服务器证书添加到要使用的 TrustStore 中。
     b. 指定使用驱动程序启动 Java 应用程序时要使用的 TrustStore 和密码。例如：

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

6. 请选择一种：
   - 要验证证书，请将 SSLMode 属性设置为 verify-ca。
   - 要验证证书并确认证书中的主机名，请将 SSLMode 属性设置为 verify-full。

配置 IAM 身份验证

如果您使用 IAM 身份验证连接到 Amazon Redshift 服务器，请将以下属性设置为数据源连接字符串的一部分。

有关 IAM 身份验证的更多信息，请参阅 Amazon Redshift 中的 Identity and Access Management (p. 356)。

要使用 IAM 身份验证，请使用以下连接字符串格式之一：

连接字符串	描述
`jdbc:redshift:iam:// [host]:[port]/ [db]`	常规连接字符串。驱动程序从主机推断 ClusterID 和区域。

连接字符串	描述
`jdbc:redshift:iam:// [cluster-id]: [region]/[db]`	在已知 ClusterID 和区域的情况下，驱动程序将检索主机信息。
`jdbc:redshift:iam:// [host]/[db]`	驱动程序默认为端口 5439，并从主机推断 ClusterID 和区域。

指定配置文件

如果您使用 IAM 身份验证，则可以在配置文件名称下指定任何其他必需或可选的连接属性。通过这样做，您可以避免将某些信息直接放入连接字符串中。您可以使用 Profile 属性在连接字符串中指定配置文件名称。

配置文件可以添加到 Amazon 凭证文件。此文件的默认位置为：`~/.aws/credentials`

您可以通过在以下环境变量中设置路径更改默认值：`AWS_CREDENTIAL_PROFILES_FILE`

有关配置文件的更多信息，请参阅 Amazon SDK for Java 中的使用 Amazon 凭证。

使用实例配置文件凭证

如果您在与 IAM 角色关联的 Amazon EC2 实例上运行应用程序，则可以使用实例配置文件凭证进行连接。

为此，请使用上表中的 IAM 连接字符串格式之一，并将 dbuser 连接属性设置为您正要以其身份连接的 Amazon Redshift 用户名。

有关实例配置文件的更多信息，请参阅 IAM 用户指南中的访问控制。

使用凭证提供程序

驱动程序还支持来自以下服务的凭证提供程序插件：

- Active Directory 联合身份验证服务 (ADFS)
- JSON Web Token (JWT) 服务
- Microsoft Azure Active Directory (AD) 服务和浏览器 Microsoft Azure Active Directory (AD) 服务
- Okta 服务
- PingFederate 服务
- 适用于 SAML 服务（如 Okta、Ping 或 ADFS）的浏览器 SAML

如果您使用上述服务之一，则连接 URL 需要指定以下属性：

- Plugin_Name – 凭证提供程序插件类的完全限定类路径。
- IdP_Host：– 您用于对 Amazon Redshift 进行身份验证的服务的主机。
- IdP_Port – 身份验证服务的主机侦听的端口。Okta 不需要。
- User – idp_host 服务器的用户名。
- Password – 与 idp_host 用户名关联的密码。
- DbUser – 您连接时所依据的 Amazon Redshift 用户名。
- SSL_Insecure – 指示是否应验证 IDP 服务器证书。
- Client_ID – 与 Azure AD 门户中的用户名关联的客户端 ID。仅用于 Azure AD。
- Client_Secret – 与 Azure AD 门户中的客户端 ID 关联的客户端密钥。仅用于 Azure AD。
- IdP_Tenant – 适用于您的 Amazon Redshift 应用程序的 Azure AD 租户 ID。仅用于 Azure AD。
- App_ID – 您的 Amazon Redshift 应用程序的 Okta 应用程序 ID。仅适用于 Okta。
- 应用程序名称 – 您的 Amazon Redshift 应用程序的可选 Okta 应用程序名称。仅适用于 Okta。
- Partner_SPID – 可选的合作伙伴 SPID（服务提供商 ID）值。仅用于 PingFederate。

如果您将浏览器插件用于这些服务之一，则连接 URL 还可以包括：

- Login_URL – 通过浏览器插件使用安全断言标记语言 (SAML) 或 Azure AD 服务时，身份提供者网站上的资源的 URL。如果使用浏览器插件，则此参数是必需的。
- Listen_Port – 通过浏览器插件使用 SAML 或 Azure AD 服务时，驱动程序用于从身份提供者获取 SAML 响应的端口。
- IdP_Response_Timeout – 通过浏览器插件使用 SAML 或 Azure AD 服务时，驱动程序等待身份提供者的 SAML 响应的时间（以秒为单位）。

有关其他连接字符串属性的信息，请参阅JDBC 驱动程序版本 2.1 配置的选项 (p. 149)。

配置 日志记录

您可以在驱动程序中打开日志记录以帮助诊断问题。

您可以使用以下方法记录驱动程序信息：

- 要将记录的信息保存在 .log 文件中，请参阅 使用日志文件 (p. 145)。
- 要将记录的信息发送到 DriverManager 中指定的 LogStream 或 LogWriter，请参阅 使用 LogStream 或 LogWriter (p. 146)。

在连接 URL 中将配置信息提供给驱动程序。有关连接 URL 的语法的更多信息，请参阅 构建连接 URL (p. 139)。

使用日志文件

只有打开足够长的日志记录才能捕获问题。日志记录会降低性能，并会占用大量磁盘空间。

在连接 URL 中设置 LogLevel 键以打开日志记录并指定包含在日志文件中的详细信息量。下表列出了 Amazon Redshift JDBC 驱动程序版本 2.1 提供的日志记录级别，按从最不详细到最详细的顺序排列。

LogLevel 值	描述
1	记录将导致驱动程序中止的严重错误事件。
2	记录也许不会导致驱动程序中止运行的错误事件。
3	记录在未执行操作时可能导致错误的事件。
4	记录描述驱动程序进程的一般信息。
5	记录用于调试驱动程序的详细信息。
6	记录所有驱动程序活动。

要设置使用日志文件的日志记录

1. 将 LogLevel 属性设置为要包含在日志文件中的所需信息级别。
2. 将 LogPath 属性设置为您要保存日志文件的目标文件夹的完整路径。

   例如，以下连接 URL 启用日志记录级别 3 并将日志文件保存在 C:\temp 文件夹中：`jdbc:redshift://redshift.company.us-west- 1.redshift.amazonaws.com:9000/Default;DSILogLevel=3; LogPath=C:\temp`

3. 要确保新设置生效，请重新启动 JDBC 应用程序并重新连接到服务器。

   Amazon Redshift JDBC 驱动程序在 LogPath 属性中指定的位置生成以下日志文件：

   - redshift_jdbc.log 文件，该文件记录不特定于连接的驱动程序活动。
   - 与数据库建立的每个连接的 redshift_jdbc_connection_[Number].log 文件，其中 [Number] 是标识每个日志文件的编号。此文件记录特定于连接的驱动程序活动。

如果 LogPath 值无效，则驱动程序将记录的信息发送到标准输出流（`System.out`）

使用 LogStream 或 LogWriter

只有打开足够长的日志记录才能捕获问题。日志记录会降低性能，并会占用大量磁盘空间。

在连接 URL 中设置 LogLevel 键以打开日志记录，并指定发送到 DriverManager 中指定的 LogStream 或 LogWriter 的详细信息量。

要打开使用 LogStream 或 LogWriter 的日志记录：

1. 要将驱动程序配置为记录描述驱动程序进度的一般信息，请将 LogLevel 属性设置为 1 或 INFO。
2. 要确保新设置生效，请重新启动 JDBC 应用程序并重新连接到服务器。

要关闭使用 LogStream 或 LogWriter 的日志记录：

1. 从连接 URL 中删除 LogLevel 属性。
2. 要确保新设置生效，请重新启动 JDBC 应用程序并重新连接到服务器。

转换数据类型

Amazon Redshift JDBC 驱动程序版本 2.1 支持许多常见的数据格式，从而可在 Amazon Redshift、SQL 和 Java 数据类型之间进行转换。

下表列出了支持的数据类型映射。

Amazon Redshift 类型	SQL 类型	Java 类型
BIGINT	SQL_BIGINT	长整型
BOOLEAN	SQL_BIT	Boolean
CHAR	SQL_CHAR	字符串
DATE	SQL_TYPE_DATE	java.sql.Date
DECIMAL	SQL_NUMERIC	BigDecimal
DOUBLE PRECISION	SQL_DOUBLE	Double
GEOMETRY	SQL_ LONGVARBINARY	byte[]
INTEGER	SQL_INTEGER	整数
OID	SQL_BIGINT	长整型
SUPER	SQL_LONGVARCHAR	字符串
REAL	SQL_REAL	Float

Amazon Redshift 类型	SQL 类型	Java 类型
SMALLINT	SQL_SMALLINT	短型
TEXT	SQL_VARCHAR	字符串
TIME	SQL_TYPE_TIME	java.sql.Time
TIMETZ	SQL_TYPE_TIME	java.sql.Time
TIMESTAMP	SQL_TYPE_ TIMESTAMP	java.sql.Timestamp
TIMESTAMPTZ	SQL_TYPE_ TIMESTAMP	java.sql.Timestamp
VARCHAR	SQL_VARCHAR	字符串

使用预编译的语句支持

Amazon Redshift JDBC 驱动程序支持预编译的语句。您可以使用预编译的语句来提高需要在同一连接过程中多次运行的参数化查询的性能。

预编译的语句是在服务器端编译但不立即运行的 SQL 语句。在关闭对象或连接之前，已编译的语句作为 PreparedStatement 对象存储在服务器上。当该对象存在时，您可以根据需要使用不同的参数值多次运行预编译的语句，而无需再次编译该语句。此操作降低了开销，可以更快地运行一组查询。

有关预编译语句的更多信息，请参阅来自 Oracle 的 JDBC 基础知识教程中的“使用预编译语句”。

您可以预编译包含多个查询的语句。例如，以下预编译语句包含两个 INSERT 查询：

```
PreparedStatement pstmt = conn.prepareStatement("INSERT INTO
MyTable VALUES (1, 'abc'); INSERT INTO CompanyTable VALUES
(1, 'abc');");
```

请注意，这些查询不依赖于在同一预编译语句内指定的其他查询的结果。由于查询在预编译步骤期间未运行，因此尚未返回结果，并且不可用于同一预编译语句中的其他查询。

例如，不允许使用以下预编译语句，该语句将创建一个表，然后将值插入到该新创建的表中：

```
PreparedStatement pstmt = conn.prepareStatement("CREATE
TABLE MyTable(col1 int, col2 varchar); INSERT INTO myTable
VALUES (1, 'abc');");
```

如果您尝试预编译此语句，服务器将返回一个错误，指出目标表 (myTable) 尚不存在。必须先运行 CREATE 查询，然后才能预编译 INSERT 查询。

JDBC 驱动程序 2.1 版本与 1.x 版本之间的差异

本节介绍 JDBC 驱动程序的 2.1 和 1.x 版本返回的信息的差异。JDBC 驱动程序 1.x 版本已停产。

下表列出了由 getDatabaseProductName() 和 getDatabaseProductVersion() 函数为每个版本的 JDBC 驱动程序返回的 DatabaseMetadata 信息。JDBC 驱动程序版本 2.1 在建立连接时获取值。JDBC 驱动程序版本 1.x 通过查询获取值。

JDBC 驱动程序版本	getDatabaseProductName() 结果	getDatabaseProductVersion() 结果
2.1	Redshift	8.0.2

JDBC 驱动程序版本	getDatabaseProductName() 结果	getDatabaseProductVersion() 结果
1.x	PostgreSQL	08.00.0002

下表列出了由 getTypeInfo 函数为每个版本的 JDBC 驱动程序返回的 DatabaseMetadata 信息。

JDBC 驱动程序版本	getTypeInfo 结果
2.1	与 Redshift 数据类型一致
1.x	与 PostgreSQL 数据类型保持一致

为 JDBC 驱动程序版本 2.1 创建初始化（.ini）文件

通过对 Amazon Redshift JDBC 驱动程序 2.1 版本使用初始化（.ini）文件，您可以指定系统级别的配置参数。例如，联合 IdP 身份验证参数可能因每个应用程序而异。.ini 文件为 SQL 客户端提供了获取所需配置参数的常见位置。

您可以创建包含 SQL 客户端配置选项的 JDBC 驱动程序 2.1 版本初始化（.ini）文件。文件的默认名称为 `rsjdbc.ini`。JDBC 驱动程序 2.1 版本在按优先级顺序列出的以下位置检查 .ini 文件：

- `IniFile`连接 URL 或 SQL 客户端的连接属性对话框中的 参数。请确保 `IniFile` 参数包含 .ini 文件的完整路径，其中包括文件名。有关 `IniFile` 参数的信息，请参阅 IniFile (p. 157)。如果 `IniFile` 参数错误地指定了 .ini 文件的位置，将显示错误。
- 环境变量，例如具有完整路径 AMAZON_REDSHIFT_JDBC_INI_FILE，包括文件名。您可以使用 `rsjdbc.ini` 或指定文件名。如果 AMAZON_REDSHIFT_JDBC_INI_FILE 环境变量错误地指定了 .ini 文件的位置，将显示一个错误。
- 驱动程序 JAR 文件所在的目录。
- 用户主目录。
- 系统的临时目录。

您可以将 .ini 文件组织成各个部分，例如 [DRIVER]。每个部分都包含键-值对，这些键-值对将指定各种连接参数。您可以使用 `IniSection` 参数来指定 .ini 文件中的部分。有关 `IniSection` 参数的信息，请参阅 IniSection (p. 157)。

以下是 .ini 文件格式的示例，其中包含了 [DRIVER]、[DEV]、[QA] 和 [PROD] 的部分。[DRIVER] 部分可以应用于任何连接。

```
[DRIVER]
key1=val1
key2=val2

[DEV]
key1=val1
key2=val2

[QA]
key1=val1
key2=val2

[PROD]
key1=val1
key2=val2
```

JDBC 驱动程序 2.1 版本从按优先级顺序列出的以下位置加载配置参数：

- 应用程序代码中的默认配置参数。
- .ini 文件中的 [DRIVER] 部分属性（如果包含）。
- 自定义部分配置参数，如果 `IniSection` 选项在连接 URL 或 SQL 客户端的连接属性对话框中提供。
- `getConnection` 调用中指定的连接属性对象的属性。
- 连接 URL 中指定的配置参数。

JDBC 驱动程序版本 2.1 配置的选项

下面，您可以找到您可以为 Amazon Redshift JDBC 驱动程序 2.1 版本指定的选项的说明。

您可以使用连接 URL 设置配置属性。有关更多信息，请参阅构建连接 URL (p. 139)。

主题

- AccessKeyID (p. 150)
- AllowDBUserOverride (p. 151)
- App_ID (p. 151)
- App_Name (p. 151)
- ApplicationName (p. 151)
- AuthProfile (p. 152)
- AutoCreate (p. 152)
- Client_ID (p. 152)
- Client_Secret (p. 152)
- ClusterID (p. 152)
- connectTimeout (p. 153)
- databaseMetadataCurrentDbOnly (p. 153)
- DbUser (p. 153)
- DbGroups (p. 153)
- DBNAME (p. 153)
- defaultRowFetchSize (p. 154)
- DisableIsValidQuery (p. 154)
- enableFetchReadAndProcessBuffers (p. 154)
- enableFetchRingBuffer (p. 154)
- enableMultiSqlSupport (p. 155)
- fetchRingBufferSize (p. 155)
- ForceLlowcase (p. 155)
- groupFederation (p. 155)
- HOST (p. 156)
- IAMDisableCache (p. 156)
- IAMDuration (p. 156)
- IdP_Host (p. 156)
- IdP_Port (p. 157)
- IdP_Tenant (p. 157)
- IdP_Response_Timeout (p. 157)
- IniFile (p. 157)

- IniSection (p. 157)
- isServerless (p. 158)
- Login_URL (p. 158)
- loginTimeout (p. 158)
- loginToRp (p. 158)
- LogLevel (p. 158)
- LogPath (p. 159)
- Partner_SPID (p. 159)
- Password (p. 160)
- Plugin_Name (p. 160)
- PORT (p. 160)
- Preferred_Role (p. 160)
- Profile (p. 161)
- PWD (p. 161)
- queryGroup (p. 161)
- readOnly (p. 161)
- Region (p. 161)
- reWriteBatchedInserts (p. 162)
- reWriteBatchedInsertsSize (p. 162)
- roleArn (p. 162)
- roleSessionName (p. 162)
- scope (p. 162)
- SecretAccessKey (p. 162)
- SessionToken (p. 163)
- serverlessAcctId (p. 163)
- serverlessWorkGroup (p. 163)
- socketFactory (p. 163)
- socketTimeout (p. 163)
- SSL (p. 164)
- SSL_Insecure (p. 164)
- SSLCert (p. 164)
- SSLFactory (p. 164)
- SSLKey (p. 165)
- SSLMode (p. 165)
- SSLPassword (p. 165)
- SSLRootCert (p. 165)
- StsEndpointUrl (p. 165)
- tcpKeepAlive (p. 165)
- UID (p. 166)
- User (p. 166)
- webIdentityToken (p. 166)

AccessKeyID

- 默认值 – 无

- 数据类型 – 字符串

您可以指定此参数以输入 IAM 用户或角色的 IAM 访问密钥。您通常可以通过查看现有的字符串或用户配置文件来查找密钥。如果您指定此参数，还必须指定 `SecretAccessKey` 参数。

此参数为可选项。

AllowDBUserOverride

- 默认值 - 0
- 数据类型 – 字符串

此选项指定驱动程序是使用 SAML 断言中的 `DbUser` 值，还是连接 URL 的 `DbUser` 连接属性中指定的值。

此参数为可选项。

1

驱动程序使用 SAML 断言中的 `DbUser` 值。

如果 SAML 断言没有为 `DBUser` 指定值，则驱动程序将使用 `DBUser` 连接属性中指定的值。如果连接属性也没有指定值，则驱动程序将使用连接配置文件中指定的值。

0

驱动程序使用 `DBUser` 连接属性中指定的 `DBUser` 值。

如果 `DBUser` 连接属性没有指定值，则驱动程序将使用连接配置文件中指定的值。如果连接配置文件也没有指定值，则驱动程序将使用 SAML 断言中的值。

App_ID

- 默认值 – 无
- 数据类型 – 字符串

Okta 提供的与您的 Amazon Redshift 应用程序关联的唯一 ID。

如果通过 Okta 服务进行身份验证，则此参数是必需的。

App_Name

- 默认值 – 无
- 数据类型 – 字符串

您用于验证与 Amazon Redshift 的连接的 Okta 应用程序的名称。

此参数为可选项。

ApplicationName

- 默认值 – null
- 数据类型 – 字符串

传递给 Amazon Redshift 以供审计的应用程序的名称。

此参数为可选项。

AuthProfile

- 默认值 – 无
- 数据类型 – 字符串

用于连接到 Amazon Redshift 的身份验证配置文件的名称。

此参数为可选项。

AutoCreate

- 默认值 – false
- 数据类型 – Boolean

此选项指定在指定用户不存在时驱动程序是否导致新用户被创建。

此参数为可选项。

true

如果通过 `DBUser` 或唯一 ID (UID) 指定的用户不存在，则会创建具有该名称的新用户。

false

驱动程序不会导致新用户被创建。如果指定的用户不存在，则身份验证将失败。

Client_ID

- 默认值 – 无
- 数据类型 – 字符串

使用 Azure AD 服务对连接进行身份验证时使用的客户端 ID。

如果通过 Azure AD 服务进行身份验证，则此参数是必需的。

Client_Secret

- 默认值 – 无
- 数据类型 – 字符串

使用 Azure AD 服务对连接进行身份验证时使用的客户端密钥。

如果通过 Azure AD 服务进行身份验证，则此参数是必需的。

ClusterID

- 默认值 – 无
- 数据类型 – 字符串

要连接到的 Amazon Redshift 集群的名称。

此参数为可选项。

connectTimeout

- 默认值 – 10
- 数据类型 – 整数

用于套接字连接操作的超时值。如果建立 Amazon Redshift 连接所需的时间超过此值，则系统将该连接视为不可用。超时以秒为单位指定。值为 0 表示未指定超时。

此参数为可选项。

databaseMetadataCurrentDbOnly

- 默认值 – true
- 数据类型 – Boolean

此选项指定元数据 API 是从所有可访问的数据库中检索数据，还是仅从连接的数据库检索数据。

此参数为可选项。

可以指定以下值：

true

应用程序从单个数据库中检索元数据。

false

应用程序从所有可访问的数据库中检索元数据。

DbUser

- 默认值 – 无
- 数据类型 – 字符串

用于您的 Amazon Redshift 账户的用户 ID。如果您启用了 AutoCreate 属性，则可以使用当前不存在的 ID。

此参数为可选项。

DbGroups

- 默认值 – PUBLIC
- 数据类型 – 字符串

`DBUser` 为当前会话加入的现有数据库组名称的逗号分隔列表。

此参数为可选项。

DBNAME

- 默认值 – null
- 数据类型 – 字符串

要连接的数据库的名称。您可以使用此选项在 JDBC 连接 URL 中指定数据库名称。

此参数为必需参数。您必须在连接 URL 或客户端应用程序的连接属性中指定数据库名称。

defaultRowFetchSize

- 默认值：0
- 数据类型 – 整数

此选项可指定 getFetchSize 的默认值。

此参数为可选项。

可以指定以下值：

0

在单一操作中取回所有行。

正整数

对于 ResultSet 的每次取回迭代，要从数据库中取回的行数。

DisableIsValidQuery

- 默认值 – False
- 数据类型 – Boolean

此选项指定驱动程序在使用 Connection.isValid() 方法来确定数据库连接是否处于活动状态时是否提交新的数据库查询。

此参数为可选项。

true

驱动程序在使用 Connection.isValid() 方法来确定数据库连接是否处于活动状态时不提交查询。如果数据库服务器意外关闭，这可能会导致驱动程序错误地将数据库连接标识为活动状态。

false

驱动程序在使用 Connection.isValid() 方法来确定数据库连接是否处于活动状态时提交查询。

enableFetchReadAndProcessBuffers

- 默认值 – true
- 数据类型 – Boolean

使用此选项，可以让 Amazon Redshift 使用环形缓冲区和单独线程上的处理缓冲区来提取行，进而提高性能。

此参数为可选项。

enableFetchRingBuffer

- 默认值 – true
- 数据类型 – Boolean

此选项指定驱动程序使用单独线程上的环形缓冲区取回行。fetchRingBufferSize 参数指定环形缓冲区的大小。

此参数为可选项。

enableMultiSqlSupport

- 默认值 – true
- 数据类型 – Boolean

此选项指定是否处理语句中以分号分隔的多个 SQL 命令。

此参数为可选项。

可以指定以下值：

true

驱动程序处理语句对象中多个用分号分隔的 SQL 命令。

false

驱动程序为单个语句中的多个 SQL 命令返回错误。

fetchRingBufferSize

- 默认值 – 1G
- 数据类型 – 字符串

此选项指定在取回结果集时使用的环形缓冲区的大小。您可以指定以字节为单位的大小，例如 1K 表示 1 KB，5000 代表 5000 字节，1M 表示 1 MB，1G 表示 1 GB，依此类推。您还可以指定堆内存的百分比。驱动程序在达到限制时停止取回行。当应用程序读取行并释放环形缓冲区中的空间时，取回将恢复。

此参数为可选项。

ForceLlowcase

- 默认值 – false
- 数据类型 – Boolean

此选项指定在使用单点登录身份验证时，驱动程序是否会将从身份提供者发送到 Amazon Redshift 的所有数据库组 (DbGroup) 设为小写。

此参数为可选项。

true

驱动程序会小写从身份提供程序发送的所有数据库组。

false

驱动程序不会更改数据库组。

groupFederation

- 默认值 – false
- 数据类型 – Boolean

此选项指定是否使用 Amazon Redshift IDP 组。此选项由 GetClusterCredentialsV2 API 支持。

此参数为可选项。

true

使用 Amazon Redshift 身份提供者（IDP）组。

false

使用 STS API 和 GetClusterCredentials 进行用户联合身份验证，并明确指定用于连接的 DbGroups。

HOST

- 默认值 – null
- 数据类型 – 字符串

要连接到 Amazon Redshift 服务器的主机名。您可以使用此选项在 JDBC 连接 URL 中指定主机名。

此参数为必需参数。您必须在连接 URL 或客户端应用程序的连接属性中指定主机名。

IAMDisableCache

- 默认值 – false
- 数据类型 – Boolean

此选项指定是否缓存 IAM 凭证。

此参数为可选项。

true

IAM 凭证不会被缓存。

false

IAM 凭证将被缓存。例如，当对 API 网关的请求受到限制时，这会提高性能。

IAMDuration

- 默认值 – 900
- 数据类型 – 整数

临时 IAM 凭证过期之前的时间长度 (以秒为单位)。

- 最小值 – 900
- 最大值 – 3,600

此参数为可选项。

IdP_Host

- 默认值 – 无
- 数据类型 – 字符串

您用于对 Amazon Redshift 进行身份验证的 IdP（身份提供者）主机。该选项可以在连接字符串或配置文件中指定。

此参数为可选项。

IdP_Port

- 默认值 – 无
- 数据类型 – 字符串

IdP（身份提供者）使用的端口。您可以在连接字符串或配置文件中指定端口。默认端口为 5439。

此参数为可选项。

IdP_Tenant

- 默认值 – 无
- 数据类型 – 字符串

适用于您的 Amazon Redshift 应用程序的 Azure AD 租户 ID。

如果通过 Azure AD 服务进行身份验证，则此参数是必需的。

IdP_Response_Timeout

- 默认值 – 120
- 数据类型 – 整数

当通过浏览器插件使用 SAML 或 Azure AD 服务时，驱动程序等待身份提供者发出 SAML 响应的时间（以秒为单位）。

此参数为可选项。

IniFile

- 默认值 – 无
- 数据类型 – 字符串

.ini 文件的完整路径，包括文件名。例如：

```
IniFile="C:\tools\rsjdbc.ini"
```

有关 .ini 文件的信息，请参阅为 JDBC 驱动程序版本 2.1 创建初始化（.ini）文件 (p. 148)。

此参数为可选项。

IniSection

- 默认值 – 无
- 数据类型 – 字符串

.ini 文件中包含配置选项的部分的名称。有关 .ini 文件的信息，请参阅为 JDBC 驱动程序版本 2.1 创建初始化（.ini）文件 (p. 148)。

以下示例指定 .ini 文件的 [Prod] 部分：

```
IniSection="Prod"
```

此参数为可选项。

isServerless

- 默认值 – false
- 数据类型 – Boolean

此选项指定 Amazon Redshift 端点主机是否为无服务器实例。驱动程序将尝试从给定主机中检测此参数。如果您使用的是网络负载均衡器 (NLB)，则驱动程序将无法检测到它，因此您可以在此处对其进行设置。

此参数为可选项。

true

Amazon Redshift 端点主机是一个无服务器实例。

false

Amazon Redshift 端点主机是一个预置集群。

Login_URL

- 默认值 – 无
- 数据类型 – 字符串

通过浏览器插件使用 SAML 或 Azure AD 服务时，身份提供者网站上的资源 URL。

如果通过浏览器插件使用 SAML 或 Azure AD 服务进行身份验证，则此参数是必需的。

loginTimeout

- 默认值：0
- 数据类型 – 整数

连接服务器并对服务器进行身份验证时发生超时前等待的秒数。如果建立连接的用时长于此阈值，则连接将被中止。

当此属性设置为 0 时，连接不会发生超时。

此参数为可选项。

loginToRp

- 默认值 – `urn:amazon:webservices`
- 数据类型 – 字符串

要用于 AD FS 身份验证类型的信赖方信任。

此参数为可选项。

LogLevel

- 默认值 - 0
- 数据类型 – 整数

使用此属性可以打开或关闭驱动程序中的日志记录并指定包含在日志文件中的详细信息量。

只有启用足够长的日志记录才能捕获问题。日志记录会降低性能，并会占用大量磁盘空间。

此参数为可选项。

将参数设置为以下值之一：

0

禁用所有日志记录。

1

启用 FATAL 级别的日志记录，该级别日志记录将记录导致驱动程序中止的非常严重错误事件。

2

启用 ERROR 级别的日志记录，该级别日志记录将记录可能仍然允许驱动程序继续运行的错误事件。

3

启用 WARNING 级别的日志记录，该级别日志记录将记录在未执行操作时可能导致错误的事件。

4

启用 INFO 级别的日志记录，该级别日志记录将记录描述驱动程序进程的一般信息。

5

启用 DEBUG 级别的日志记录，该级别日志记录将记录对调试驱动程序很有用的详细信息。

6

启用 TRACE 级别的日志记录，该级别日志记录将记录所有驱动程序活动。

启用日志记录后，驱动程序会在 `LogPath` 属性指定的位置生成以下日志文件：

- **`redshift_jdbc.log`** – 记录不特定于连接的驱动程序活动的文件。
- **`redshift_jdbc_connection_[Number].log`** – 与数据库建立的每个连接的文件，其中 `[Number]` 是区分每个日志文件和其他日志文件的数字。此文件记录特定于连接的驱动程序活动。

如果 LogPath 值无效，则驱动程序将记录的信息发送到标准输出流 `System.out`。

LogPath

- 默认值 – 当前工作目录。
- 数据类型 – 字符串

启用 DSILogLevel 属性时驱动程序保存日志文件所在的文件夹的完整路径。

为了确保连接 URL 与所有 JDBC 应用程序兼容，我们建议您通过键入另一个反斜杠来转义文件路径中的反斜杠 (\)。

此参数为可选项。

Partner_SPID

- 默认值 – 无
- 数据类型 – 字符串

在使用 PPingFederate 服务验证连接时使用的合作伙伴 SPID（服务提供商 ID）值。

此参数为可选项。

Password

- 默认值 – 无
- 数据类型 – 字符串

使用 IAM 身份验证通过 IDP 进行连接时，它是 IDP_Host 服务器的密码。使用标准身份验证时，它可用于 Amazon Redshift 数据库密码，而不是 PWD。

此参数为可选项。

Plugin_Name

- 默认值 – 无
- 数据类型 – 字符串

实施特定凭证提供程序插件的完全限定类名称。

此参数为可选项。

以下提供程序选项受支持：

- **`AdfsCredentialsProvider`** – Active Directory 联合身份验证服务
- **`AzureCredentialsProvider`** – Microsoft Azure Active Directory (AD) 服务
- **`BasicJwtCredentialsProvider`** – JSON Web Token (JWT) 服务
- **`BasicSamlCredentialsProvider`** – 您可以与许多 SAML 服务提供商一起使用的安全断言标记语言（SAML）凭据。
- **`BrowserAzureCredentialsProvider`** – 浏览器 Microsoft Azure Active Directory (AD) 服务
- **`BrowserAzureOAuth2CredentialsProvider`** – 用于本机身份验证的浏览器 Microsoft Azure Active Directory (AD) 服务
- **`BrowserSamlCredentialsProvider`** – 用于 SAML 服务（如 Okta、Ping 或 ADFS）的浏览器 SAML
- **`OktaCredentialsProvider`** – Okta 服务
- **`PingCredentialsProvider`** – PingFederate 服务

PORT

- 默认值 – null
- 数据类型 – 整数

要连接到 Amazon Redshift 服务器的端口。您可以使用此选项在 JDBC 连接 URL 中指定端口。

此参数为可选项。

Preferred_Role

- 默认值 – 无
- 数据类型 – 字符串

您希望在 Amazon Redshift 连接期间代入的 IAM 角色。

此参数为可选项。

Profile

- 默认值 – 无
- 数据类型 – 字符串

用于 IAM 身份验证的配置文件的名称。此配置文件包含未在连接字符串中指定的任何其他连接属性。

此参数为可选项。

PWD

- 默认值 – 无
- 数据类型 – 字符串

与您使用属性 UID 提供的 Amazon Redshift 用户名相对应的密码。

此参数为可选项。

queryGroup

- 默认值 – null
- 数据类型 – 字符串

此选项通过将查询分配到相应的查询组在运行时向队列分配查询。将为会话设置查询组。在连接上运行的所有查询都属于此查询组。

此参数为可选项。

readOnly

- 默认值 – false
- 数据类型 – Boolean

此属性指定驱动程序是否处于只读模式。

此参数为可选项。

true

连接处于只读模式，无法写入数据存储。

false

连接不处于只读模式，可以写入数据存储。

Region

- 默认值 – null
- 数据类型 – 字符串

此选项指定集群所在的 Amazon 区域。如果指定 StsEndPoint 选项，则会忽略 Region（区域）选项。Redshift `GetClusterCredentials` API 操作也使用 Region（区域）选项。

此参数为可选项。

reWriteBatchedInserts

- 默认值 – false
- 数据类型 – Boolean

通过此选项，可以优化批处理的兼容 INSERT 语句的重写和合并。

此参数为可选项。

reWriteBatchedInsertsSize

- 默认值 – 128
- 数据类型 – 整数

通过此选项，可以优化批处理的兼容 INSERT 语句的重写和合并。此值必须以 2 为幂呈指数增加。

此参数为可选项。

roleArn

- 默认值 – 无
- 数据类型 – 字符串

角色的 Amazon Resource Name (ARN)。在为 Plugin_Name 选项指定 BasicJwtCredentialsProvider 时，请确保指定此参数。采用以下格式指定 ARN：

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

如果您为 Plugin_Name 选项指定 BasicJwtCredentialsProvider，则此参数为必需项。

roleSessionName

- 默认值 – jwt_redshift_session
- 数据类型 – 字符串

所代入角色会话的标识符。通常，您可以传递与应用程序用户关联的名称或标识符。您的应用程序使用的临时安全凭证与该用户相关联。在为 Plugin_Name 选项指定 BasicJwtCredentialsProvider 时，您可以指定此参数。

此参数为可选项。

scope

- 默认值 – 无
- 数据类型 – 字符串

用户可以同意的范围列表，以空格分隔。您可以指定此参数，以便 Microsoft Azure 应用程序可以获得您想调用的 API 的同意。在为 Plugin_Name 选项指定 BrowserAzureOAuth2CredentialsProvider 时，您可以指定此参数。

此参数是 BrowserAzureOAuth2CredentialsProvider 插件必需的。

SecretAccessKey

- 默认值 – 无

- 数据类型 – 字符串

用户或角色的 IAM 访问密钥。如果指定了此选项，则还必须指定 AccessKeyID。

此参数为可选项。

SessionToken

- 默认值 – 无
- 数据类型 – 字符串

与您用于身份验证的 IAM 角色关联的临时 IAM 会话令牌。

此参数为可选项。

serverlessAcctId

- 默认值 – null
- 数据类型 – 字符串

Amazon Redshift Serverless 账户 ID。驱动程序将尝试从给定主机中检测此参数。如果您使用的是网络负载均衡器 (NLB)，则驱动程序将无法检测到它，因此您可以在此处对其进行设置。

此参数为可选项。

serverlessWorkGroup

- 默认值 – null
- 数据类型 – 字符串

Amazon Redshift Serverless 工作组名称。驱动程序将尝试从给定主机中检测此参数。如果您使用的是网络负载均衡器 (NLB)，则驱动程序将无法检测到它，因此您可以在此处对其进行设置。

此参数为可选项。

socketFactory

- 默认值 – null
- 数据类型 – 字符串

此选项指定了用于创建套接字的套接字产生组件。

此参数为可选项。

socketTimeout

- 默认值 - 0
- 数据类型 – 整数

套接字读取操作发生超时前等待的秒数。如果操作用时长于此阈值，则连接将被关闭。当此属性设置为 0 时，连接不会发生超时。

此参数为可选项。

SSL

- 默认值 – TRUE
- 数据类型 – 字符串

使用此属性可以打开或关闭连接的 SSL。

此参数为可选项。

可以指定以下值：

TRUE

驱动程序通过 SSL 连接到服务器。

FALSE

驱动程序在不使用 SSL 的情况下连接到服务器。IAM 身份验证不支持此选项。

或者，您也可以配置 AuthMech 属性。

SSL_Insecure

- 默认值 – true
- 数据类型 – 字符串

此属性指示是否应验证 IDP 主机服务器证书。

此参数为可选项。

可以指定以下值：

true

驱动程序不检查 IDP 服务器证书的真实性。

false

驱动程序检查 IDP 服务器证书的真实性。

SSLCert

- 默认值 – 无
- 数据类型 – 字符串

.pem 或 .crt 文件的完整路径，其中包含在使用 SSL 时用于验证 Amazon Redshift 服务器实例的其他受信任 CA 证书。

如果指定了 SSLKey，则此参数为必填项。

SSLFactory

- 默认值 – 无
- 数据类型 – 字符串

在不使用服务器证书的情况下，通过 TLS/SSL 连接到服务器时使用的 SSL 出厂设置。

SSLKey

- 默认值 – 无
- 数据类型 – 字符串

.der 文件的完整路径，包含用于验证 SSLCert 中指定的证书的 PKCS8 密钥文件。

如果指定了 SSLCert，则此参数为必填项。

SSLMode

- 默认值 – verify-ca
- 数据类型 – 字符串

使用此属性指定启用 TLS/SSL 时驱动程序如何验证证书。

此参数为可选项。

可以指定以下值：

verify-ca

驱动程序验证证书是否来自受信任的证书颁发机构 (CA)。

verify-full

驱动程序验证证书来自受信任的 CA，以及证书中的主机名是否与连接 URL 中指定的主机名匹配。

SSLPassword

- 默认值 - 0
- 数据类型 – 字符串

在 SSLKey 中指定的加密密钥文件的密码。

如果指定了 SSLKey 且对密钥文件进行了加密，则此参数为必填项。

SSLRootCert

- 默认值 – 无
- 数据类型 – 字符串

.pem 或 .crt 文件的完整路径，其中包含在使用 SSL 时用于验证 Amazon Redshift 服务器实例的根 CA 证书。

StsEndpointUrl

- 默认值 – null
- 数据类型 – 字符串

您可以指定 Amazon Security Token Service (Amazon STS) 端点。如果指定此选项，则 Region（区域）选项将被忽略。您只能为此端点指定安全协议 (HTTPS)。

tcpKeepAlive

- 默认值 – TRUE

- 数据类型 – 字符串

使用此属性可打开或关闭 TCP Keepalive。

此参数为可选项。

可以指定以下值：

TRUE

驱动程序将使用 TCP Keepalive 来防止连接超时。

FALSE

驱动程序不使用 TCP Keepalive。

UID

- 默认值 – 无
- 数据类型 – 字符串

用于访问数据库的用户名。

此参数为必需参数。

User

- 默认值 – 无
- 数据类型 – 字符串

使用 IAM 身份验证通过 IDP 进行连接时，它是 idp_host 服务器的用户名。使用标准身份验证时，它可用于 Amazon Redshift 数据库用户名。

此参数为可选项。

webIdentityToken

- 默认值 – 无
- 数据类型 – 字符串

身份提供者提供的 OAuth 2.1 访问令牌或 OpenID Connect ID 令牌。您的应用程序必须通过 Web 身份提供者对您的应用程序用户进行身份验证来获取此令牌。在为 Plugin_Name 选项指定 BasicJwtCredentialsProvider 时，请确保指定此参数。

如果您为 Plugin_Name 选项指定 BasicJwtCredentialsProvider，则此参数为必填项。

JDBC 驱动程序版本 2.1 的以前版本

仅当您的工具需要使用某个特定版本的驱动程序时，才能下载 Amazon Redshift JDBC 驱动程序版本 2.1 的以前版本。

以下是以前的与 JDBC 4.2 兼容的 JDBC 驱动程序版本 2.1 驱动程序：

- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.8/redshift-jdbc42-2.1.0.8.zip 在中国（北京）区域，请使用以下链接：https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/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 在中国（北京）区域，请使用以下链接：https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/jdbc/2.1.0.7/redshift-jdbc42-2.1.0.7.zip

配置 Amazon Redshift Python 连接器

通过使用适用于 Python 的 Amazon Redshift 连接器，您可以将工作与适用于 Python 的 Amazon SDK（Boto3）以及 Pandas 和 Numerical Python（NumPy）集成。有关 pandas 的更多信息，请参阅 pandas GitHub 存储库。有关 NumPy 的更多信息，请参阅 NumPy GitHub 存储库。

Amazon Redshift Python 连接器提供了一个开源解决方案。您可以浏览源代码、请求增强功能、报告问题和提供文章。

要使用 Amazon Redshift Python 连接器，请确保使用 Python 3.6 或更高版本。有关更多信息，请参阅Amazon Redshift Python 驱动程序许可协议。

Amazon Redshift Python 连接器提供以下内容：

- Amazon Identity and Access Management（IAM）身份验证 有关更多信息，请参阅Amazon Redshift 中的 Identity and Access Management (p. 356)。
- 使用联合 API 访问进行身份提供者身份验证 企业身份提供者支持联合 API 访问，如下所示：
  - Azure AD 有关更多信息，请参阅 Amazon 大数据博客文章 Federate Amazon Redshift access with Microsoft Azure AD single sign-on。
  - Active Directory 联合身份验证服务 有关更多信息，请参阅 Amazon 大数据博客文章 Federate access to your Amazon Redshift cluster with Active Directory Federation Services (AD FS): Part 1。
  - Okta。有关更多信息，有关更多信息，请参阅 Amazon 大数据博客文章 Federate Amazon Redshift access with Okta as an identity provider。
  - PingFederate。有关更多信息，请参阅 PingFederate 站点。
  - JumpCloud。有关的更多信息，请参阅 JumpCloud 站点。
- Amazon Redshift 数据类型。

Amazon Redshift Python 连接器实施 Python 数据库 API 规范 2.0。有关更多信息，请参阅 Python 网站上的 PEP 249 – Python 数据库 API 规范 v2.0。

主题

- 安装 Amazon Redshift Python 连接器 (p. 167)
- Amazon Redshift Python 连接器的配置选项 (p. 168)
- 导入 Python 连接器 (p. 177)
- 将 Python 连接器与 NumPy 集成 (p. 177)
- 将 Python 连接器与 pandas 集成 (p. 177)
- 使用身份提供者插件 (p. 177)
- 使用 Amazon Redshift Python 连接器的示例 (p. 179)
- Amazon Redshift Python 连接器的 API 参考 (p. 181)

安装 Amazon Redshift Python 连接器

您可以使用以下任意一种方法安装 Amazon Redshift Python 连接器：

- Python 包索引（PyPI）
- Conda

- 克隆 GitHub 存储库

从 PyPI 安装 Python 连接器

要从 Python 包索引（PyPI）安装 Python 连接器，您可以使用 pip。要执行此操作，请运行以下命令。

```
>>> pip install redshift_connector
```

您可以在虚拟环境中安装连接器。要执行此操作，请运行以下命令。

```
>>> pip install redshift_connector
```

或者，你可以用连接器安装 pandas 和 NumPy。

```
>>> pip install "redshift_connector[full]"
```

有关 pip 的更多信息，请参阅 pip 站点。

从 Conda 安装 Python 连接器

你可以从 Anaconda.orgg 安装 Python 连接器。

```
>>>conda install -c conda-forge redshift_connector
```

通过从 Amazon 中克隆 GitHub 存储库来安装 Python 连接器

要从源代码安装 Python 连接器，请从 Amazon 克隆 GitHub 存储库。安装 Python 和 virtualenv 之后，通过运行以下命令来设置环境并安装所需的依赖项。

```
$ 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
```

Amazon Redshift Python 连接器的配置选项

下面，您可以找到您可以为 Amazon Redshift Python 连接器指定的选项的说明。

access_key_id

- 默认值 – 无
- 数据类型 – 字符串

为 IAM 数据库身份验证配置的 IAM 角色或 IAM 用户的访问密钥。

此参数为可选项。

allow_db_user_override

- 默认值 – False
- 数据类型 – Boolean

True

指定连接器使用安全断言标记语言（SAML）断言中的 `DbUser` 值。

False

指定使用 `DbUser` 连接参数中的值。

此参数为可选项。

app_name

- 默认值 – 无
- 数据类型 – 字符串

用于身份验证的身份提供者（IdP）应用程序的名称。

此参数为可选项。

auth_profile

- 默认值 – 无
- 数据类型 – 字符串

连接属性为 JSON 的 Amazon Redshift 身份验证配置文件的名称。有关命名连接参数的更多信息，请参阅 `RedshiftProperty` 类。`RedshiftProperty` 类存储由最终用户提供的连接参数，如果适用，在 IAM 身份验证过程中生成（例如，临时 IAM 凭证）。有关更多信息，请参阅 RedshiftProperty 类。

此参数为可选项。

auto_create

- 默认值 – False
- 数据类型 – Boolean

一个值，指示在用户不存在的情况下是否创建用户。

此参数为可选项。

client_id

- 默认值 – 无
- 数据类型 – 字符串

Azure IdP 中的客户端 ID。

此参数为可选项。

client_secret

- 默认值 – 无
- 数据类型 – 字符串

Azure IdP 中的客户端密钥。

此参数为可选项。

cluster_identifier

- 默认值 – 无
- 数据类型 – 字符串

Amazon Redshift 集群的集群标识符。

此参数为可选项。

credentials_provider

- 默认值 – 无
- 数据类型 – 字符串

对 Amazon Redshift 进行身份验证的 IdP。有效值如下所示：

- `OktaCredentialsProvider`
- `AzureCredentialsProvider`
- `BrowserAzureCredentialsProvider`
- `PingCredentialsProvider`
- `BrowserSamlCredentialsProvider`
- `AdfsCredentialsProvider`

此参数为可选项。

数据库

- 默认值 – 无
- 数据类型 – 字符串

要连接到的数据库的名称。

此参数为可选项。

database_metadata_current_db_only

- 默认值 – True
- 数据类型 – Boolean

一个值，指示应用程序是否支持多数据库数据共享目录。默认值 True 表示应用程序不支持多数据库数据共享目录以实现向后兼容性。

此参数为可选项。

db_groups

- 默认值 – 无

- 数据类型 – 字符串

DbUser 指示的用户为当前会话加入的现有数据库组名称的逗号分隔列表。

此参数为可选项。

db_user

- 默认值 – 无
- 数据类型 – 字符串

用于 Amazon Redshift 的用户 ID。

此参数为可选项。

endpoint_url

- 默认值 – 无
- 数据类型 – 字符串

Amazon Redshift 端点 URL。此选项仅供 Amazon 内部使用。

此参数为必需参数。

group_federation

- 默认值 – False
- 数据类型 – Boolean

此选项指定是否使用 Amazon Redshift IDP 组。

此参数为可选项。

true

使用 Amazon Redshift 身份提供者（IDP）组。

false

使用 STS API 和 GetClusterCredentials 进行用户联合身份验证，并指定用于连接的 db_groups。

host

- 默认值 – 无
- 数据类型 – 字符串

Amazon Redshift 集群的主机名。

此参数为可选项。

iam

- 默认值 – False
- 数据类型 – Boolean

IAM 身份验证已启用。

此参数为必需参数。

iam_disable_cache

- 默认值 – False
- 数据类型 – Boolean

此选项指定是否缓存 IAM 凭证。IAM 凭证将默认被缓存。当对 API 网关的请求受到限制时，这样可以提高性能。

此参数为可选项。

idpPort

- 默认值 – 7890
- 数据类型 – 整数

IdP 将 SAML 断言发送到的侦听端口。

此参数为必需参数。

idp_response_timeout

- 默认值 – 120
- 数据类型 – 整数

从 IdP 检索 SAML 断言的超时时间。

此参数为必需参数。

idp_tenant

- 默认值 – 无
- 数据类型 – 字符串

IdP 租户。

此参数为可选项。

listen_port

- 默认值 – 7890
- 数据类型 – 整数

IdP 将 SAML 断言发送到的侦听端口。

此参数为可选项。

login_url

- 默认值 – 无
- 数据类型 – 字符串

IdP 的单点登录 Url。

此参数为可选项。

max_prepared_statements

- 默认值：1000
- 数据类型 – 整数

可以同时打开的最大预处理语句数。

此参数为必需参数。

numeric_to_float

- 默认值 – False
- 数据类型 – Boolean

此选项指定连接器是否将数字数据类型值从 decimal.Decimal 转换为浮点数。默认情况下，连接器将数字数据类型值作为 decimal.Decimal 接收，而不会转换它们。

我们不建议为需要精确度的用例启用 numeric_to_float（数字转浮点），因为结果可能会四舍五入。

有关 decimal.Decimal 以及它与浮点数之间的权衡的更多信息，请参阅 Python 网站上的 decimal — 十进制定点和浮点算术。

此参数为可选项。

partner_sp_id

- 默认值 – 无
- 数据类型 – 字符串

用于 Ping 身份验证的合作伙伴 SP ID。

此参数为可选项。

password

- 默认值 – 无
- 数据类型 – 字符串

用于身份验证的密码。

此参数为可选项。

port

- 原定设置值 – 5439
- 数据类型 – 整数

Amazon Redshift 集群的端口号。

此参数为必需参数。

preferred_role

- 默认值 – 无
- 数据类型 – 字符串

当前连接首选的 IAM 角色。

此参数为可选项。

principal_arn

- 默认值 – 无
- 数据类型 – 字符串

要为其生成策略的 IAM 用户或角色的 Amazon Resource Name（ARN）。

此参数为可选项。

profile

- 默认值 – 无
- 数据类型 – 字符串

包含 Amazon 凭据的 Amazon 凭据文件中的配置文件的名称。

此参数为可选项。

provider_name

- 默认值 – 无
- 数据类型 – 字符串

Redshift 本机验证提供程序的名称。

此参数为可选项。

region

- 默认值 – 无
- 数据类型 – 字符串

集群所在的 Amazon Web Services 区域。

此参数为可选项。

role_arn

- 默认值 – 无
- 数据类型 – 字符串

调用方承担的角色的 Amazon Resource Name（ARN）。此参数由 `JwtCredentialsProvider` 指示的提供程序使用。

对于 `JwtCredentialsProvider` 提供商，此参数为必填项。否则，此参数位可选项。

role_session_name

- 默认值 – jwt_redshift_session
- 数据类型 – 字符串

所代入角色会话的标识符。通常，您可以传递与使用您的应用程序的用户关联的名称或标识符。您的应用程序使用的临时安全凭证与该用户相关联。此参数由 `JwtCredentialsProvider` 指示的提供程序使用。

此参数为可选项。

scope

- 默认值 – 无
- 数据类型 – 字符串

用户可以同意的范围列表，以空格分隔。您可以指定此参数，以便应用程序可以获得您想调用的 API 的同意。在为 Plugin_Name 选项指定 BrowserAzureOAuth2CredentialsProvider 时，您可以指定此参数。

此参数是 BrowserAzureOAuth2CredentialsProvider 插件必需的。

secret_access_key_id

- 默认值 – 无
- 数据类型 – 字符串

为 IAM 数据库身份验证配置的 IAM 角色或用户的秘密访问密钥。

此参数为可选项。

session_token

- 默认值 – 无
- 数据类型 – 字符串

为 IAM 数据库身份验证配置的 IAM 角色或用户的访问密钥 ID。如果使用临时 Amazon 凭证，则需要此参数。

此参数为可选项。

serverless_acct_id

- 默认值 – 无
- 数据类型 – 字符串

Amazon Redshift Serverless 账户 ID。

此参数为可选项。

serverless_work_group

- 默认值 – 无
- 数据类型 – 字符串

Amazon Redshift Serverless 工作组名称。

此参数为可选项。

ssl

- 默认值 – True
- 数据类型 – Boolean

已启用安全套接字层（SSL）

此参数为必需参数。

ssl_insecure

- 默认值 – True
- 数据类型 – Boolean

一个值，指定是否验证 IdP 主机服务器证书。

此参数为可选项。

sslmode

- 默认值 – verify-ca
- 数据类型 – 字符串

与 Amazon Redshift 的连接的安全性。您可以指定以下任一值：

- verify-ca
- verify-full

此参数为必需参数。

timeout

- 默认值 – 无
- 数据类型 – 整数

连接服务器时发生超时前等待的秒数。

此参数为可选项。

user

- 默认值 – 无
- 数据类型 – 字符串

用于身份验证的用户名。

此参数为可选项。

web_identity_token

- 默认值 – 无
- 数据类型 – 字符串

身份提供者提供的 OAuth 2.0 访问令牌或 OpenID Connect ID 令牌。通过使用 Web 身份提供者对使用您的应用程序的用户进行身份验证，确保您的应用程序获取此令牌。`JwtCredentialsProvider` 指示的提供商使用此参数。

对于 `JwtCredentialsProvider` 提供商，此参数为必填项。否则，此参数位可选项。

导入 Python 连接器

要导入 Python 连接器，请运行以下命令。

```
>>> import redshift_connector
```

导入 NumPy 并连接到 Amazon Redshift

要导入 Amazon Redshift Python 连接器和 Numerical Python（NumPy），请运行以下命令。

```
import redshift_connector
import numpy
```

要使用 Amazon 凭证连接到 Amazon Redshift 集群，请运行以下命令。

```
conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
 )
```

将 Python 连接器与 NumPy 集成

以下是将 Python 连接器与 NumPy 集成的示例。

```
>>>  import numpy
cursor.execute("select * from book")

result: numpy.ndarray = cursor.fetch_numpy_array()
print(result)
```

以下是结果。

```
[['One Hundred Years of Solitude' 'Gabriel García Márquez']
['A Brief History of Time' 'Stephen Hawking']]
```

将 Python 连接器与 pandas 集成

以下是将 Python 连接器与 pandas 集成的示例。

```
>>>  import pandas

cursor.execute("select * from book")
result: pandas.DataFrame = cursor.fetch_dataframe()
print(result)
```

使用身份提供者插件

有关如何使用身份提供者插件的一般信息，请参阅用于提供 IAM 凭证的选项 (p. 401)。

使用 ADFS 身份提供者插件进行身份验证

以下是使用 Active Directory 联合身份验证服务（ADFS）身份提供者插件对连接到 Amazon Redshift 数据库的用户进行身份验证的示例。

```
>>> 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'
)
```

使用 Azure 身份提供者插件进行身份验证

以下是使用 Azure 身份提供者插件进行身份验证的示例。您可以为 `client_id` 和 `client_secret` 创建值用于 Azure 企业应用程序，如下所示。

```
>>>  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'
)
```

使用 Azure 浏览器身份提供者插件进行身份验证

以下是使用 Azure 浏览器身份提供者插件对连接到 Amazon Redshift 数据库的用户进行身份验证的示例。

浏览器中会发生多重验证，其中用户名和密码由用户提供。

```
>>>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',
)
```

使用 Okta 身份提供者插件进行身份验证

以下是使用 Okta 身份提供者插件进行身份验证的示例。你可以通过 Okta 应用程序获取 `idp_host`、`app_id` 和 `app_name` 的值。

```
>>> 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'
)
```

使用 JumpCloud 和通用 SAML 浏览器身份提供者插件进行身份验证

以下是使用 JumpCloud 和通用 SAML 浏览器身份提供者插件进行身份验证的示例。

密码参数是必需的。但是，您不必输入此参数，因为浏览器中会发生多重验证。

```
>>> 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'
)
```

使用 Amazon Redshift Python 连接器的示例

以下为如何使用 Amazon Redshift Python 连接器的示例。要运行它们，您必须先安装 Python 连接器。有关安装 Amazon Redshift Python 连接器的更多信息，请参阅安装 Amazon Redshift Python 连接器 (p. 167)。

主题

- 使用 Amazon 凭证连接到 Amazon Redshift 集群并进行查询 (p. 179)
- 启用自动提交 (p. 180)
- 使用 COPY 从 Amazon S3 桶中复制数据，然后使用 UNLOAD 将数据写入该桶 (p. 180)

使用 Amazon 凭证连接到 Amazon Redshift 集群并进行查询

下面的示例将指导您使用 Amazon 凭证连接到 Amazon Redshift 集群，然后查询表并检索查询结果。

```
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
     host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
     database='dev',
     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'])
```

启用自动提交

根据 Python 数据库 API 规范，默认情况下自动提交属性处于关闭状态。在执行回滚命令后，您可以使用以下命令打开连接的 autocommit 属性，以确保事务不在进行中。

```
#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
```

使用 COPY 从 Amazon S3 桶中复制数据，然后使用 UNLOAD 将数据写入该桶

以下示例说明如何将数据从 Amazon S3 桶复制到表中，然后从该表卸载回到此桶中。

包含以下数据的名为 `category_csv.txt` 的文本文件将上载到 Amazon S3 桶中。

```
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"
```

以下是 Python 代码的示例，该代码首先连接到 Amazon Redshift 数据库。然后创建一个名为 `category` 的表并将 S3 桶中的 CSV 数据复制到表中。

```
#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'])
```

数据卸载到 S3 桶的 `unloaded_category_csv.text0000_part00` 文件中，内容如下：

```
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"
```

Amazon Redshift Python 连接器的 API 参考

您可以在文中找到有关 Amazon Redshift Python 连接器 API 操作的说明。

redshift_connector

在下文中，您可以找到有关 `redshift_connector` API 操作的描述。

`connect(user, database, password[, port, …])`

创建到 Amazon Redshift 集群的连接。此函数可验证用户输入，可以选择使用身份提供者插件进行身份验证，然后构造连接对象。

`apilevel`

支持的 DBAPI 级别，目前为“2.0”。

`paramstyle, str(object='') -> str str(bytes_or_buffer[, encoding[, errors]]) -> str`

要在全局使用的数据库 API 参数样式。

连接

您可以在文中找到有关 Amazon Redshift Python 连接器的连接 API 操作的说明。

`__init__(user, password, database[, host, …])`

初始化原始连接对象。

`cursor`

创建绑定到此连接的游标对象。

`commit`

提交当前数据库事务。

`rollback`

回滚当前的数据库事务。

`close`

关闭数据库连接。

`execute(cursor, operation, vals)`

运行指定的 SQL 命令。您可以将参数作为序列或映射提供，具体取决于 `redshift_connector.paramstyle` 的值。

`run(sql[, stream])`

运行指定的 SQL 命令。或者，您也可以提供与 COPY 命令一起使用的流。

`xid(format_id, global_transaction_id, …)`

创建事务 ID。postgres 中只使用了 `global_transaction_id` 参数。postgres 中不使用 format_id 和 branch_qualifier。`global_transaction_id` 可以是 postgres 支持的任何返回元组的字符串标识符（`format_id`、`global_transaction_id`、`branch_qualifier`）。

`tpc_begin(xid)`

使用由格式 ID、全局事务 ID 和分支限定符组成的事务 ID `xid` 开始 TPC 事务。

`tpc_prepare`

执行以 .tpc_begin 开始的事务的第一阶段。

`tpc_commit([xid])`

在没有参数的情况下进行调用时，.tpc_commit 会提交之前使用 .tpc_prepare() 准备的 TPC 事务。

`tpc_rollback([xid])`

在没有参数的情况下进行调用时，.tpc_rollback 会回滚 TPC 事务。

`tpc_recover`

返回适合与 .tpc_commit(xid) 或 .tpc_rollback(xid) 一起使用的待处理事务 ID 列表。

Cursor

在下文中，您可以找到有关 游标 API 操作的描述。

`__init__(connection[, paramstyle])`

初始化原始游标对象。

```
insert_bulk_data(filename, table_name, parameter_indices, column_names,
delimiter, batch_size)
```

运行批量 INSERT 语句。

`execute(operation[, args, stream, …])`

运行数据库操作。

`executemany(operation, param_sets)`

准备数据库操作，然后为提供的所有参数序列或映射运行该操作。

`fetchone`

获取查询结果集的下一行。

`fetchmany([num])`

获取查询结果的下一个行集。

`fetchall`

获取查询结果的所有剩余行。

`close`

立即关闭光标。

`__iter__`

可以迭代游标对象以从查询中检索行。

`fetch_dataframe([num])`

返回最后查询结果的数据框。

`write_dataframe(df, table)`

将相同的结构数据框写入 Amazon Redshift 数据库。

`fetch_numpy_array([num])`

返回最后查询结果的 NumPy 数组。

`get_catalogs`

Amazon Redshift 不支持来自单个连接的多个目录。Amazon Redshift 只返回当前目录。

`get_tables([catalog, schema_pattern, …])`

返回系统中用户定义的唯一公共表。

`get_columns([catalog, schema_pattern, …])`

返回 Amazon Redshift 数据库中特定表中所有列的列表。

AdfsCredentialsProvider 插件

以下是 Amazon Redshift Python 连接器的 AdfsCredentialsProvider 插件 API 操作的语法。

```
redshift_connector.plugin.AdfsCredentialsProvider()
```

AzureCredentialsProvider 插件

以下是 Amazon Redshift Python 连接器的 AzureCredentialsProvider 插件 API 操作的语法。

```
redshift_connector.plugin.AzureCredentialsProvider()
```

BrowserAzureCredentialsProvider 插件

以下是 Amazon Redshift Python 连接器的 BrowserAzureCredentialsProvider 插件 API 操作的语法。

```
redshift_connector.plugin.BrowserAzureCredentialsProvider()
```

BrowserSamlCredentialsProvider 插件

以下是 Amazon Redshift Python 连接器的 BrowserSamlCredentialsProvider 插件 API 操作的语法。

```
redshift_connector.plugin.BrowserSamlCredentialsProvider()
```

OktaCredentialsProvider 插件

以下是 Amazon Redshift Python 连接器的 OktaCredentialsProvider 插件 API 操作的语法。

```
redshift_connector.plugin.OktaCredentialsProvider()
```

PingCredentialsProvider 插件

以下是 Amazon Redshift Python 连接器的 PingCredentialsProvider 插件 API 操作的语法。

```
redshift_connector.plugin.PingCredentialsProvider()
```

SamlCredentialsProvider 插件

以下是 Amazon Redshift Python 连接器的 SamlCredentialsProvider 插件 API 操作的语法。

```
redshift_connector.plugin.SamlCredentialsProvider()
```

为 Amazon Redshift 配置 ODBC 驱动程序版本 2.x 连接

您可以使用 ODBC 连接将许多第三方 SQL 客户端工具和应用程序连接到您的 Amazon Redshift 集群。如果您的客户端工具支持 JDBC，您可以选择使用 JDBC 类型的连接，而非 ODBC 连接，因为 JDBC 连接更加易于配置。但是，如果您的客户端工具不支持 JDBC，您可以按照本节中的步骤在您的客户端计算机或 Amazon EC2 实例上设置 ODBC 连接。

Amazon Redshift 提供了适用于 Linux 和 Windows 操作系统的 64 位 ODBC 驱动程序；32 位 ODBC 驱动程序已停用。目前不支持 macOS X。除了紧急安全补丁外，不会发布针对 32 位 ODBC 驱动程序的进一步更新。要下载并安装适用于 macOS X 和 32 位操作系统的 ODBC 驱动程序，请参阅配置 ODBC 连接。

有关 ODBC 驱动程序更改的最新信息，请参阅更改日志。

主题

- 获取 ODBC URL (p. 184)
- 在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 185)
- 在 Linux 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 187)
- 配置身份验证 (p. 189)
- 转换数据类型 (p. 194)
- 配置 ODBC 驱动程序选项 (p. 195)

获取 ODBC URL

Amazon Redshift 在 Amazon Redshift 控制台中显示您的集群的 ODBC URL。此 URL 包含在您的客户端计算机与数据库之间建立连接所需的信息。

ODBC URL 采用以下格式：

```
Driver={driver}; Server=endpoint_host; Database=database_name; UID=user_name; PWD=password;
 Port=port_number
```

上述格式的字段具有以下值：

ODBC URL 字段值

字段	值
Driver	要使用的 64 位 ODBC 驱动程序的名称：Amazon Redshift ODBC Driver (x64)（Amazon Redshift ODBC 驱动程序 (x64)）
Server	Amazon Redshift 集群的端点主机。
Database	您为集群创建的数据库。

字段	值
UID	有权连接到数据库的用户账户的用户名。虽然此值是数据库级权限，而非集群级权限，但您可以使用您在启动集群时设置的管理员用户账户。
PWD	用户账户用于连接数据库的密码。
Port	您在启动集群时指定的端口号。如果您启用了防火墙，请确保此端口处于打开状态，可供您使用。

以下是一个示例 ODBC URL：

```
Driver={Amazon Redshift ODBC Driver (x64)}; Server=examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com; Database=dev; UID=adminuser;
 PWD=insert_your_admin_user_password_here; Port=5439
```

有关在何处查找 ODBC URL 的信息，请参阅 Finding your cluster connection string（查找集群连接字符串）。

在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序

系统要求

您必须在可访问 Amazon Redshift 数据仓库的客户端计算机上安装 Amazon Redshift ODBC 驱动程序。对于您要在其上安装该驱动程序的每台计算机，有以下最低要求：

- 计算机上的管理员权限。
- 计算机满足以下系统要求：
  - 以下操作系统之一：
    - Windows 10 或 8.1。
    - Windows Server 2019、2016 或 2012。
  - 100MB 可用磁盘空间。
  - 已安装适用于 64 位 Windows 的 Visual C++ Redistributable for Visual Studio 2015。您可以在 Microsoft 网站上的 Download Visual C++ Redistributable for Visual Studio 2015（下载 Visual C++ Redistributable for Visual Studio 2015）下载安装包。

安装 Amazon Redshift ODBC 驱动程序

使用以下过程下载并安装适用于 Windows 操作系统的 Amazon Redshift ODBC 驱动程序。仅在您当前运行的第三方应用程序获得了使用 Amazon Redshift 的认证并且需要不同驱动程序时，才能使用该特定驱动程序。

要下载并安装 ODBC 驱动程序，请执行以下操作：

1. 下载以下驱动程序：64 位 ODBC 驱动程序版本 2.0.0.1 在中国（北京）区域，请使用以下链接：64 位 ODBC 驱动程序版本 2.0.0.1

   此驱动程序的名称为 Amazon Redshift ODBC Driver (x64)（Amazon Redshift ODBC 驱动程序 (x64)）。

   Note

   32 位 ODBC 驱动程序已停用。除了紧急安全补丁外，不会发布进一步的更新。要下载并安装适用于 32 位操作系统的 ODBC 驱动程序，请参阅在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序。

2. 审核 Amazon Redshift ODBC 驱动程序版本 2.x 许可证。
3. 双击 .msi 文件，然后按照向导中的步骤安装驱动程序。

为 ODBC 连接创建系统 DSN 条目

下载并安装 ODBC 驱动程序后，将数据源名称 (DSN) 条目添加到客户端计算机或 Amazon EC2 实例。SQL 客户端工具可以使用此数据源连接到 Amazon Redshift 数据库。

建议您创建系统 DSN 而不是用户 DSN。有些应用程序使用不同的用户账户加载数据，因而可能无法检测在其他用户账户下创建的用户 DSN。

> Note
>
> 对于使用 Amazon Identity and Access Management (IAM) 凭证或身份提供者 (IdP) 凭证进行的身份验证，需要执行其他步骤。有关更多信息，请参阅配置 JDBC 或 ODBC 连接以使用 IAM 凭证。

要为 ODBC 连接创建系统 DSN 条目，请执行以下操作：

1. 在 Start（开始）菜单上，键入 ODBC Data Sources（ODBC 数据源）。选择 ODBC Data Sources（ODBC 数据源）。

   请确保您选择的 ODBC Data Source Administrator 的位数与用于连接 Amazon Redshift 的客户端应用程序的位数相同。
2. 在 ODBC Data Source Administrator（ODBC 数据源管理器）中，选择 Driver（驱动程序）选项卡，然后找到以下驱动程序文件夹：Amazon Redshift ODBC Driver (x64)（Amazon Redshift ODBC 驱动程序 (x64)）。
3. 选择 System DSN (系统 DSN) 选项卡为计算机上的所有用户配置驱动程序，或选择 User DSN (用户 DSN) 选项卡仅为您的用户账户配置驱动程序。
4. 选择 Add (添加)。系统随即打开 Create New Data Source 窗口。
5. 选择 Amazon Redshift ODBC driver (x64)（Amazon Redshift ODBC 驱动程序 (x64)），然后选择 Finish（完成）。系统随即打开 Amazon Redshift ODBC Driver DSN Setup 窗口。
6. 在 Connection Settings（连接设置）部分下，输入以下信息：

   Data source name

   输入数据源的名称。例如，如果您遵循的是《Amazon Redshift 入门指南》，则可键入 `exampleclusterdsn`，以便轻松记住将与此 DSN 关联的集群。

   服务器

   为您的 Amazon Redshift 集群指定端点主机。您可以在 Amazon Redshift 控制台中的集群详细信息页面上找到该信息。有关更多信息，请参阅 Configuring connections in Amazon Redshift（在 Amazon Redshift 中配置连接）。

   端口

   输入数据库使用的端口号。默认情况下，Amazon Redshift 将使用 5439，但您应使用在集群启动时配置使用的端口。

   数据库。

   输入 Amazon Redshift 数据库的名称。如果您在未指定数据库名称的情况下启动了集群，请输入 `dev`。否则，请使用您在启动过程中选择的名称。如果您遵循的是《Amazon Redshift 入门指南》，输入 `dev`。
7. 在 Authentication（身份验证）下，指定配置选项以配置标准或 IAM 身份验证。
8. 选择 SSL Options（SSL 选项），然后指定以下项目的值：

   身份验证模式

选择处理安全套接字层 (SSL) 的模式。在测试环境中，可以使用 `prefer`。但是，对于生产环境以及在需要安全交换数据时，请使用 `verify-ca` 或 `verify-full`。

9. 在 Proxy（代理）选项卡中，指定任何代理连接设置。
10. 在 Cursor（游标）选项卡中，指定有关如何将查询结果返回至您的 SQL 客户端工具或应用程序的选项。
11. 在 Advanced Options（高级选项）中，指定日志记录选项和其他选项的值。
12. 选择 Test（测试）。如果客户端计算机可以连接到 Amazon Redshift 数据库，将显示以下消息：Connection successful（连接成功）。如果客户端计算机无法连接到数据库，您可以通过生成日志文件并联系 Amazon 支持部门，对可能的问题进行故障排除。有关生成日志的信息，请参阅 (LINK)。
13. 选择 OK（确定）。

在 Linux 上安装和配置 Amazon Redshift ODBC 驱动程序

系统要求

您必须在可访问 Amazon Redshift 数据仓库的客户端计算机上安装 Amazon Redshift ODBC 驱动程序。对于您要在其上安装该驱动程序的每台计算机，有以下最低要求：

- 计算机上的根访问权限。
- 以下分发之一：
  - Red Hat® Enterprise Linux® (RHEL) 7 或 8
  - CentOS 7 或 8。
- 150MB 可用磁盘空间。
- unixODBC 2.2.14 或更高版本。
- glibc 2.17 或更高版本。

安装 Amazon Redshift ODBC 驱动程序

要下载并安装适用于 Linux 的 Amazon Redshift ODBC 驱动程序版本 2.x，请执行以下操作：

1. 下载以下驱动程序：64 位 RPM 驱动程序版本 2.0.0.1 在中国（北京）区域，请使用以下链接：64 位 ODBC 驱动程序版本 2.0.0.1

   Note

   32 位 ODBC 驱动程序已停用。除了紧急安全补丁外，不会发布进一步的更新。
2. 转至您下载程序包的位置，然后运行以下命令之一。使用适用于您的 Linux 发行版的命令。

   在 RHEL 和 CentOS 操作系统上，运行以下命令：

```
yum --nogpgcheck localinstall RPMFileName
```

   将 `RPMFileName` 替换为 RPM 包文件名。例如，以下命令将演示如何安装 64 位驱动程序：

```
yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-2.x.xx.xxxx.x86_64.rpm
```

使用 ODBC 驱动程序管理器在 Linux 上配置 ODBC 驱动程序

在 Linux 上，您可以使用 ODBC 驱动程序管理器来配置 ODBC 连接设置。ODBC 驱动程序管理器使用配置文件来定义和配置 ODBC 数据源和驱动程序。您可以使用的 ODBC 驱动程序管理器取决于您使用的操作系统。

使用 unixODBC 驱动程序管理器配置 ODBC 驱动程序

要配置 Amazon Redshift ODBC 驱动程序，需要以下文件：

- amazon.redshiftodbc.ini
- odbc.ini
- odbcinst.ini

如果您将驱动程序安装在默认位置，则 amazon.redshiftodbc.ini 配置文件将位于 /opt/amazon/redshiftodbcx64 中。

此外，在 /opt/amazon/redshiftodbcx64 下，您可以找到示例 odbc.ini 和 odbcinst.ini 文件。您可以使用这些文件作为配置 Amazon Redshift ODBC 驱动程序和数据源名称 (DSN) 的示例。

我们不建议使用 Amazon Redshift ODBC 驱动程序安装目录来存储配置文件。安装目录中的示例文件仅用作示例。如果您日后重新安装 Amazon Redshift ODBC 驱动程序，或将其升级到新版本，安装目录会被覆盖。您将丢失对安装目录中的文件所做的所有更改。

为了避免出现这种情况，请将 amazon.redshiftodbc.ini 文件复制到安装目录以外的其他目录中。如果您要将此文件复制到用户的主目录，请在文件名的开头添加一个句点 (.)，使其成为隐藏文件。

对于 odbc.ini 和 odbcinst.ini 文件，应在用户的主目录中使用配置文件，或者在其他目录中创建新版本。默认情况下，您的 Linux 操作系统应在用户的主目录 (/home/$USER 或 ~/.) 中包含 odbc.ini 文件和 odbcinst.ini 文件。这些默认文件均为隐藏文件 (通过在每个文件名的前面添加圆点 (.) 表示) 。这些文件仅当您使用 -a 标志列出目录内容时显示。

对于 odbc.ini 和 odbcinst.ini 文件，不管您选择哪个选项，都需对这些文件进行修改，以添加驱动程序和 DSN 配置信息。如果您创建新文件，则还需设置环境变量，以指定这些配置文件的目标存储位置。

默认情况下，ODBC 驱动程序管理器将配置为使用位于主目录中的 odbc.ini 和 odbcinst.ini 配置文件的隐藏版本 (名为 .odbc.ini 和 .odbcinst.ini) 。它们也被配置为使用驱动程序安装目录中的 amazon.redshiftodbc.ini 文件。如果您将这些配置文件存储在其他位置，请设置如下所述的环境变量，以便驱动程序管理器能够找到这些文件。

如果您使用的是 unixODBC，请执行以下操作：

- 将 ODBCINI 设置到 odbc.ini 文件的完整路径和文件名。
- 将 ODBCSYSINI 设置到包含 odbcinst.ini 文件的目录的完整路径。
- 将 AMAZONREDSHIFTODBCINI 设置到 amazon.redshiftodbc.ini 文件的完整路径和文件名。

以下是设置上述值的示例：

```
export ODBCINI=/usr/local/odbc/odbc.ini
export ODBCSYSINI=/usr/local/odbc
export AMAZONREDSHIFTODBCINI=/etc/amazon.redshiftodbc.ini
```

在 Linux 上使用数据源名称 (DSN) 配置连接

在使用数据源名称 (DSN) 连接到数据存储时，请配置 odbc.ini 文件以定义数据源名称 (DSN)。在 odbc.ini 文件中设置属性以创建指定数据存储的连接信息的 DSN。

在 Linux 操作系统上，使用以下格式：

```
[ODBC Data Sources]
```

```
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file
Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

以下示例显示了在 Linux 操作系统上使用 64 位 ODBC 驱动程序配置 `odbc.ini`。

```
[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
```

在 Linux 上配置没有 DSN 的连接

要通过不带 DSN 的连接来连接到数据存储，请在 `odbcinst.ini` 文件中定义驱动程序。然后，在应用程序中提供一个无 DSN 的连接字符串。

在 Linux 操作系统上，使用以下格式：

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

以下示例显示了在 Linux 操作系统上使用 64 位 ODBC 驱动程序配置 `odbcinst.ini`。

```
[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
```

配置身份验证

为了防止数据遭到未经授权的访问，Amazon Redshift 数据存储要求所有连接都使用用户凭据进行身份验证。

下表说明了可用于连接到 Amazon Redshift ODBC 驱动程序版本 2.x 的每种身份验证方法的必需和可选连接选项：

ODBC 身份验证方法的必需和可选连接选项

身份验证方法	必填	可选
标准	• Host • 端口（默认值为 5439） • 数据库。 • UID • Password	
IAM 配置文件	• Host • 端口（默认值为 5439） • 数据库。 • IAM • Profile	• ClusterID • 区域 • AutoCreate • EndpointURL • StsEndpointURL • InstanceProfile Note 如果没有单独设置 ClusterID 和 Region（区域），则必须在 Host（主机）中设置它们。
IAM 凭证	• Host • 端口（默认值为 5439） • 数据库。 • IAM • AccessKeyID • SecretAccessKey	• ClusterID • 区域 • AutoCreate • EndpointURL • StsEndpointURL • SessionToken • UID Note 如果没有单独设置 ClusterID 和 Region（区域），则必须在 Host（主机）中设置它们。
AD FS	• Host • 端口（默认值为 5439） • 数据库。 • IAM • plugin_name • UID • Password • IdP_Host • IdP_Port	• ClusterID • 区域 • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • loginToRp • SSL_Insecure

身份验证方法	必填	可选
		Note 如果没有单独设置 ClusterID 和 Region（区域），则必须在 Host（主机）中设置它们。
Azure AD	• Host • 端口（默认值为 5439） • 数据库。 • IAM • plugin_name • UID • Password • IdP_Tenant • Client_ID • Client_Secret	• ClusterID • 区域 • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter Note 如果没有单独设置 ClusterID 和 Region（区域），则必须在 Host（主机）中设置它们。
JWT	• Host • 端口（默认值为 5439） • 数据库。 • IAM • plugin_name • web_identity_token	• provider_name
Okta	• Host • 端口（默认值为 5439） • 数据库。 • IAM • plugin_name • UID • Password • IdP_Host • App_Name • App_ID	• ClusterID • 区域 • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role Note 如果没有单独设置 ClusterID 和 Region（区域），则必须在 Host（主机）中设置它们。

身份验证方法	必填	可选
Ping Federate	• Host • 端口（默认值为 5439） • 数据库。 • IAM • plugin_name • UID • Password • IdP_Host • IdP_Port	• ClusterID • 区域 • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • SSL_Insecure • partner_spid Note 如果没有单独设置 ClusterID 和 Region（区域），则必须在 Host（主机）中设置它们。
浏览器 Azure AD	• Host • 端口（默认值为 5439） • 数据库。 • IAM • plugin_name • IdP_Tenant • Client_ID • UID	• ClusterID • 区域 • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter • IdP_Response_Timeout • listen_port Note 如果没有单独设置 ClusterID 和 Region（区域），则必须在 Host（主机）中设置它们。

身份验证方法	必填	可选
浏览器 SAML	• Host • 端口（默认值为 5439） • 数据库。 • IAM • plugin_name • login_url • UID	• ClusterID • 区域 • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter • IdP_Response_Timeout • listen_port **Note** 如果没有单独设置 ClusterID 和 Region（区域），则必须在 Host（主机）中设置它们。
身份验证配置文件	• Host • 端口（默认值为 5439） • 数据库。 • AccessKeyID • SecretAccessKey	
浏览器 Azure AD OAUTH2	• Host • 端口（默认值为 5439） • 数据库。 • IAM • plugin_name • IdP_Tenant • Client_ID • UID	• ClusterID • 区域 • EndpointUrl • IdP_Response_Timeout • listen_port • scope • provider_name **Note** 如果没有单独设置 ClusterID 和 Region（区域），则必须在 Host（主机）中设置它们。

使用外部凭证服务

除了对 AD FS、Azure AD 和 Okta 的内置支持外，Amazon Redshift ODBC 驱动程序的 Windows 版本还提供了对其他凭证服务的支持。该驱动程序可以使用您选择的任何基于 SAML 的凭证提供程序插件对连接进行身份验证。

要在 Windows 上配置外部凭证服务，请执行以下操作：

1. 创建一个 IAM 配置文件，根据需要指定凭证提供程序插件和其他身份验证参数。配置文件必须采用 ASCII 编码，并且必须包含以下键值对，其中 `PluginPath` 是插件应用程序的完整路径：

```
plugin_name = PluginPath
```

例如：

```
plugin_name = C:\Users\kjson\myapp\CredServiceApp.exe
```

有关如何创建配置文件的信息，请参阅《Amazon Redshift 集群管理指南》中的 Using a Configuration Profile（使用配置文件）。
2. 将驱动程序配置为使用此配置文件。驱动程序将检测并使用配置文件中指定的身份验证设置。

转换数据类型

Amazon Redshift ODBC 驱动程序版本 2.x 支持许多常见的数据格式，从而可在 Amazon Redshift 和 SQL 数据类型之间进行转换。

下表列出了支持的数据类型映射。

Amazon Redshift 类型	SQL 类型
BIGINT	SQL_BIGINT
BOOLEAN	SQL_BIT
CHAR	SQL_CHAR
DATE	SQL_TYPE_DATE
DECIMAL	SQL_NUMERIC
DOUBLE PRECISION	SQL_DOUBLE
GEOGRAPHY	SQL_ LONGVARBINARY
GEOMETRY	SQL_ LONGVARBINARY
INTEGER	SQL_INTEGER
REAL	SQL_REAL
SMALLINT	SQL_SMALLINT
SUPER	SQL_LONGVARCHAR
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

配置 ODBC 驱动程序选项

可以使用驱动程序配置选项来控制 Amazon Redshift ODBC 驱动程序的行为。驱动程序选项不区分大小写。

在 Microsoft Windows 中，您通常可以在配置数据源名称 (DSN) 时设置驱动程序选项。您还能在以编程方式连接时，或者通过在 `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\your_DSN` 中添加或更改注册表项来设置驱动程序选项。有关配置 DSN 的更多信息，请参阅在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 208)。

在 Linux 中，您可以在 `odbc.ini` 和 `amazon.redshiftodbc.ini` 文件中设置驱动程序配置选项，如 使用 ODBC 驱动程序管理器在 Linux 和 macOS X 操作系统上配置驱动程序 (p. 212) 中所述。在 `amazon.redshiftodbc.ini` 文件中设置的配置选项适用于所有连接。相反，`odbc.ini` 文件中的设置配置选项特定于一个连接。在 `odbc.ini` 中设置的配置选项优先于在 `amazon.redshiftodbc.ini` 中设置的配置选项。

以下是您可以为 Amazon Redshift ODBC 版本 2.x 驱动程序指定的选项的说明：

AccessKeyID

- 默认值 – 无
- 数据类型 – 字符串

用户或角色的 IAM 访问密钥。如果您设置此参数，则还必须指定 SecretAccessKey。

此参数为可选项。

app_id

- 默认值 – 无
- 数据类型 – 字符串

Okta 提供的与您的 Amazon Redshift 应用程序关联的唯一 ID。

此参数为可选项。

app_name

- 默认值 – 无
- 数据类型 – 字符串

您用于验证与 Amazon Redshift 的连接的 Okta 应用程序的名称。

此参数为可选项。

AuthProfile

- 默认值 – 无
- 数据类型 – 字符串

用于管理连接设置的身份验证配置文件。如果您设置此参数，则还必须设置 AccessKeyID 和 SecretAccessKey。

此参数为可选项。

AuthType

- Default Value（默认值）：Standard（标准）

- 数据类型 – 字符串

此选项指定在您使用 Amazon Redshift ODBC Driver DSN Setup（Amazon Redshift ODBC 驱动程序 DSN 设置）对话框配置 DSN 时驱动程序使用的身份验证模式：

- Standard（标准）：使用您的 Amazon Redshift 用户名和密码的标准身份验证。
- Amazon Profile（Amazon 配置文件）：使用配置文件的 IAM 身份验证。
- Amazon IAM Credentials（Amazon IAM 凭证）：使用 IAM 凭证的 IAM 身份验证。
- Identity Provider: AD FS（身份提供程序：AD FS）：使用 Active Directory 联合身份验证服务 (AD FS) 的 IAM 身份验证。
- Identity Provider: Azure AD（身份提供程序：Azure AD）：使用 Azure AD 门户的 IAM 身份验证。
- Identity Provider: JWT（身份提供程序：JWT）：使用 JSON Web 令牌 (JWT) 的 IAM 身份验证。
- Identity Provider: Okta（身份提供程序：Okta）：使用 Okta 的 IAM 身份验证。
- Identity Provider: PingFederate（身份提供程序：PingFederate）：使用 PingFederate 的 IAM 身份验证。

仅当您使用 Windows 驱动程序中的“Amazon Redshift ODBC Driver DSN Setup”（Amazon Redshift ODBC 驱动程序 DSN 设置）对话框配置 DSN 时，此选项才可用。当您使用连接字符串或非 Windows 计算机配置连接时，驱动程序将根据您指定的凭证，自动确定是使用 Standard（标准）、Amazon Profile（Amazon 配置文件）还是 Amazon IAM Credentials（Amazon IAM 凭证）身份验证。要使用身份提供程序，您必须设置 plugin_name 属性。

此参数为必需参数。

AutoCreate

- 默认值：0
- 数据类型 – Boolean

一个布尔值，用于指定当指定的用户不存在时驱动程序是否创建新用户。

- 1 | TRUE：如果通过 UID 指定的用户不存在，则驱动程序将创建新用户。
- 0 | FALSE：驱动程序不会创建新用户。如果指定的用户不存在，则身份验证将失败。

此参数为可选项。

CaFile

- 默认值 – 无
- 数据类型 – 字符串

用于某些形式的 IAM 身份验证的 CA 证书文件的文件路径。

此参数仅在 Linux 上可用。

此参数为可选项。

client_id

- 默认值 – 无
- 数据类型 – 字符串

与 Azure AD 中的 Amazon Redshift 应用程序关联的客户端 ID。

如果通过 Azure AD 服务进行身份验证，则此参数是必需的。

client_ secret

- 默认值 – 无
- 数据类型 – 字符串

与 Azure AD 中的 Amazon Redshift 应用程序关联的秘密密钥。

如果通过 Azure AD 服务进行身份验证，则此参数是必需的。

ClusterId

- 默认值 – 无
- 数据类型 – 字符串

您要连接到的 Amazon Redshift 集群的名称。它将在 IAM 身份验证中使用。集群 ID 不会在 Server（服务器）参数中指定。

此参数为可选项。

数据库。

- 默认值 – 无
- 数据类型 – 字符串

您要访问的 Amazon Redshift 数据库的名称。

此参数为必需参数。

DatabaseMetadataCurrentDbOnly

- Default Value（默认值）：1
- 数据类型 – Boolean

一个布尔值，用于指定驱动程序是否从多个数据库和集群返回元数据。

- 1 | TRUE：驱动程序仅从当前数据库返回元数据。
- 0 | FALSE。驱动程序将跨多个 Amazon Redshift 数据库和集群返回元数据。

此参数为可选项。

dbgroups_filter

- 默认值 – 无
- 数据类型 – 字符串

在使用 Azure、浏览器 Azure 和浏览器 SAML 身份验证类型时，您可以指定的正则表达式，用于筛选出从 Amazon Redshift 的 SAML 响应中收到的数据库组 (DbGroup)。

此参数为可选项。

驱动程序

- Default Value（默认值）：Amazon Redshift ODBC Driver (x64)（Amazon Redshift ODBC 驱动程序 (x64)）
- 数据类型 – 字符串

驱动程序的名称。唯一受支持的值是 Amazon Redshift ODBC Driver (x64)（Amazon Redshift ODBC 驱动程序 (x64)）。

如果您未设置 DSN，则此参数是必需的。

DSN

- 默认值 – 无
- 数据类型 – 字符串

驱动程序数据源名称的名称。应用程序将在 SQLDriverConnect API 中指定 DSN。

如果您未设置 Driver（驱动程序），则此参数是必需的。

EndpointUrl

- 默认值 – 无
- 数据类型 – 字符串

用于与 Amazon Redshift Coral 服务通信以进行 IAM 身份验证的覆盖端点。

此参数为可选项。

ForceLlowcase

- 默认值：0
- 数据类型 – Boolean

一个布尔值，用于指定在使用单点登录身份验证时，驱动程序是否会将从身份提供者发送到 Amazon Redshift 的所有数据库组 (DbGroup) 小写。

- 1 | TRUE：驱动程序会将从身份提供程序发送的所有数据库组 (DbGroup) 小写。
- 0 | FALSE：驱动程序不会更改数据库组 (DbGroup)。

此参数为可选项。

https_proxy_host

- 默认值 – 无
- 数据类型 – 字符串

您要通过其来传递 IAM 身份验证过程的代理服务器的主机名或 IP 地址。

此参数为可选项。

https_proxy_password

- 默认值 – 无

- 数据类型 – 字符串

用于访问代理服务器的密码。它将用于 IAM 身份验证。

此参数为可选项。

https_proxy_port

- 默认值 – 无
- 数据类型 – 整数

代理服务器用于侦听客户端连接的端口号。它将用于 IAM 身份验证。

此参数为可选项。

https_proxy_username

- 默认值 – 无
- 数据类型 – 字符串

用于访问代理服务器的用户名。它将用于 IAM 身份验证。

此参数为可选项。

IAM

- 默认值：0
- 数据类型 – Boolean

一个布尔值，用于指定驱动程序是否使用 IAM 身份验证方法对连接进行身份验证。

- 1 | TRUE：驱动程序将使用某种 IAM 身份验证方法（使用访问密钥和秘密密钥对、配置文件或凭证服务）。
- 0 | FALSE。驱动程序将使用标准身份验证（使用您的数据库用户名和密码）。

此参数为可选项。

idp_host

- 默认值 – 无
- 数据类型 – 字符串

您用于对 Amazon Redshift 进行身份验证的 IdP（身份提供者）主机。

此参数为可选项。

idp_port

- 默认值 – 无
- 数据类型 – 整数

您用于对 Amazon Redshift 进行身份验证的 IdP（身份提供程序）的端口。默认端口为 5439。

此参数为可选项。

idp_response_timeout

- 默认值 – 120
- 数据类型 – 整数

当通过浏览器插件使用 SAML 或 Azure AD 服务时，驱动程序等待身份提供程序发出 SAML 响应的秒数。

此参数为可选项。

idp_tenant

- 默认值 – 无
- 数据类型 – 字符串

与您的 Amazon Redshift 应用程序关联的 Azure AD 租户 ID。

如果通过 Azure AD 服务进行身份验证，则此参数是必需的。

idp_use_https_proxy

- 默认值：0
- 数据类型 – Boolean

一个布尔值，用于指定驱动程序是否通过代理服务器传递身份提供程序 (IdP) 的身份验证过程。

- 1 | TRUE：驱动程序将通过代理服务器传递 IdP 身份验证过程。
- 0 | FALSE。驱动程序不会通过代理服务器传递 IdP 身份验证过程。

此参数为可选项。

InstanceProfile

- 默认值：0
- 数据类型 – Boolean

一个布尔值，用于指定驱动程序在配置为使用配置文件进行身份验证时是否使用 Amazon EC2 实例配置文件。

- 1 | TRUE：驱动程序将使用 Amazon EC2 实例配置文件。
- 0 | FALSE。驱动程序将改用通过 Profile Name（配置文件名称）选项（Profile（配置文件））指定的串联角色配置文件。

此参数为可选项。

KeepAlive

- Default Value（默认值）：1
- 数据类型 – Boolean

一个布尔值，用于指定驱动程序是否使用 TCP keepalive 来防止连接超时。

- 1 | TRUE：驱动程序将使用 TCP keepalive 来防止连接超时。
- 0 | FALSE。驱动程序不会使用 TCP keepalive。

此参数为可选项。

KeepAliveCount

- 默认值：0
- 数据类型 – 整数

连接被视为断开前可能丢失的 TCP keepalive 包的数量。当此参数设置为 0 时，驱动程序将使用此设置的系统默认值。

此参数为可选项。

KeepAliveInterval

- 默认值：0
- 数据类型 – 整数

两次传输 TCP keepalive 间隔的秒数。当此参数设置为 0 时，驱动程序将使用此设置的系统默认值。

此参数为可选项。

KeepAliveTime

- 默认值：0
- 数据类型 – 整数

驱动程序发送 TCP Keepalive 包前处于不活动状态的秒数。当此参数设置为 0 时，驱动程序将使用此设置的系统默认值。

此参数为可选项。

listen_port

- Default Value（默认值）：7890
- 数据类型 – 整数

通过浏览器插件使用 SAML 或 Azure AD 服务时，驱动程序用于接收来自身份提供程序的 SAML 响应的端口。

此参数为可选项。

login_url

- 默认值 – 无
- 数据类型 – 字符串

在使用通用浏览器 SAML 插件时，身份提供程序网站上的资源的 URL。

如果通过浏览器插件使用 SAML 或 Azure AD 服务进行身份验证，则此参数是必需的。

loginToRp

- Default Value（默认值）：urn:amazon:webservices
- 数据类型 – 字符串

要用于 AD FS 身份验证类型的信赖方信任。

此字符串为可选项。

LogLevel

- 默认值：0
- 数据类型 – 整数

使用此属性可以启用或禁用驱动程序中的日志记录，并指定包含在日志中的详细信息量。我们建议您启用日志记录的时长仅足以捕获问题即可，因为日志记录会降低性能，并会占用大量磁盘空间。

将该属性设置为以下值之一：

- 0：OFF（关闭）。禁用所有日志记录。
- 1：ERROR（错误）。记录也许不会导致驱动程序中止运行但会生成错误的错误事件。
- 2：API_CALL。记录带有函数参数值的 ODBC API 函数调用。
- 3：INFO（信息）。记录描述驱动程序进度的一般信息。
- 4：MSG_PROTOCOL。记录驱动程序消息协议的详细信息。
- 5：DEBUG（调试）。记录所有驱动程序活动
- 6：DEBUG_APPEND。保留所有驱动程序活动的附加日志。

启用日志记录后，驱动程序将在您在 LogPath 属性中指定的位置生成以下日志文件：

- 一个 `redshift_odbc.log.1` 文件，它将记录连接握手期间发生的驱动程序活动。
- 一个 `redshift_odbc.log` 文件，用于与数据库建立连接后的所有驱动程序活动。

此参数为可选项。

LogPath

- Default Value（默认值）：特定于操作系统的 TEMP 目录
- 数据类型 – 字符串

当 LogLevel 大于 0 时，驱动程序保存日志文件的文件夹的完整路径。

此参数为可选项。

Min_TLS

- Default Value（默认值）：1.0
- 数据类型 – 字符串

驱动程序允许数据存储以用于对连接进行加密的 TLS/SSL 的最低版本。例如，如果指定了 TLS 1.1，则无法使用 TLS 1.0 对连接进行加密。

Min_TLS 接受以下值：

- 1.0：连接必须至少使用 TLS 1.0。
- 1.1：连接必须至少使用 TLS 1.1。
- 1.2：连接必须至少使用 TLS 1.2。

此参数为可选项。

partner_spid

- 默认值 – 无
- 数据类型 – 字符串

在使用 PPingFederate 服务验证连接时使用的合作伙伴 SPID（服务提供商 ID）值。

此参数为可选项。

Password（密码）| PWS

- 默认值 – 无
- 数据类型 – 字符串

与您在 User（用户）字段（UID | User（用户）| LogonID）中提供的用户名相对应的密码。

此参数为可选项。

plugin_name

- 默认值 – 无
- 数据类型 – 字符串

要用于身份验证的凭证提供程序插件名称。

支持下列值：

- `ADFS`：使用 Active Directory 联合身份验证服务进行身份验证。
- `AzureAD`：使用 Microsoft Azure Active Directory (AD) 服务进行身份验证。
- `BrowserAzureAD`：使用适用于 Microsoft Azure Active Directory (AD) 服务的浏览器插件进行身份验证。
- `BrowserSAML`：使用适用于 SAML 服务（如 Okta 或 Ping）的浏览器插件进行身份验证。
- `JWT`：使用 JSON Web 令牌 (JWT) 进行身份验证。
- `Ping`：使用 PingFederate 服务进行身份验证。
- `Okta`：使用 Okta 服务进行身份验证。

此参数为可选项。

Port（端口）| PortNumber

- Default Value（默认值）：5439
- 数据类型 – 整数

Amazon Redshift 服务器用于侦听客户端连接的 TCP 端口号。

此参数为可选项。

preferred_role

- 默认值 – 无
- 数据类型 – 字符串

您希望在 Amazon Redshift 连接期间担任的角色。它将用于 IAM 身份验证。

此参数为可选项。

Profile

- 默认值 – 无
- 数据类型 – 字符串

用于在 Amazon Redshift 中进行身份验证的用户 Amazon 配置文件的名称。

- 如果 Use Instance Profile（使用实例配置文件）参数（InstanceProfile 属性）设置为 1 | TRUE，则该设置将优先，驱动程序将改用 Amazon EC2 实例配置文件。
- 包含配置文件的凭证文件的默认位置为 `~/.aws/Credentials`。`AWS_SHARED_CREDENTIALS_FILE` 环境变量可用于指向其他凭证文件。

此参数为可选项。

provider_name

- 默认值 – 无
- 数据类型 – 字符串

用户使用 CREATE IDENTITY PROVIDER（创建身份提供程序）查询创建的身份验证提供程序。它将用于本机 Amazon Redshift 身份验证。

此参数为可选项。

ProxyHost

- 默认值 – 无
- 数据类型 – 字符串

要通过其连接的代理服务器的主机名或 IP 地址。

此参数为可选项。

ProxyPort

- 默认值 – 无
- 数据类型 – 整数

代理服务器用于侦听客户端连接的端口号。

此参数为可选项。

ProxyPwd

- 默认值 – 无
- 数据类型 – 字符串

用于访问代理服务器的密码。

此参数为可选项。

ProxyUid

- 默认值 – 无
- 数据类型 – 字符串

用于访问代理服务器的用户名。

此参数为可选项。

ReadOnly

- 默认值：0
- 数据类型 – Boolean

一个布尔值，用于指定驱动程序是否处于只读模式。

- 1 | TRUE：连接处于只读模式，无法写入数据存储。
- 0 | FALSE：连接不处于只读模式，可以写入数据存储。

此参数为可选项。

region

- 默认值 – 无
- 数据类型 – 字符串

您的集群所在的 Amazon 区域。

此参数为可选项。

SecretAccessKey

- 默认值 – 无
- 数据类型 – 字符串

用户或角色的 IAM 秘密密钥。如果您设置此参数，则还必须设置 AccessKeyID。

此参数为可选项。

SessionToken

- 默认值 – 无
- 数据类型 – 字符串

与您用于身份验证的 IAM 角色关联的临时 IAM 会话令牌。

此参数为可选项。

Server（服务器）| HostName | Host（主机）

- 默认值 – 无
- 数据类型 – 字符串

要连接到的端点服务器。

此参数为必需参数。

ssl_insecure

- 默认值：0

- 数据类型 – Boolean

一个布尔值，用于指定驱动程序是否检查 IdP 服务器证书的真实性。

- 1 | TRUE：驱动程序不检查 IdP 服务器证书的真实性。
- 0 | FALSE：驱动程序检查 IdP 服务器证书的真实性

此参数为可选项。

SSLMode

- 默认值 – `verify-ca`
- 数据类型 – 字符串

在连接到 Amazon Redshift 时要使用的 SSL 证书验证模式。以下是可能的值：

- `verify-full`：仅使用 SSL、受信任的证书颁发机构和与证书匹配的服务器名称进行连接。
- `verify-ca`：仅使用 SSL 和受信任的证书颁发机构进行连接。
- `require`：仅使用 SSL 进行连接。
- `prefer`：使用 SSL 进行连接（如果可用）。否则，将在不使用 SSL 的情况下进行连接。
- `allow`：默认情况下，不使用 SSL 进行连接。如果服务器需要 SSL 连接，则使用 SSL。
- `disable`：不使用 SSL 进行连接。

此参数为可选项。

StsConnectionTimeout

- 默认值：0
- 数据类型 – 整数

IAM 连接的最长等待时间（以秒为单位）。如果设置为 0 或未指定，驱动程序将为每次 Amazon STS 调用等待 60 秒。

此参数为可选项。

StsEndpointUrl

- 默认值 – 无
- 数据类型 – 字符串

此选项指定用于与 Amazon Security Token Service (Amazon STS) 通信的覆盖端点。

此参数为可选项。

UID | User（用户）| LogonID

- 默认值 – 无
- 数据类型 – 字符串

用于访问 Amazon Redshift 服务器的用户名。

如果使用数据库身份验证，则此参数是必需项。

web_identity_token

- 默认值 – 无
- 数据类型 – 字符串

身份提供程序提供的 OAUTH 令牌。它将在 JWT 插件中使用。

如果您将 plugin_name 参数设置为 BasicJwtCredentialsProvider，则此参数是必需项。

配置 ODBC 连接

您可以使用 ODBC 连接将许多第三方 SQL 客户端工具和应用程序连接到您的 Amazon Redshift 集群。为此，请在您的客户端计算机或 Amazon EC2 实例上设置连接。如果您的客户端工具支持 JDBC，您可以选择使用 JDBC 连接而非 ODBC 连接，因为 JDBC 连接更加易于配置。但是，如果您的客户端工具不支持 JDBC，请按此部分中的步骤配置 ODBC 连接。

Amazon Redshift 提供了适用于 Linux、Windows 和 macOS X 操作系统的 64-bit ODBC 驱动程序。32 位 ODBC 驱动程序已停产。除了紧急安全补丁外，不会发布进一步的更新。

有关 ODBC 驱动程序功能和先决条件的最新信息，请参阅 Amazon Redshift ODBC 驱动程序发布说明。在中国 Amazon 区域中，使用以下链接：Amazon Redshift ODBC 驱动程序发布说明。

有关 Amazon Redshift ODBC 驱动程序的安装和配置信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南。

如果要使用 ODBC 连接，请执行以下步骤。

主题

- 获取集群的 ODBC URL (p. 207)
- 在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 208)
- 在 Linux 上安装 Amazon Redshift ODBC 驱动程序 (p. 210)
- 在 macOS X 上安装 Amazon Redshift ODBC 驱动程序 (p. 211)
- 使用 ODBC 驱动程序管理器在 Linux 和 macOS X 操作系统上配置驱动程序 (p. 212)
- 配置 ODBC 驱动程序选项 (p. 216)
- 早期 ODBC 驱动程序版本 (p. 216)

获取集群的 ODBC URL

Amazon Redshift 在 Amazon Redshift 控制台中显示您的集群的 ODBC URL。此 URL 包含在客户端计算机与数据库之间建立连接时所需的信息。

ODBC URL 采用以下格式：

```
Driver={driver};Server=endpoint;Database=database_name;UID=user_name;PWD=password;Port
```

前面显示的格式的字段具有以下值。

字段	值
`Driver`	要使用的 64 位 ODBC 驱动程序的名称：Amazon Redshift (x64)。 32 位 ODBC 驱动程序的名称：Amazon Redshift (x86)。
`Server`	Amazon Redshift 集群的端点。

字段	值
Database	您为集群创建的数据库。
UID	有权连接到数据库的用户账户的用户名。该值是数据库权限，而非 Amazon Redshift 权限，但是您可以使用您在启动集群时设置的管理员用户账户。
PWD	用户账户用于连接数据库的密码。
Port	您在启动集群时指定的端口号。如果您启用了防火墙，请确保此端口处于打开状态，可供您使用。

以下是一个示例 ODBC URL：`Driver={Amazon Redshift (x64)}; Server=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com; Database=dev; UID=adminuser; PWD=insert_your_admin_user_password_here; Port=5439`

有关如何获取 ODBC 连接的信息，请参阅 查找集群连接字符串 (p. 136)。

在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序

系统要求

您可以在可访问 Amazon Redshift 数据仓库的客户端计算机上安装 Amazon Redshift ODBC 驱动程序。在其上安装该驱动程序的每台计算机都必须满足一系列最低系统要求。有关最低系统要求的信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南。

在 Windows 操作系统上安装 Amazon Redshift 驱动程序

使用以下过程下载适用于 Windows 操作系统的 Amazon Redshift ODBC 驱动程序。仅在您当前运行的第三方应用程序获得了使用 Amazon Redshift 的认证并且需要特定的驱动程序时，才使用上述驱动程序之外的驱动程序。

安装 ODBC 驱动程序

1. 根据您的 SQL 客户端工具或应用程序的系统架构，下载以下驱动程序之一：

   - 64 位 ODBC 驱动程序版本 1.4.56 在中国 Amazon 区域，使用以下链接：64 位 ODBC 驱动程序版本 1.4.56。

     此驱动程序的名称为 Amazon Redshift (x64)。
   - 32 位 ODBC 驱动程序版本 1.4.52 在中国 Amazon 区域，使用以下链接：32 位 ODBC 驱动程序版本 1.4.52

     此驱动程序的名称为 Amazon Redshift (x86)。32 位 ODBC 驱动程序已停产。除了紧急安全补丁外，不会发布进一步的更新。

     Note

     根据您的 SQL 客户端工具或应用程序的系统架构，下载相应的 MSI 包。例如，如果您的 SQL 客户端工具是 64 位，则安装 64 位驱动程序。

   然后，下载并查看 Amazon Redshift ODBC 和 JDBC 驱动程序许可证协议。在中国（北京）区域中，使用以下链接：Amazon Redshift ODBC 和 JDBC 驱动程序许可证协议。
2. 双击 .msi 文件，然后按照向导中的步骤安装驱动程序。

在 Microsoft Windows 上为 ODBC 连接创建系统 DSN 条目

下载并安装 ODBC 驱动程序后，将数据源名称 (DSN) 条目添加到客户端计算机或 Amazon EC2 实例。SQL 客户端工具将使用此数据源连接到 Amazon Redshift 数据库。

建议您创建系统 DSN 而不是用户 DSN。一些应用程序使用不同的用户账户加载数据。这些应用程序可能无法检测在其他用户账户下创建的用户 DSN。

> Note
>
> 对于使用 Amazon Identity and Access Management (IAM) 凭证或身份提供者 (IdP) 凭证进行的身份验证，需要执行其他步骤。有关更多信息，请参阅配置 JDBC 或 ODBC 连接以使用 IAM 凭证 (p. 397)。

有关如何创建系统 DSN 条目的信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南。

在 Windows 上为 ODBC 连接创建系统 DSN 条目

1. 在 Start (开始) 菜单上，打开 ODBC Data Sources (ODBC 数据源)。

   请确保您选择的 ODBC Data Source Administrator 的位数与用于连接 Amazon Redshift 的客户端应用程序的位数相同。
2. 在 ODBC Data Source Administrator 中，选择 Driver（驱动程序）选项卡并找到驱动程序文件夹。

   - Amazon Redshift ODBC 驱动程序（64 位）
   - Amazon Redshift ODBC 驱动程序（32 位）
3. 选择 System DSN (系统 DSN) 选项卡为计算机上的所有用户配置驱动程序，或选择 User DSN (用户 DSN) 选项卡仅为您的用户账户配置驱动程序。
4. 选择 Add (添加)。系统随即打开 Create New Data Source 窗口。
5. 选择 Amazon Redshift ODBC 驱动程序，然后选择 Finish（完成）。系统随即打开 Amazon Redshift ODBC Driver DSN Setup 窗口。
6. 在 Connection Settings 下，输入以下信息：

   Data source name

   输入数据源的名称。在稍后创建到集群的连接时，您可以使用任何名称来标识该数据源。例如，如果您遵循的是《Amazon Redshift 入门指南》，则可键入 `exampleclusterdsn`，以便轻松记住将与此 DSN 关联的集群。

   服务器

   为您的 Amazon Redshift 集群指定端点。您可以在 Amazon Redshift 控制台中的集群详细信息页面上找到该信息。有关更多信息，请参阅在 Amazon Redshift 中配置连接 (p. 136)。

   端口

   输入数据库使用的端口号。预设情况下，Amazon Redshift 使用 5439，但应使用在集群启动时配置使用的端口。

   数据库。

   输入 Amazon Redshift 数据库的名称。如果您在未指定数据库名称的情况下启动了集群，请输入 *dev*。否则，请使用您在启动过程中选择的名称。如果您遵循的是《Amazon Redshift 入门指南》，输入 *dev*。
7. 在 Authentication (身份验证) 下，指定配置选项以配置标准或 IAM 身份验证。有关身份验证选项的信息，请参阅《Amazon Redshift ODBC 驱动程序安装和配置指南》中的“在 Windows 上配置身份验证”。
8. 在 SSL Settings 下，指定以下项目的值：

SSL authentication

选择处理安全套接字层 (SSL) 的模式。在测试环境中，可以使用 `prefer`。但是，对于生产环境以及在需要安全交换数据时，请使用 `verify-ca` 或 `verify-full`。有关在 Windows 上使用 SSL 的更多信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南中的“在 Windows 上配置 SSL 验证”。

9. 在 Additional Options (其他选项) 下，指定有关如何将查询结果返回至您的 SQL 客户端工具或应用程序的选项。有关更多信息，请参阅 Amazon Redshift ODBC 驱动程序安装和配置指南中的“在 Windows 上配置其他选项”。
10. 在 Logging Options (日志记录选项) 中，指定日志记录选项的值。有关更多信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南中的“在 Windows 上配置日志记录选项”。

    然后选择 OK（确定）。
11. 在 Data Type Options (数据类型选项) 下，指定数据类型的值。有关更多信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南中的“在 Windows 上配置数据类型选项”。

    然后选择 OK（确定）。
12. 选择测试。如果客户端计算机可以连接到 Amazon Redshift 数据库，您会看到以下消息：Connection successful（连接成功）。

    如果客户端计算机无法连接到数据库，您可以进行故障排除，解决可能存在的问题。有关更多信息，请参阅解决 Amazon Redshift 中的连接问题 (p. 263)。
13. 在 Windows 上配置 TCP Keepalive 以防止连接超时。有关如何在 Windows 上配置 TCP Keepalive 的信息，请参阅 Amazon Redshift ODBC 驱动程序安装和配置指南。
14. 要帮助进行故障排除，请配置日志记录。有关如何在 Windows 上配置日志记录的信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南。

在 Linux 上安装 Amazon Redshift ODBC 驱动程序

系统要求

您可以在可访问 Amazon Redshift 数据仓库的客户端计算机上安装 Amazon Redshift ODBC 驱动程序。在其上安装该驱动程序的每台计算机都必须满足一系列最低系统要求。有关最低系统要求的信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南。

在 Linux 操作系统上安装 Amazon Redshift 驱动程序

按照此部分中的步骤在受支持的 Linux 发行版上下载并安装 Amazon Redshift ODBC 驱动程序。在安装过程中，驱动程序文件将被安装到以下目录中：

- `/opt/amazon/redshiftodbc/lib/64`（对于 64 位驱动程序）
- `/opt/amazon/redshiftodbc/ErrorMessages`
- `/opt/amazon/redshiftodbc/Setup`
- `/opt/amazon/redshiftodbc/lib/32`（对于 32 位驱动程序）

要安装 Amazon Redshift ODBC 驱动程序

1. 根据您的 SQL 客户端工具或应用程序的系统架构，下载以下驱动程序之一：
   - 64 位 RPM 驱动程序版本 1.4.56 在中国 Amazon 区域，使用以下链接：64 位 RPM 驱动程序版本 1.4.56。
   - 64 位 Debian 驱动程序版本 1.4.56 在中国 Amazon 区域，使用以下链接：64 位 Debian 驱动程序版本 1.4.56。

- 32 位 RPM 驱动程序版本 1.4.52 在中国 Amazon 区域，使用以下链接：32 位 RPM 驱动程序版本 1.4.52
- 32 位 Debian 驱动程序版本 1.4.52 在中国 Amazon 区域，使用以下链接：32 位 Debian 驱动程序版本 1.4.52

这些驱动程序的名称均是 Amazon Redshift ODBC 驱动程序。32 位 ODBC 驱动程序已停产。除了紧急安全补丁外，不会发布进一步的更新。

Note

下载适用于您的 SQL 客户端工具或应用程序系统架构的程序包。例如，如果您的客户端工具是 64 位，则安装 64 位驱动程序。

然后，下载并查看 Amazon Redshift ODBC 和 JDBC 驱动程序许可证协议。在中国（北京）区域中，使用以下链接：Amazon Redshift ODBC 和 JDBC 驱动程序许可证协议。

2. 转至您下载程序包的位置，然后运行以下命令之一。使用适用于您的 Linux 发行版的命令。

   - 在 RHEL 和 CentOS 操作系统上，运行以下命令。

   ```
   yum --nogpgcheck localinstall RPMFileName
   ```

   将 *RPMFileName* 替换为 RPM 包文件名。例如，以下命令将演示如何安装 64 位驱动程序。

   ```
   yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-1.x.xx.xxxx-x.x86_64.rpm
   ```

   - 在 SLES 上，运行以下命令。

   ```
   zypper install RPMFileName
   ```

   将 *RPMFileName* 替换为 RPM 包文件名。例如，以下命令将演示如何安装 64 位驱动程序。

   ```
   zypper install AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.rpm
   ```

   - 在 Debian 上，运行以下命令。

   ```
   sudo apt install ./DEBFileName.deb
   ```

   将 *DEBFileName.deb* 替换为 Debian 包文件名。例如，以下命令将演示如何安装 64 位驱动程序。

   ```
   sudo apt install ./AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.deb
   ```

Important

安装完驱动程序后，请对其进行配置以在您的系统上使用。有关驱动程序配置的更多信息，请参阅使用 ODBC 驱动程序管理器在 Linux 和 macOS X 操作系统上配置驱动程序 (p. 212)。

在 macOS X 上安装 Amazon Redshift ODBC 驱动程序

系统要求

您可以在可访问 Amazon Redshift 数据仓库的客户端计算机上安装驱动程序。在其上安装该驱动程序的每台计算机都必须满足一系列最低系统要求。有关最低系统要求的信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南。

在 macOS X 上安装 Amazon Redshift ODBC 驱动程序

按照此部分中的步骤操作，在受支持的 macOS X 版本上下载和安装 Amazon Redshift ODBC 驱动程序。在安装过程中，驱动程序文件将被安装到以下目录中：

- `/opt/amazon/redshift/lib/universal`
- `/opt/amazon/redshift/ErrorMessages`
- `/opt/amazon/redshift/Setup`

要在 macOS X 上安装 Amazon Redshift ODBC 驱动程序

1. 下载 macOS X 驱动程序版本 1.4.56。此驱动程序的名称均是 Amazon Redshift ODBC 驱动程序。在中国 Amazon 区域，使用以下链接：macOS X 驱动程序版本 1.4.56。

   然后，下载并查看 Amazon Redshift ODBC 和 JDBC 驱动程序许可证协议。在中国（北京）区域中，使用以下链接：Amazon Redshift ODBC 和 JDBC 驱动程序许可证协议。
2. 双击 AmazonRedshiftODBC.dmg 以挂载磁盘映像。
3. 双击 AmazonRedshiftODBC.pkg 以运行安装程序。
4. 按照安装程序中的步骤完成驱动程序的安装过程。要执行安装，需同意许可协议的条款。

   Important

   安装完驱动程序后，请对其进行配置以在您的系统上使用。有关驱动程序配置的更多信息，请参阅使用 ODBC 驱动程序管理器在 Linux 和 macOS X 操作系统上配置驱动程序 (p. 212)。

使用 ODBC 驱动程序管理器在 Linux 和 macOS X 操作系统上配置驱动程序

在 Linux 和 macOS X 操作系统上，您可以使用 ODBC 驱动程序管理器来配置 ODBC 连接设置。ODBC 驱动程序管理器使用配置文件来定义和配置 ODBC 数据源和驱动程序。您可以使用的 ODBC 驱动程序管理器取决于您使用的操作系统：

- unixODBC 驱动程序管理器（适用于 Linux 操作系统）
- iODBC 驱动程序管理器（适用于 macOS X 操作系统）

有关用来配置 Amazon Redshift ODBC 驱动程序的受支持的 ODBC 驱动程序管理器的更多信息，请参阅系统要求 (p. 210)（适用于 Linux 操作系统）和系统要求 (p. 211)（适用于 macOS X 操作系统）。另请参阅 Amazon Redshift ODBC 连接器安装和配置指南中的“在非 Windows 计算机上指定 ODBC 驱动程序管理器”。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南

要配置 Amazon Redshift ODBC 驱动程序，需要提供以下三个文件：`amazon.redshiftodbc.ini`、`odbc.ini` 和 `odbcinst.ini`。

如果您将驱动程序安装在默认位置，`amazon.redshiftodbc.ini` 配置文件则位于以下目录之一：

- `/opt/amazon/redshiftodbc/lib/64`（适用于 Linux 操作系统上的 64 位驱动程序）
- `/opt/amazon/redshiftodbc/lib/32`（适用于 Linux 操作系统上的 32 位驱动程序）
- `/opt/amazon/redshift/lib`（适用于 macOS X 上的驱动程序）

此外，在 `/opt/amazon/redshiftodbc/Setup` (Linux) 或 /opt/amazon/redshift/Setup (macOS X) 下，提供了示例 `odbc.ini` 和 `odbcinst.ini` 文件。您可以使用这些文件作为配置 Amazon Redshift ODBC 驱动程序和数据源名称 (DSN) 的示例。

我们不建议使用 Amazon Redshift ODBC 驱动程序安装目录来存储配置文件。`Setup` 目录中的示例文件仅用作示例。如果您日后重新安装 Amazon Redshift ODBC 驱动程序，或将其升级到新版本，安装目录会被覆盖。之后，您将丢失对这些文件所做的全部更改。

为了避免出现这种情况，请将 amazon.redshiftodbc.ini 文件复制到安装目录以外的其他目录中。如果您要将此文件复制到用户的主目录，请在文件名的开头添加一个句点 (.)，使其成为隐藏文件。

对于 odbc.ini 和 odbcinst.ini 文件，应在用户的主目录中使用配置文件，或者在其他目录中创建新版本。默认情况下，您的 Linux 或 macOS X 操作系统应在用户的主目录（odbc.ini 或 odbcinst.ini）中提供有 /home/$USER 文件和 ~/ 文件。这些默认文件均为隐藏文件（通过在每个文件名的前面添加圆点 (.) 表示）。这些文件仅当您使用 -a 标志列出目录内容时显示。

对于 odbc.ini 和 odbcinst.ini 文件，不管您选择哪个选项，都需对这些文件进行修改，以添加驱动程序和 DSN 配置信息。如果您创建新文件，则还需设置环境变量，以指定这些配置文件的目标存储位置。

原定设置情况下，ODBC 驱动程序管理器将配置为使用主目录中隐藏的 odbc.ini 和 odbcinst.ini 配置文件版本（名为 .odbc.ini 和 .odbcinst.ini）。它们也被配置为使用驱动程序安装目录的 amazon.redshiftodbc.ini 子文件夹中的 /lib 文件。如果您将这些配置文件存储在其他位置，请设置如下所述的环境变量，以便驱动程序管理器能够找到这些文件。有关更多信息，请参阅 Amazon Redshift ODBC 驱动程序安装和配置指南中的“指定驱动程序配置文件的位置”。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南

在 Linux 和 macOS X 操作系统上创建数据源名称

在使用数据源名称 (DSN) 连接到数据存储时，请配置 odbc.ini 文件以定义 DSN。在 odbc.ini 文件中设置属性以创建指定数据存储的连接信息的 DSN。

有关如何配置 odbc.ini 文件的信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南中的“在非 Windows 计算机上创建数据源名称”在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南

请在 Linux 操作系统上使用以下格式。

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file

Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

以下示例显示了在 Linux 操作系统上使用 64 位 ODBC 驱动程序配置 odbc.ini。

```
[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
```

以下示例显示了在 Linux 操作系统上使用 32 位 ODBC 驱动程序配置 odbc.ini。

```
[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
```

请在 macOS X 操作系统上使用以下格式。

```
[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
```

以下示例显示了 odbc.ini 在 macOS X 操作系统上的配置。

```
[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
```

在 Linux 和 macOS X 操作系统上配置没有 DSN 的连接

要通过不带 DSN 的连接来连接到数据存储，请在 odbcinst.ini 文件中定义驱动程序。然后，在应用程序中提供一个无 DSN 的连接字符串。

有关在这种情况下如何配置 odbcinst.ini 文件的信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南中的“在非 Windows 计算机上配置没有 DSN 的连接”。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南

请在 Linux 操作系统上使用以下格式。

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

以下示例显示了安装在 Linux 操作系统默认目录中的 64 位驱动程序的 odbcinst.ini 配置。

```
[ODBC Drivers]
Amazon Redshift (x64)=Installed

[Amazon Redshift (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
```

以下示例显示了安装在 Linux 操作系统默认目录中的 32 位驱动程序的 odbcinst.ini 配置。

```
[ODBC Drivers]
Amazon Redshift (x86)=Installed

[Amazon Redshift (x86)]
Description=Amazon Redshift ODBC Driver (32-bit)
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so
```

请在 macOS X 操作系统上使用以下格式。

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/lib/amazonredshiftodbc.dylib

...
```

以下示例显示了安装在 macOS X 操作系统默认目录中的驱动程序的 odbcinst.ini 配置。

```
[ODBC Drivers]
Amazon RedshiftODBC DSN=Installed

[Amazon RedshiftODBC DSN]
Description=Amazon Redshift ODBC Driver for macOS X
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
```

配置环境变量

使用正确的 ODBC 驱动程序管理器加载正确的驱动程序。为此，请设置库路径环境变量。有关更多信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南中的“在非 Windows 计算机上指定 ODBC 驱动程序管理器”。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南

原定设置情况下，ODBC 驱动程序管理器将配置为使用主目录中隐藏的 odbc.ini 和 odbcinst.ini 配置文件版本（名为 .odbc.ini 和 .odbcinst.ini）。它们也被配置为使用驱动程序安装目录的 /lib 子文件夹中的 amazon.redshiftodbc.ini 文件。如果您将这些配置文件存储在其他位置，请设置环境变量，以便驱动程序管理器能够找到这些文件。有关更多信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南中的“指定驱动程序配置文件的位置”。

配置连接功能

可以为 ODBC 设置配置以下连接功能：

- 配置 ODBC 驱动程序以提供凭证并验证与 Amazon Redshift 数据库的连接。
- 如果要连接到启用了 SSL 的 Amazon Redshift 服务器，请将 ODBC 驱动程序配置为连接到启用了安全套接字层 (SSL) 的套接字。
- 将 ODBC 驱动程序配置为通过代理服务器连接到 Amazon Redshift。
- 将 ODBC 驱动程序配置为使用查询处理模式来防止查询占用过多内存。
- 将 ODBC 驱动程序配置为通过代理服务器传递 IAM 身份验证过程。
- 将 ODBC 驱动程序配置为使用 TCP Keepalive 来防止连接超时。

有关这些连接功能的信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南。

配置 ODBC 驱动程序选项

可以使用配置选项来控制 Amazon Redshift ODBC 驱动程序的行为。

在 Microsoft Windows 中，您通常可以在配置数据源名称 (DSN) 时设置驱动程序选项。您还能在以编程方式连接时，或者通过在 `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\your_DSN` 中添加或更改注册表项来设置驱动程序选项。有关配置 DSN 的更多信息，请参阅在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 208)。有关在连接字符串中设置驱动程序选项的示例，请参阅以编程方式连接到集群 (p. 258)。

在 Linux 和 macOS X 中，您可以在 `odbc.ini` 和 `amazon.redshiftodbc.ini` 文件中设置驱动程序配置选项，如使用 ODBC 驱动程序管理器在 Linux 和 macOS X 操作系统上配置驱动程序 (p. 212)中所述。在 `amazon.redshiftodbc.ini` 文件中设置的配置选项适用于所有连接。相反，`odbc.ini` 文件中的设置配置选项特定于一个连接。在 `odbc.ini` 中设置的配置选项优先于在 `amazon.redshiftodbc.ini` 中设置的配置选项。

有关如何设置 ODBC 驱动程序配置选项的信息，请参阅 Amazon Redshift ODBC 连接器安装和配置指南。在中国 Amazon 区域，使用以下链接：Amazon Redshift ODBC 连接器安装和配置指南。

早期 ODBC 驱动程序版本

仅当您的工具需要使用某个特定版本的驱动程序时，才能下载 Amazon Redshift ODBC 驱动程序的以前版本。

使用适用于 Windows 的以前 ODBC 驱动程序版本

以下是 64 位驱动程序：

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.53.1000/AmazonRedshiftODBC64-1.4.53.1000.msi 在中国 Amazon 区域，使用以下链接。https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/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 在中国 Amazon 区域，使用以下链接。https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC64-1.4.52.1000.msi

32 位驱动程序已停用，并且早期版本不受支持。

使用适用于 Linux 的以前 ODBC 驱动程序版本

以下是 64 位驱动程序版本：

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-64-bit-1.4.52.1000-1.x86_64.rpm 在中国 Amazon 区域，使用以下链接。https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/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 在中国 Amazon 区域，使用以下链接。https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-64-bit-1.4.52.1000-1.x86_64.deb

32 位驱动程序已停用，并且早期版本不受支持。

使用适用于 macOS X 的以前 ODBC 驱动程序版本

以下是适用于 macOS X 的 Amazon Redshift ODBC 驱动程序版本：

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-1.4.52.1000.dmg 在中国 Amazon 区域，使用以下链接。https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-1.4.52.1000.dmg

配置连接的安全选项

Amazon Redshift 支持安全套接字层 (SSL) 连接来加密数据和服务器证书，以验证客户端连接到的服务器证书。

使用 SSL 进行连接

为了支持 SSL 连接，Amazon Redshift 会在每个集群中创建并安装 Amazon Certificate Manager (ACM) 颁发的 SSL 证书。ACM 证书受到大多数操作系统、Web 浏览器和客户端的公开信任。如果您的 SQL 客户端或应用程序使用 SSL 连接到 Amazon Redshift，并且 `sslmode` 连接选项设置为 `require`、`verify-ca` 或 `verify-full`，则您可能需要下载证书捆绑包。如果您的客户需要，Amazon Redshift 会提供如下捆绑证书：

- 捆绑包下载地址：https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt。
  - 预期的 MD5 校验码为 418dea9b6d5d5d5de7a8f1ac42e164cdcf。
  - sha256 预期的 MD5 校验码是 36dba8e4b8041cd14b9d601593963301bcbb92e1c456847784de2acb5bd550。

  不要使用位于 `https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt` 的之前的证书捆绑包。
- 在中国 Amazon Web Services 区域，请从以下网址下载捆绑包：https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt。
  - 预期的 MD5 校验码为 418dea9b6d5d5d5de7a8f1ac42e164cdcf。
  - sha256 预期的 MD5 校验码是 36dba8e4b8041cd14b9d601593963301bcbb92e1c456847784de2acb5bd550。

  不要使用位于 `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` 和 `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem` 的以前的证书捆绑包

  Important

  Amazon Redshift 改变了我们管理 SSL 证书的方法。您可能需要更新当前的信任根 CA 证书，才能继续使用 SSL 连接集群。有关更多信息，请参阅将 SSL 连接过渡到 ACM 证书 (p. 220)。

默认情况下，无论连接是否使用 SSL，集群数据库都会接受该连接。要将您的集群配置为需要使用 SSL 连接，请在与集群关联的参数组中将 `require_SSL` 参数设置为 `true`。

Amazon Redshift 支持符合联邦信息处理标准 (FIPS) 140-2 的 SSL 模式。符合 FIPS 的 SSL 模式在默认情况下处于禁用状态。

Important

仅在您的系统需要与 FIPS 兼容时才启用与 FIPS 兼容的 SSL 模式。

要启用符合 FIPS 的 SSL 模式，请在与集群关联的参数组中将 `use_fips_ssl` 参数和 `require_SSL` 参数设置为 `true`。有关修改参数组的信息，请参阅Amazon Redshift 参数组 (p. 299)。

Amazon Redshift 支持 Elliptic Curve Diffie—Hellman Ephemeral (ECDHE) 密钥协商协议。ECDHE 使得客户端和服务器各有一个椭圆曲线公有/私有密钥对，用来在不安全的通道上创建共享密钥。您无需在 Amazon

Redshift 中进行任何配置即可启用 ECDHE。如果您从使用 ECDHE 来加密客户端与服务器间通信的 SQL 客户端工具进行连接，则 Amazon Redshift 将使用提供的密码列表来建立合适的连接。有关更多信息，请参阅 Wikipedia 上的 Elliptic curve diffie—hellman 和 OpenSSL 网站上的密码。

在 ODBC 中使用 SSL 和信任 CA 证书

如果您使用最新 Amazon Redshift ODBC 驱动程序 (1.3.7.1000 版或更高版本) 连接，则可以跳过此部分。要下载最新驱动程序，请参阅配置 ODBC 连接 (p. 207)。

您可能需要更新当前的信任根 CA 证书，才能继续使用 SSL 连接集群。有关更多信息，请参阅使用 SSL 进行连接 (p. 217)。

您可以验证下载的证书是否与此预期的 MD5 校验和码匹配。为此，您可以在 Linux 操作系统上使用 Md5sum 程序，或者在 Windows 和 macOS X 操作系统上使用其他工具。

ODBC DSN 中的 `sslmode` 设置用于确定如何处理客户端连接加密和服务器证书验证。Amazon Redshift 支持客户端连接中的以下 `sslmode` 值：

- `disable`

  SSL 处于禁用状态，且连接未加密。
- `allow`

  如果服务器需要，则使用 SSL。
- `prefer`

  如果服务器支持，则使用 SSL。Amazon Redshift 支持 SSL，因此您可以在将 `sslmode` 设置为 `prefer` 时使用 SSL。
- `require`

  需要使用 SSL。
- `verify-ca`

  必须使用 SSL，且必须验证服务器证书。
- `verify-full`

  必须使用 SSL。必须验证服务器证书，且服务器主机名必须与证书上的主机名属性一致。

您可以确定是否使用了 SSL 以及是否在客户端和服务器之间的连接中验证了服务器证书。为此，您需要查看客户端上 ODBC DSN 的 `sslmode` 设置以及服务器上 Amazon Redshift 集群的 `require_SSL` 设置。下表介绍了各种客户端与服务器设置组合的加密结果：

sslmode（客户端）	require_SSL（服务器）	结果
`disable`	`false`	连接未加密。
`disable`	`true`	由于服务器需要使用 SSL，但客户端针对该连接禁用了 SSL，因此无法建立连接。
`allow`	`true`	连接经过加密。
`allow`	`false`	连接未加密。
`prefer` 或者 `require`	`true`	连接经过加密。

sslmode（客户端）	require_SSL（服务器）	结果
prefer 或者 require	false	连接经过加密。
verify-ca	true	连接经过加密，且验证了服务器证书。
verify-ca	false	连接经过加密，且验证了服务器证书。
verify-full	true	连接经过加密，且验证了服务器证书和主机名。
verify-full	false	连接经过加密，且验证了服务器证书和主机名。

在 Microsoft Windows 上使用服务器证书和 ODBC 进行连接

如果要使用 SSL 和服务器证书连接到集群，请先将证书下载到客户端计算机或 Amazon EC2 实例。然后配置 ODBC DSN。

1. 将 Amazon Redshift 证书颁发机构包下载到客户端计算机上的驱动程序安装目录中的 lib 文件夹，然后将该文件另存为 root.crt。有关下载信息，请参阅使用 SSL 进行连接 (p. 217)。
2. 打开 ODBC Data Source Administrator，然后添加或编辑 ODBC 连接的系统 DSN 条目。对于 SSL Mode，如果不使用 DNS 别名，请选择 verify-full。如果您使用 DNS 别名，请选择 verify-ca。然后选择 Save (保存)。

   有关配置 ODBC DSN 的更多信息，请参阅配置 ODBC 连接 (p. 207)。

在 Java 中使用 SSL 和服务器证书

SSL 通过加密可在您的客户端与集群之间移动的数据来提供一个安全层。使用服务器证书可验证集群是否为 Amazon Redshift 集群，从而提供一个额外的安全层。具体方法是，检查自动安装在您预配置的所有集群上的服务器证书。有关将服务器证书 JDBC 一起使用的更多信息，请转到 PostgreSQL 文档中的配置客户端。

在 Java 中使用信任 CA 证书以进行连接

> **Important**
>
> Amazon Redshift 改变了我们管理 SSL 证书的方法。您可能需要更新当前的信任根 CA 证书，才能继续使用 SSL 连接集群。有关更多信息，请参阅使用 SSL 进行连接 (p. 217)。

使用信任 CA 证书进行连接

您可以使用 redshift-keytool.jar 文件将 Amazon Redshift 证书颁发机构包中的 CA 证书导入 Java 信任存储库或您的私有信任存储库中。

1. 如果您使用 Java 命令行 -Djavax.net.ssl.trustStore 选项，请尽量将其从命令行中删除。
2. 下载 redshift-keytool.jar。
3. 请执行下列操作之一：

   - 要将 Amazon Redshift 证书颁发机构捆绑包导入 Java 信任存储库中，请运行以下命令。

     ```
     java -jar redshift-keytool.jar -s
     ```

   - 要将 Amazon Redshift 证书颁发机构捆绑包导入您的私有信任存储库中，请运行以下命令：

     ```
     java -jar redshift-keytool.jar -k <your_private_trust_store> -p <keystore_password>
     ```

将 SSL 连接过渡到 ACM 证书

Amazon Redshift 正将您的集群中的 SSL 证书替换为 Amazon Certificate Manager (ACM) 颁发的证书。ACM 是一个可信的公有证书颁发机构 (CA)，受当前大多数系统信任。您可能需要更新当前的信任根 CA 证书，才能继续使用 SSL 连接集群。

仅当满足以下所有条件时，此更改才会影响到您：

- 您的 SQL 客户端或应用程序使用 SSL 连接 Amazon Redshift 集群，并将 `sslMode` 连接选项设置为 `require`、`verify-ca` 或 `verify-full` 配置选项。
- 您不使用 Amazon Redshift ODBC 或 JDBC 驱动程序，或者您使用的是 ODBC 版本 1.3.7.1000 或 JDBC 版本 1.2.8.1005 之前的 Amazon Redshift 驱动程序。

如果此更改影响到您的 Amazon Redshift 商业区域，那么您必须在 2017 年 10 月 23 日之前更新当前的信任根 CA 证书。Amazon Redshift 会在现在至 2017 年 10 月 23 日之间将您的集群过渡为使用 ACM 证书。该更改对您集群的性能或可用性应该影响不大或者没有任何影响。

如果此更改对 Amazon GovCloud (US)（美国）区域产生影响，则必须在 2020 年 4 月 1 日之前更新当前的信任根 CA 证书，以避免服务中断。从该日期开始，使用 SSL 加密连接来连接到 Amazon Redshift 集群的客户端需要额外的受信任的证书颁发机构 (CA)。当客户端连接到 Amazon Redshift 集群时，将使用受信任的证书颁发机构来确认该集群的身份。您需要执行相应操作来更新 SQL 客户端和应用程序，以使用包含新的受信任 CA 的更新的证书包。

> Important
>
> 2021 年 1 月 5 日，在中国区域，Amazon Redshift 正在将您的集群中的 SSL 证书替换为 Amazon Certificate Manager (ACM) 颁发的证书。如果此更改对中国（北京）区域或中国（宁夏）区域产生影响，则必须在 2021 年 1 月 5 日之前更新当前的信任根 CA 证书，以避免服务中断。从该日期开始，使用 SSL 加密连接来连接到 Amazon Redshift 集群的客户端需要额外的受信任的证书颁发机构 (CA)。当客户端连接到 Amazon Redshift 集群时，将使用受信任的证书颁发机构来确认该集群的身份。您需要执行相应操作来更新 SQL 客户端和应用程序，以使用包含新的受信任 CA 的更新的证书包。

- 使用最新的 Amazon Redshift ODBC 或 JDBC 驱动程序 (p. 220)
- 使用较早的 Amazon Redshift ODBC 或 JDBC 驱动程序 (p. 220)
- 使用其他 SSL 连接类型 (p. 221)

使用最新的 Amazon Redshift ODBC 或 JDBC 驱动程序

首选方法是使用最新的 Amazon Redshift ODBC 或 JDBC 驱动程序。从 ODBC 版本 1.3.7.1000 和 JDBC 版本 1.2.8.1005 开始的 Amazon Redshift 驱动程序可自动管理从 Amazon Redshift 自签名证书到 ACM 证书的过渡。要下载最新驱动程序，请参阅配置 ODBC 连接 (p. 207)或为 Amazon Redshift 配置 JDBC 驱动程序版本 2.1 连接 (p. 136)。

如果您使用的是最新的 Amazon Redshift JDBC 驱动程序，最好不要使用 JVM 选项中的 `-Djavax.net.ssl.trustStore`。如果必须使用 `-Djavax.net.ssl.trustStore`，请将 Redshift 证书颁发机构包导入到它指向的信任存储库中。有关下载信息，请参阅使用 SSL 进行连接 (p. 217)。有关更多信息，请参阅将 Amazon Redshift 证书颁发机构捆绑包导入信任存储库 (p. 221)。

使用较早的 Amazon Redshift ODBC 或 JDBC 驱动程序

- 如果您的 ODBC DSN 配置了 `SSLCertPath`，请覆盖指定路径中的证书文件。
- 如果未设置 `SSLCertPath`，则请覆盖驱动程序 DLL 位置中名为 `root.crt` 的证书文件。

如果必须使用版本 1.2.8.1005 之前的 Amazon Redshift JDBC 驱动程序，请执行以下操作之一：

- 如果您的 JDBC 连接字符串使用 `sslCert` 选项，请删除 `sslCert` 选项。然后，将 Redshift 证书颁发机构包导入到 Java 信任存储库中。有关下载信息，请参阅使用 SSL 进行连接 (p. 217)。有关更多信息，请参阅将 Amazon Redshift 证书颁发机构捆绑包导入信任存储库 (p. 221)。
- 如果您使用 Java 命令行 `-Djavax.net.ssl.trustStore` 选项，请尽量将其从命令行中删除。然后，将 Redshift 证书颁发机构包导入到 Java 信任存储库中。有关下载信息，请参阅使用 SSL 进行连接 (p. 217)。有关更多信息，请参阅将 Amazon Redshift 证书颁发机构捆绑包导入信任存储库 (p. 221)。

将 Amazon Redshift 证书颁发机构捆绑包导入信任存储库

您可以使用 `redshift-keytool.jar` 将 Amazon Redshift 证书颁发机构包中的 CA 证书导入 Java 信任存储库或您的私有信任存储库中。

要将 Amazon Redshift 证书颁发机构捆绑包导入信任存储库

1. 下载 redshift-keytool.jar。
2. 请执行下列操作之一：
   - 要将 Amazon Redshift 证书颁发机构捆绑包导入 Java 信任存储库中，请运行以下命令。

     ```
     java -jar redshift-keytool.jar -s
     ```

   - 要将 Amazon Redshift 证书颁发机构捆绑包导入您的私有信任存储库中，请运行以下命令：

     ```
     java -jar redshift-keytool.jar -k <your_private_trust_store> -p <keystore_password>
     ```

使用其他 SSL 连接类型

如果您使用以下任何方式进行连接，请执行本部分中的步骤：

- 开源 ODBC 驱动程序
- 开源 JDBC 驱动程序
- psql 命令行界面
- 基于 libpq 的任何语言绑定，如 psycopg2 (Python) 和 ruby-pg (Ruby)

将 ACM 证书与其他 SSL 连接类型结合使用：

1. 下载 Amazon Redshift 证书颁发机构捆绑包。有关下载信息，请参阅使用 SSL 进行连接 (p. 217)。
2. 将包中的证书放入您的 `root.crt` 文件中。
   - 在 Linux 和 macOS X 操作系统中，该文件为 `~/.postgresql/root.crt`。
   - 在 Microsoft Windows 上，该文件为 `%APPDATA%\postgresql\root.crt`。

通过客户端工具和代码连接到集群

如果您尚且没有商业智能工具可供您连接到集群，则可使用此部分中针对第三方工具提供的一些选项进行连接。另外，此部分还介绍了如何以编程方式连接到您的集群。

主题

- Amazon Redshift SQL (p. 222)
- 使用 SQL Workbench/J 连接到集群 (p. 250)

- 使用 psql 工具连接到集群 (p. 254)
- 以编程方式连接到集群 (p. 258)
- 使用身份验证配置文件连接到 Amazon Redshift (p. 261)

Amazon Redshift SQL

Amazon Redshift RSQL 是一个命令行客户端，用于与 Amazon Redshift 集群和数据库进行交互。您可以连接到 Amazon Redshift 集群、描述数据库对象、查询数据以及查看各种输出格式的查询结果。

Amazon Redshift RSQL 支持 PostgreSQL psql 命令行工具的功能以及特定于 Amazon Redshift 的额外功能。这些功能包括：

- 您可以使用 ADFS、PingIdentity、Okta、Azure ADm 或其他基于 SAML/JWT 的身份提供者实现单点登录身份验证。您还可以使用基于浏览器的 SAML 身份提供者进行多重身份验证（MFA）。
- 您可以描述 Amazon Redshift 对象的特性或属性，例如表分发键、表排序键、后期绑定视图（LBV）和具体化视图。您还可以描述 Amazon Glue 目录或 Apache Hive Metastore 中外部表的特性或属性、Amazon RDS for PostgreSQL、Amazon Aurora PostgreSQL 兼容版、RDS for MySQL（预览版）和 Amazon Aurora MySQL 兼容版（预览版）中的外部数据库，以及使用 Amazon Redshift 数据共享共享的表。
- 您还可以使用增强的控制流命令，例如 `IF`（`\ELSEIF`、`\ELSE`, `\ENDIF`）`\GOTO` 和 `\LABEL`。

借助 Amazon Redshift RSQL 批处理模式（运行作为输入参数传递的脚本），您可以运行包含 SQL 和复杂业务逻辑的脚本。如果您有现有的自我管理的本地数据仓库，您可以使用 Amazon Redshift RSQL 替换现有的提取、传输、加载（ETL）和自动化脚本，例如 Teradata BTEQ 脚本。使用 RSQL 有助于避免以过程语言手动重新实现脚本。

Amazon Redshift RSQL 适用于 Linux、Windows 和 macOS X 操作系统。

如需报告 Amazon Redshift RSQL 的问题，请发送邮件至 `<redshift-rsql-support@amazon.com>`。

Amazon Redshift RSQL 入门

在具有 Linux、macOS 或微软 Windows 操作系统的计算机上安装 Amazon Redshift RSQL。

先决条件

Linux：

1. 使用以下命令安装驱动程序：

   ```
   sudo yum install unixODBC openssl
   ```

   Linux 发行版需要 OpenSSL。OpenSSL 库位于 Linux OpenSSL GitHub 存储库中。有关 OpenSSL 的更多信息，请参阅 OpenSSL。
2. 安装 ODBC 驱动程序：在 Linux 操作系统上安装 Amazon Redshift 驱动程序 (p. 210)。
3. 将 ini 文件复制到您的主目录：

   ```
   cp /opt/amazon/redshiftodbc/Setup/odbc.ini ~/.odbc.ini
   ```
4. 将环境变量设置为指向文件的位置：

   ```
   export ODBCINI=~/.odbc.ini
   export ODBCSYSINI=/opt/amazon/redshiftodbc/Setup
   export AMAZONREDSHIFTODBCINI=/opt/amazon/redshiftodbc/lib/64/amazon.redshiftodbc.ini
   ```

   有关配置 ODBC 环境变量的更多信息，请参阅配置环境变量 (p. 215)。

Mac OSX：

1. 使用以下命令安装驱动程序：

```
brew install unixodbc openssl@1.1 --build-from-source
```

2. 安装 ODBC 驱动程序：在 macOS X 上安装 Amazon Redshift ODBC 驱动程序 (p. 211)。
3. 将 ini 文件复制到您的主目录：

```
cp /opt/amazon/redshift/Setup/odbc.ini ~/.odbc.ini
```

4. 将环境变量设置为指向文件的位置：

```
export ODBCINI=~/.odbc.ini
export ODBCSYSINI=/opt/amazon/redshift/Setup
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshift/lib/amazon.redshiftodbc.ini
```

   有关配置 ODBC 环境变量的更多信息，请参阅配置环境变量 (p. 215)。
5. 如果它不在`/usr/local/lib` 中，则将 `DYLD_LIBRARY_PATH` 设置为 libodbc.dylib 的位置。

```
export DYLD_LIBRARY_PATH=$DYLD_LIBRARY_PATH:/usr/local/lib
```

Windows:

请按照 在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 208) 中的说明安装驱动程序。Windows 不需要驱动程序管理器。

Windows 上的 Amazon Redshift RSQL 需要 OpenSSL。Windows OpenSSL 库位于 Windows OpenSSL GitHub 存储库中。有关 OpenSSL 的更多信息，请参阅 OpenSSL。

下载 RSQL

- Linux 64 位 RPM：RSQL 版本 1.0.5。在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.5 rpm 文件
- Mac OS 64 位 DMG：RSQL 版本 1.0.5。在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.5 dmg 文件
- Windows 64 位 MSI：RSQL 版本 1.0.5。在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.5 msi 文件

请在 Amazon Redshift RSQL 更改日志 (p. 224)中参阅以前版本的更改日志和下载。

安装 RSQL

根据您的操作系统选择步骤。

- Linux：

```
sudo rpm -i AmazonRedshiftRsql-<version>-1.x86_64.rpm
```

- Mac OS：

  1. 双击 dmg 文件以挂载磁盘镜像。
  2. 双击 pkg 文件运行安装程序。
  3. 按照安装向导中的步骤完成安装。同意许可协议条款。

- Windows:

  1. 双击该文件以运行安装程序。
  2. 按照提示完成安装。

Amazon Redshift RSQL 更改日志

1.0.5（2022 年 6 月 27 日）

错误修复

- 将 SQL 错误消息发送到标准错误 (stderr)。
- 修复了使用 ON_ERROR_STOP 时退出代码的问题。现在，脚本将在遇到错误后终止，并返回正确的退出代码。
- Maxerror 现在不区分大小写。

New

- 增加了对 ODBC 2.x 驱动程序的支持。

1.0.4 (2022-03-19)

- 添加对 RSPASWORD 环境变量的支持。设置密码以连接到 Amazon Redshift。例如：`export RSPASSWORD=TestPassw0rd`。

1.0.3（2021 年 12 月 8 日）

错误修复

- 修复了在 Windows 操作系统中使用 `\c` 或 `\logon` 切换数据库时弹出的对话框。
- 修复了检查 ssl 信息时发生的崩溃。

1.0.2（2021 年 11 月 26 日）

错误修复

- 修复了使用 IAM 身份验证时提示超级用户的问题。
- 修复了运行不返回任何行的查询时不正确的“Failed”状态消息。
- 修复了在 DSN 文件中使用 SingleRowMode 时发生的崩溃。

New

- 帮助内容增加了 DSN 连接选项。

Amazon Redshift RSQL 的以前版本

请根据您的操作系统，选择其中一个链接以下载所需的 Amazon Redshift RSQL 版本。

Linux 64 位 RPM

- RSQL 版本 1.0.4。在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.4 rpm 文件

- RSQL 版本 1.0.3在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.3
- RSQL 版本 1.0.2在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.2
- RSQL 版本 1.0.1在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.1

Mac OS 64 位 DMG

- RSQL 版本 1.0.4在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.4
- RSQL 版本 1.0.3在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.3
- RSQL 版本 1.0.2在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.2
- RSQL 版本 1.0.1在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.1

Windows 64 位 MSI

- RSQL 版本 1.0.4。在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.4 msi 文件
- RSQL 版本 1.0.3在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.3
- RSQL 版本 1.0.2在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.2
- RSQL 版本 1.0.1在中国（北京）区域，使用以下链接：64 位 RSQL 版本 1.0.1

使用 Amazon Redshift RSQL 连接到集群

在没有 DSN 的情况下连接

1. 在 Amazon Redshift 控制台上，选择要连接到的集群，然后记下端点、数据库和端口。
2. 在命令提示符下，使用命令行参数指定连接信息。

```
rsql -h <endpoint> -U <username> -d <databasename> -p <port>
```

在这里，以下内容适用：

- *<endpoint>* 是您在上一步中记录的 Endpoint（端点）。
- *<userid>* 是有权连接到集群的用户。
- *<databasename>* 是您在上一步中记录的 Database Name（数据库名称）。
- *<port>* 是您在上一步中记录的 Port（端口）。*<port>* 是一个可选参数，默认值为 5439。

以下为示例。

```
rsql -h testcluster.example.amazonaws.com -U user1 -d dev -p 5439
```

3. 在密码提示符处，输入 *<username>* 用户的密码。

成功的连接响应如下所示。

```
% 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=#
```

要连接的命令在 Linux、Mac OS 和 Windows 上具有相同的参数。

使用 DSN 进行连接

您可以使用数据源名称（DSN）将 RSQL 连接到 Amazon Redshift，以简化连接属性的组织。有关更多信息，请参阅配置连接功能 (p. 215)。本主题包括 ODBC 驱动程序安装说明以及 DSN 属性的说明。

使用带密码的 DSN 连接

下面显示使用密码的 DSN 连接配置的示例。对于 Mac OSX 而言，默认 `<path to driver>` 为 `/opt/amazon/redshift/lib/libamazonredshiftodbc.dylib`，对于 Linux 而言，则为 `/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
```

连接成功后，输出结果如下。

```
% 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=#
```

使用单点登录 DSN

您可以配置 DSN 以进行单点登录身份验证。下面显示使用 Okta 单点登录的 DSN 连接配置的示例。

```
[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>
```

成功连接的输出示例。

```
% 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=#
```

下面显示使用 Azure 单点登录的 DSN 连接配置的示例。

```
[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>
```

将 DSN 连接与 IAM 配置文件结合使用

您可以使用配置的 IAM 配置文件连接到 Amazon Redshift。IAM 配置文件必须具有调用 `GetClusterCredentials` 的权限。以下示例演示了要使用的 DSN 属性。仅当 `Host` 不是 Amazon 提供的端点（如 `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`）时，才需要 `ClusterID` 和 `Region` 参数。

```
[testiam]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Profile=default
```

`Profile` 密钥的值是您从 Amazon CLI 凭证中选择的命名配置文件。此示例显示名为 `default` 的配置文件的凭证。

```
$ cat .aws/credentials
[default]
aws_access_key_id = ASIAIOSFODNN7EXAMPLE
```

```
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

下面显示的是连接响应。

```
$ 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=>
```

将 DSN 连接与实例配置文件结合使用

您可以使用 Amazon EC2 实例配置文件连接到 Amazon Redshift。实例配置文件必须具有调用 `GetClusterCredentials` 的权限。有关要使用的 DSN 属性，请参阅下面的示例。仅当 `Host` 不是 Amazon 提供的端点（如 `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`）时，才需要 `ClusterID` 和 `Region` 参数。

```
[testinstanceprofile]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Instanceprofile=1
```

下面显示的是连接响应。

```
$ 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=>
```

将 DSN 连接与原定设置凭证提供程序链结合使用

要使用原定设置凭证提供程序链进行连接，请仅指定 IAM 属性，Amazon Redshift RSQL 将尝试按照适用于 Java 的 Amazon SDK 中使用 Amazon 凭证所述的顺序获取凭证。链中必须至少一个提供程序具有 `GetClusterCredentials` 权限。例如，这对于从 ECS 容器进行连接非常有用。

```
[iamcredentials]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
```

Amazon Redshift RSQL 元命令

Amazon Redshift RSQL 元命令返回有关数据库或特定数据库对象的信息性记录。结果可以包括各种列和元数据。其他命令会执行特定操作。这些命令的前面都有反斜杠。

\d[S+]

列出本地用户创建的表、常规视图、后期绑定视图和具体化视图。`\dS` 还列出了表和视图，如 `\d`，但系统对象包含在返回的记录中。`+` 为所有列出的对象生成额外的元数据列 `description`。下面显示的是作为命令返回的示例记录。

```
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

描述表、视图或索引。包括列名称和类型。它还提供了 diststyle、备份配置、创建日期（2018 年 10 月之后创建的表）和约束。例如，`\dS+ sample` 返回对象属性。附加 `S+` 会导致返回的记录中包含其它列。

```
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)
```

表的分布样式或 Diststyle 可以是 KEY、AUTO、EVEN 或 ALL。

Backup（备份）指示在拍摄快照时是否备份了表。有效值为 `YES` 或 `NO`。

Created（已创建）是创建表的时间的时间戳。创建日期不适用于 2018 年 11 月之前创建的 Amazon Redshift 表。在此日期之前创建的表显示 n/a（不可用）。

Unique Constraints（独特约束）列出了表中的唯一的主键约束。

Foreign-key constraints（外键约束）列出了表中的外键越塾。

\dC[+] [PATTERN]

列出转换。包括源类型、目标类型以及转换是否为隐式。

以下显示来自 \dC+ 的结果子集：

```
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]

显示在别处未显示的对象描述。

\de

列出外部表。这包括 Amazon Glue 数据目录中的表、Hive Metastore 和来自 Amazon RDS/Aurora MySQL、Amazon RDS/Aurora PostgreSQL 和 Amazon Redshift 数据共享表的联合表。

\de NAME

描述外部表。

以下示例显示 Amazon Glue 外部表。

```
# \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"}
```

Hive Metastore 表。

```
# \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"}
```

PostgreSQL 外部表。

```
# \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]

列出各种类型的函数。例如，命令 `\df` 返回函数列表。结果包括名称、返回的数据类型、访问权限和其它元数据等属性。函数类型可以包括触发器、存储过程、窗口函数和其它类型。当您将 `S+` 附加到命令（例如 `\dfantS+`）时，会包含其它元数据列，例如 `owner`、`security` 和 `access privileges`。

\dL[S+] [PATTERN]

列出与数据库关联的过程语言的数据。信息包括名称（例如 plpgsql）和其它元数据，其中包括名称是否受信任、访问权限和描述。例如，示例调用是 `\dLS+`，它列出了语言及其属性。当您将 `S+` 附加到命令时，会包含其它元数据列，例如 `call handler` 和 `access privileges`。

示例结果：

```
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]

列出具体化视图。例如，\dmS+ 列出了具体化视图及其属性。当您将 S+ 附加到命令时，会包含其它元数据列。

\dn[S+] [PATTERN]

列出架构。当您将 S+ 附加到命令（例如 \dnS+）时，会包含其它元数据列，例如 description 和 access privileges。

\dp [PATTERN]

列出表、视图和序列访问权限。

\dt[S+] [PATTERN]

列出表 当您将 S+ 附加到命令（例如 \dtS+）时，会包含其它元数据列，例如本例中的 description。

\du

列出数据库的用户。包括他们的姓名和角色，例如超级用户和属性。

\dv[S+] [PATTERN]

列出视图。包括架构、类型和拥有者数据。当您将 S+ 附加到命令（例如 \dvS+）时，会包含其它元数据列。

\H

打开 HTML 输出。这对于快速返回格式化的结果非常有用。例如，select * from sales; \H 以 HTML 格式返回销售表中的结果。要切换回表格结果，请使用 \q，或者无提示。

\i

从文件中运行命令。例如，假设您的工作目录中有 rsql_steps.sql，以下将运行文件中的命令：\i rsql_steps.sql。

\l[+] [PATTERN]

列出数据库。包括所有者、编码和其它信息。

\q

退出，或者 \q 命令，注销数据库会话并退出 RSQL。

\sv[+] VIEWNAME

显示视图的定义。

\timing

例如，显示查询的运行时间。

\z [PATTERN]

输出与\ dp 相同。

\?

显示帮助信息。可选的参数指定要解释的项目。

\EXIT

注销所有数据库会话并退出 Amazon Redshift RSQL。此外，您可以指定可选的退出代码。例如，\EXIT 15 将退出 Amazon Redshift RSQL 终端并返回退出代码 15。

以下示例显示来自连接的输出并从 RSQL 退出。

```
% 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

指定导出文件的名称，RSQL 将该文件用于存储后续 SQL SELECT 语句返回的数据库信息。

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
```

控制台输出

```
Rformat is off.
```

```
Target width is 1500.
Heading is set to: General Title
Titledashes is on.
(exported 40 rows)
```

\LOGON

连接到数据库。您可以使用位置语法指定连接参数或将其指定作为连接字符串。

命令语法如下所示：`\logon {[DBNAME|- USERNAME|- HOST|- PORT|- [PASSWORD]] | conninfo}`

`DBNAME` 是要连接的数据库的名称。`USERNAME` 是连接的用户名。默认 `HOST` 为 `localhost`。默认 `PORT` 为 `5439`。

当在 `\LOGON` 命令中指定主机名时，它将成为其它 `\LOGON` 命令的默认主机名。要更改默认主机名，请在附加 `\LOGON` 命令中指定新的 `HOST`。

`user1` 的 `\LOGON` 命令输出示例如下。

```
(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=#
```

user2 的示例输出。

```
(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

`\echo` 命令的扩展。`\REMARK` 将指定的字符串打印到输出流。`\REMARK` 通过添加在单独的行上中断输出的能力来扩展 `\echo`。

以下示例显示了命令的输出。

```
(testcluster) user1@dev=# \remark 'hello//world'
hello
world
```

\RSET

该 `\rset` 命令将设置命令参数和变量。`\rset` 还具有交互式模式和批处理模式。它不支持 bash 选项（例如 -x）或参数（例如 --<arg>）。

它设置如下所示的变量：

- ERRORLEVEL

- HEADING 和 RTITLE
- RFORMAT
- MAXERROR
- TITLEDASHES
- WIDTH

以下示例指定一个标题。

```
\rset heading "Winter Sales Report"
```

有关如何使用 \rset 的更多示例，您可以在 Amazon Redshift RSQL 变量 (p. 239) 主题中查找示例。

\RUN

运行包含在指定文件中的 Amazon Redshift RSQL 脚本。\RUN 通过添加一个选项来跳过文件中的标题行以扩展 \i 命令。

如果文件名包含逗号、分号或空格，请用单引号将其括起来。此外，如果文本在文件名后面，请将其括在引号中。在 UNIX 中，文件名区分大小写。在 Windows 中，文件名不区分大小写。

以下示例显示了命令的输出。

```
(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

\! 命令的别名。\OS 运行作为参数传递的操作系统命令。命令运行后，控制将返回到 Amazon Redshift RSQL。例如，您可以运行以下命令以打印当前系统日期时间并返回到 RSQL 终端：\os date。

```
(testcluster) user1@dev=# \os date
```

```
Tue Sep 7 20:47:54 UTC 2021
```

\GOTO

适用于 Amazon Redshift RSQL 的新命令。\GOTO 跳过所有干预命令并在指定的 \LABEL 继续处理。\LABEL 必须是前向引用。您不能跳转到词汇上位于 \GOTO 之前的 \LABEL。

下面显示了示例输出。

```
(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

适用于 Amazon Redshift RSQL 的新命令。\LABEL 建立运行程序的入口点，作为 \GOTO 命令的目标。

以下显示了命令的输出。

```
(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 和相关命令有条件地运行部分输入脚本。PSQL \if (\elif、\else、\endif) 命令的扩展。\IF 和 \ELSEIF 支持布尔表达式，包括 AND、OR 和 NOT 条件。

以下显示了命令的示例输出。

```
(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
```

在您的分支逻辑中使用 ERRORCODE。

```
\if :'ERRORCODE' = '00000'
    \remark 'The statement was executed without error'
\else
    \remark :LAST_ERROR_MESSAGE
\endif
```

在 \IF 块内使用 \GOTO 以控制代码的运行方式。

Amazon Redshift RSQL 变量

有些关键字在 RSQL 中充当变量。您可以将每个值设置为特定值，也可以重新设置值。大多数值都由 \rset 设置，它具有交互式模式和批处理模式。命令可以用小写或大写定义。

ACTIVITYCOUNT

指示受上次提交的请求影响的行数。对于数据返回请求，这是从数据库返回到 RSQL 的行数。该值为 0 或正整数。最大值为 18,446,744,073,709,551,615。

经过特殊处理的变量 ACTIVITYCOUNT 类似于变量 ROW_COUNT。但是，在命令完成时，ROW_COUNT 不会向客户端应用程序报告受影响的 SELECT、COPY 或 UNLOAD 行数。而 ACTIVITYCOUNT 会报告相关行数。

activitycount_01.sql：

```
select viewname, schemaname
from pg_views
where schemaname = 'not_existing_schema';
\if :ACTIVITYCOUNT = 0
\remark 'views do not exist'
\endif
```

控制台输出：

```
viewname | schemaname
----------+------------
(0 rows)
```

```
views do not exist
```

ERRORLEVEL

为错误分配严重性级别。使用严重性级别来确定适当操作。如果尚未使用 ERRORLEVEL 命令，那么默认情况下，它的值为 ON。

errorlevel_01.sql：

```
\rset errorlevel 42P01 severity 0

select * from tbl;

select 1 as col;

\echo exit
\quit
```

控制台输出：

```
Errorlevel is on.
rsql: ERROR: relation "tbl" does not exist
(1 row)

col
1

exit
```

HEADING 和 RTITLE

允许用户指定显示在报告顶部的标题。使用 RSET RTITLE 命令指定的标题会自动包含客户端电脑的当前系统日期。

rset_head _rtitle_02.rsql 内容：

```
\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...
```

控制台输出：

```
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

指定 RSQL 终止任务处理的最大错误严重性级别。在完成每个作业或任务后，返回代码是 RSQL 返回到客户端操作系统的整数值。返回代码的值表示作业或任务的完成状态。如果脚本包含生成错误严重性级别大于指定 `maxerror` 值的语句，RSQL 将立即退出。因此，要将 RSQL 退出的错误严重性级别设为 8，请使用 `RSET MAXERROR 7`。

maxerror_01.sql 内容：

```
\rset maxerror 0

select 1 as col;

\quit
```

控制台输出：

```
Maxerror is default.
(1 row)

col
1
```

RFORMAT

允许用户指定是否应用格式化命令的设置。

rset_rformat.rsql 内容：

```
\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...
```

控制台输出：

```
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

获取受以前查询影响的记录数。它通常用于检查结果，如以下代码片段所示：

```
SET result = ROW_COUNT;

IF result = 0
...
```

TITLEDASHES

使用此控件，用户可以指定是否要在为 SQL 语句返回的列数据的上方打印一行破折号字符。

示例：

```
\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;
```

控制台输出：

```
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

将输出格式设置为换行并指定报告中每行的目标宽度。如果没有参数，它将返回格式和目标宽度的当前设置。

rset_width_01.rsql 内容：

```
\echo Starting...
\rset width
\rset width 50
\rset width
\quit
\echo Finishing...
```

控制台输出：

```
Starting...
Target width is 75.
Target width is 50.
Target width is 50.
Press any key to continue . . .
```

使用参数的示例：

```
\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...
```

控制台输出：

```
Starting...
Rformat is on.
Output format is wrapped.
id  |                                          long_string
500 | In general, the higher the number the more borders and lines the ta.
    |.bles will have, but details depend on the particular format.
(1 row)

Target width is 50.
id  |                                          long_string
500 | In general, the higher the number the more.
    |. borders and lines the tables will have, b.
    |.ut details depend on the particular format.
    |..
(1 row)
Press any key to continue . . .
```

Amazon Redshift RSQL 错误代码

成功消息、警告和异常：

错误代码	错误类	条件名称
00000	00 类：成功完成	successful_completion
01000	01 类：警告	warning
0100C	01 类：警告	dynamic_result_sets_returned
01008	01 类：警告	implicit_zero_bit_padding
01003	01 类：警告	null_value_eliminated_in_set_function
01007	01 类：警告	privilege_not_granted
01006	01 类：警告	privilege_not_revoked
01004	01 类：警告	string_data_right_truncation
01P01	01 类：警告	deprecated_feature
02000	02 类：无数据	no_data
02001	02 类：无数据	no_additional_dynamic_result_sets_returned
03000	03 类：SQL 语句尚未结束	sql_statement_not_yet_complete
08000	08 类：连接异常	connection_exception
08003	08 类：连接异常	connection_does_not_exist
08006	08 类：连接异常	connection_failure
08001	08 类：连接异常	sqlclient_unable_to_establish_sqlconnection
08004	08 类：连接异常	sqlserver_rejected_establishment_of_sqlconnection
08007	08 类：连接异常	transaction_resolution_unknown
08P01	08 类：连接异常	protocol_violation
09000	09 类：已触发的操作异常	triggered_action_exception
0A000	0A 类：功能不受支持	feature_not_supported
0A000	0A 类：功能不受支持	feature_not_supported
0B000	0B 类：事务启动无效	invalid_transaction_initiation
0F000	0F 类：定位器异常	locator_exception
0F001	0F 类：定位器异常	invalid_locator_specification
0L000	0L 类：授予者无效	invalid_grantor
0LP01	0L 类：授予者无效	invalid_grant_operation
0P000	0P 类：角色规范无效	invalid_role_specification
0Z000	0Z 类：诊断异常	diagnostics_exception

错误代码	错误类	条件名称
0Z002	0Z 类：诊断异常	stacked_diagnostics_accessed_without_active_handler
20000	20 类：未找到案例	case_not_found
21000	21 类：基数违规	cardinality_violation

数据异常：

错误代码	错误类	条件名称
22000	22 类：数据异常	data_exception
2202E	22 类：数据异常	array_subscript_error
22021	22 类：数据异常	character_not_in_repertoire
22008	22 类：数据异常	datetime_field_overflow
22012	22 类：数据异常	division_by_zero
22005	01 类：警告	error_in_assignment
2200B	01 类：警告	escape_character_conflict
22022	01 类：警告	indicator_overflow
22015	01 类：警告	interval_field_overflow
2201E	01 类：警告	invalid_argument_for_logarithm
2201F	01 类：警告	invalid_argument_for_power_function
2201G	01 类：警告	invalid_argument_for_width_bucket_function
22018	01 类：警告	invalid_character_value_for_cast
22007	01 类：警告	invalid_datetime_format
22019	01 类：警告	invalid_escape_character
2200D	01 类：警告	invalid_escape_octet
22025	01 类：警告	invalid_escape_sequence
22P06	01 类：警告	nonstandard_use_of_escape_character
22010	01 类：警告	invalid_indicator_parameter_value
22023	01 类：警告	invalid_parameter_value
2201B	01 类：警告	invalid_regular_expression
22009	01 类：警告	invalid_time_zone_displacement_value
2200C	01 类：警告	invalid_use_of_escape_character
2200G	01 类：警告	most_specific_type_mismatch
22004	01 类：警告	null_value_not_allowed

错误代码	错误类	条件名称
22002	01 类：警告	null_value_no_indicator_parameter
22003	01 类：警告	numeric_value_out_of_range
22026	01 类：警告	string_data_length_mismatch
22001	01 类：警告	string_data_right_truncation
22011	01 类：警告	substring_error
22027	01 类：警告	trim_error
22024	01 类：警告	unterminated_c_string
2200F	01 类：警告	zero_length_character_string
22P01	01 类：警告	floating_point_exception
22P02	01 类：警告	invalid_text_representation
22P03	01 类：警告	invalid_binary_representation
22P04	01 类：警告	bad_copy_file_format
22P05	01 类：警告	untranslatable_character

违反完整性约束：

错误代码	错误类	条件名称
23000	23 类：违反完整性约束	integrity_constraint_violation
23001	23 类：违反完整性约束	restrict_violation
23502	23 类：违反完整性约束	not_null_violation
23503	23 类：违反完整性约束	foreign_key_violation
23505	23 类：违反完整性约束	unique_violation
23514	23 类：违反完整性约束	check_violation
24000	24 类：游标状态无效	invalid_cursor_state
01004	01 类：警告	string_data_right_truncation
25000	25 类：事务状态无效	invalid_transaction_state
25001	25 类：事务状态无效	active_sql_transaction
25002	25 类：事务状态无效	invalid_transaction_state
25008	25 类：事务状态无效	held_cursor_requires_same_isolation_level
25003	25 类：事务状态无效	inappropriate_access_mode_for_branch_transaction
25004	25 类：事务状态无效	inappropriate_isolation_level_for_branch_transaction
25005	25 类：事务状态无效	no_active_sql_transaction_for_branch_transaction

错误代码	错误类	条件名称
25006	25 类：事务状态无效	read_only_sql_transaction
25007	25 类：事务状态无效	no_active_sql_transaction_for_branch_transaction
25P01	25 类：事务状态无效	no_active_sql_transaction
25P02	25 类：事务状态无效	in_failed_sql_transaction
26000	26 类：SQL 语句名称无效	invalid_sql_statement_name
28000	28 类：授权规范无效	invalid_authorization_specification
2B000	2B 类：关联权限描述符依然存在	dependent_privilege_descriptors_still_exist
2BP01	2B 类：关联权限描述符依然存在	dependent_objects_still_exist
2D000	2D 类：事务终止无效	invalid_transaction_termination
2F000	2F 类：SQL 例程异常	sql_routine_expection
2F005	2F 类：SQL 例程异常	function_executed_no_return_statement
2F002	2F 类：SQL 例程异常	modifying_sql_data_not_permitted
2F003	2F 类：SQL 例程异常	prohibited_sql_statement_attempted
2F004	2F 类：SQL 例程异常	reading_sql_data_not_permitted
34000	34 类：游标名称无效	invalid_cursor_name
38000	38 类：外部例程异常	external_routine_exception
38001	38 类：外部例程异常	containing_sql_not_permitted
38002	38 类：外部例程异常	modifying_sql_data_not_permitted
38003	38 类：外部例程异常	prohibited_sql_statement_attempted
38004	38 类：外部例程异常	reading_sql_data_not_permitted
39000	39 类：外部例程调用异常	external_routine_invocation_exception
39001	39 类：外部例程调用异常	invalid_sqlstate_returned
39004	39 类：外部例程调用异常	null_value_not_allowed
39P01	39 类：外部例程调用异常	trigger_protocol_violated
39P02	39 类：外部例程调用异常	srf_protocol_violated
3D000	3D 类：目录名称无效	invalid_catalog_name
3F000	3F 类：架构名称无效	invalid_schema_name
42000	42 类：语法错误或访问规则冲突	syntax_error_or_access_rule_violation
42601	42 类：语法错误或访问规则冲突	syntax_error
42501	42 类：语法错误或访问规则冲突	insufficient_privilege
42846	42 类：语法错误或访问规则冲突	cannot_coerce

错误代码	错误类	条件名称
42803	42 类：语法错误或访问规则冲突	grouping_error
42830	42 类：语法错误或访问规则冲突	invalid_foreign_key
42602	42 类：语法错误或访问规则冲突	invalid_name
42622	42 类：语法错误或访问规则冲突	name_too_long
42939	42 类：语法错误或访问规则冲突	reserved_name
42804	42 类：语法错误或访问规则冲突	datatype_mismatch
42P18	42 类：语法错误或访问规则冲突	indeterminate_datatype
42809	42 类：语法错误或访问规则冲突	wrong_object_type
42703	42 类：语法错误或访问规则冲突	undefined_column
42883	42 类：语法错误或访问规则冲突	undefined_function
42P01	42 类：语法错误或访问规则冲突	undefined_table
42P02	42 类：语法错误或访问规则冲突	undefined_parameter
42704	42 类：语法错误或访问规则冲突	undefined_object
42701	42 类：语法错误或访问规则冲突	duplicate_column
42P03	42 类：语法错误或访问规则冲突	duplicate_cursor
42P04	42 类：语法错误或访问规则冲突	duplicate_database
42723	42 类：语法错误或访问规则冲突	duplicate_function
42P05	42 类：语法错误或访问规则冲突	duplicate_prepared_statement
42P06	42 类：语法错误或访问规则冲突	duplicate_schema
42P07	42 类：语法错误或访问规则冲突	duplicate_table
42712	42 类：语法错误或访问规则冲突	duplicate_alias
42710	42 类：语法错误或访问规则冲突	duplicate_object
42702	42 类：语法错误或访问规则冲突	ambiguous_column
42725	42 类：语法错误或访问规则冲突	ambiguous_function
42P08	42 类：语法错误或访问规则冲突	ambiguous_parameter
42P09	42 类：语法错误或访问规则冲突	ambiguous_alias
42P10	42 类：语法错误或访问规则冲突	invalid_column_reference
42611	42 类：语法错误或访问规则冲突	invalid_column_definition
42P11	42 类：语法错误或访问规则冲突	invalid_cursor_definition
42P12	42 类：语法错误或访问规则冲突	invalid_database_definition
42P13	42 类：语法错误或访问规则冲突	invalid_function_definition

错误代码	错误类	条件名称
42P14	42 类：语法错误或访问规则冲突	invalid_prepared_statement_definition
42P15	42 类：语法错误或访问规则冲突	invalid_schema_definition
42P16	42 类：语法错误或访问规则冲突	invalid_table_definition
42P17	42 类：语法错误或访问规则冲突	invalid_object_definition
44000	44 类：WITH CHECK OPTION 违规	with_check_option_violation
53000	53 类：资源不足	insufficient_resources
53100	53 类：资源不足	disk_full
53200	53 类：资源不足	out_of_memory
53300	53 类：资源不足	too_many_connections
54000	54 类：已超出程序限制	program_limit_exceeded
54001	54 类：已超出程序限制	statement_too_complex
54011	54 类：已超出程序限制	too_many_columns
54023	54 类：已超出程序限制	too_many_arguments
55000	55 类：对象不在先决条件状态	object_not_in_prerequisite_state
55006	55 类：对象不在先决条件状态	object_in_use
55P02	55 类：对象不在先决条件状态	cant_change_runtime_param
55P03	55 类：对象不在先决条件状态	lock_not_available
57000	57 类：操作员干预	operator_intervention
57014	57 类：操作员干预	query_canceled
57P01	57 类：操作员干预	admin_shutdown
57P02	57 类：操作员干预	crash_shutdown
57P03	57 类：操作员干预	cannot_connect_now
58000	58 类：系统错误（PostgreSQL 外部的错误）	system_error
58030	58 类：系统错误（PostgreSQL 外部的错误）	io_error
58P01	58 类：系统错误（PostgreSQL 外部的错误）	undefined_file
58P02	58 类：系统错误（PostgreSQL 外部的错误）	duplicate_file
F0000	F0 类：配置文件错误	duplicate_file
F0001	F0 类：配置文件错误	lock_file_exists

错误代码	错误类	条件名称
P0000	P0 类：PL/pgSQL 错误	plpgsql_error
P0001	P0 类：PL/pgSQL 错误	raise_exception
P0002	P0 类：PL/pgSQL 错误	no_data_found
P0003	P0 类：PL/pgSQL 错误	too_many_rows
XX000	XX 类：内部错误	internal_error
XX001	XX 类：内部错误	data_corrupted
XX002	XX 类：内部错误	index_corrupted

Amazon Redshift RSQL 环境变量

Amazon Redshift RSQL 可以使用环境变量来选择默认参数值。

RSPASSWORD

Important

出于安全原因，我们不建议使用此环境变量，因为有些操作系统允许非根用户查看进程环境变量。

为 Amazon Redshift RSQL 设置连接到 Amazon Redshift 时要使用的密码。此环境变量需要 Amazon Redshift RSQL 1.0.4 及更高版本。

如果设置了 RSPASSWORD，RSQL 会优先考虑它。如果未设置 RSPASSWORD 并且您使用 DSN 进行连接，则 RSQL 将从 DSN 文件的参数中获取密码。最后，如果未设置 RSPASSWORD 且您没有使用 DSN，则 RSQL 会在尝试连接后提供密码提示。

下面为设置 RSPASSWORD 的示例：

```
export RSPASSWORD=TestPassw0rd
```

使用 SQL Workbench/J 连接到集群

Amazon Redshift 不提供或安装任何 SQL 客户端工具或库，因此您必须自行安装希望用于集群的任何工具或库。如果您已有商业智能应用程序或可使用标准 PostgreSQL JDBC 或 ODBC 驱动程序连接到集群的任何其他应用程序，则可跳过这一部分。如果您没有可连接到集群的应用程序，则可通过此部分中演示的一个选项使用 SQL Workbench/J（一款独立于 DBMS 的免费跨平台 SQL 查询工具）进行连接。

安装 SQL Workbench/J

《Amazon Redshift 入门指南》使用 SQL Workbench/J。在此部分中，我们将为您详细介绍如何使用 SQL Workbench/J 连接到集群。

安装 SQL Workbench/J

1. 查看 SQL Workbench/J 软件许可。
2. 转至 SQL Workbench/J 网站，然后将适用于您操作系统的程序包下载到您的客户端计算机或 Amazon EC2 实例上。
3. 转到安装并启动 SQL Workbench/J 页面。按照说明操作，在您的系统上安装 SQL Workbench/J。

Note

SQL Workbench/J 要求在您的系统上安装 Java 运行时环境 (JRE)。请确保您使用的 JRE 是 SQL Workbench/J 所需的正确版本。要确定系统上运行的 JRE 版本，请执行以下操作之一：

- Mac：在 System Preferences (系统首选项) 中，选择 Java 图标。
- Windows：在 Control Panel (控制面板) 中，选择 Java 图标。
- 任何系统：在命令 shell 中，键入 `java -version`。您还可以访问 https://www.java.com，选择我有 Java 吗？链接，然后选择 Verify Java (验证 Java) 按钮。

有关安装和配置 Java 运行时环境的信息，请转至 https://www.java.com。

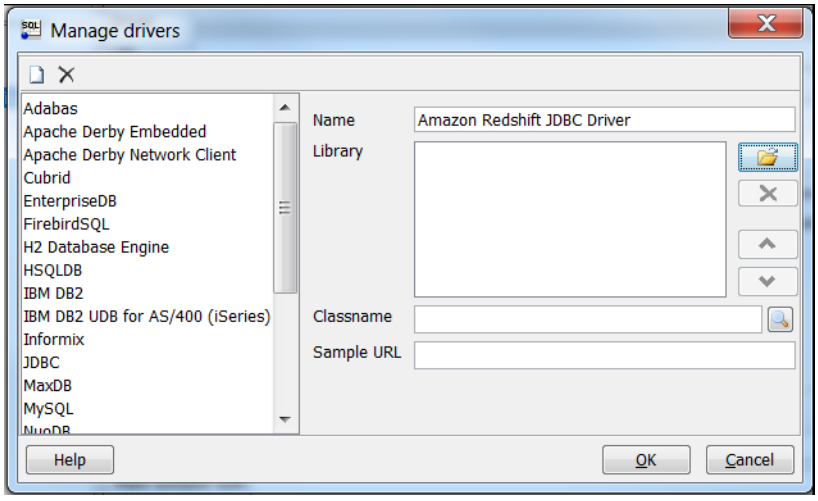
在 SQL Workbench/J 中通过 JDBC 连接到集群

Important

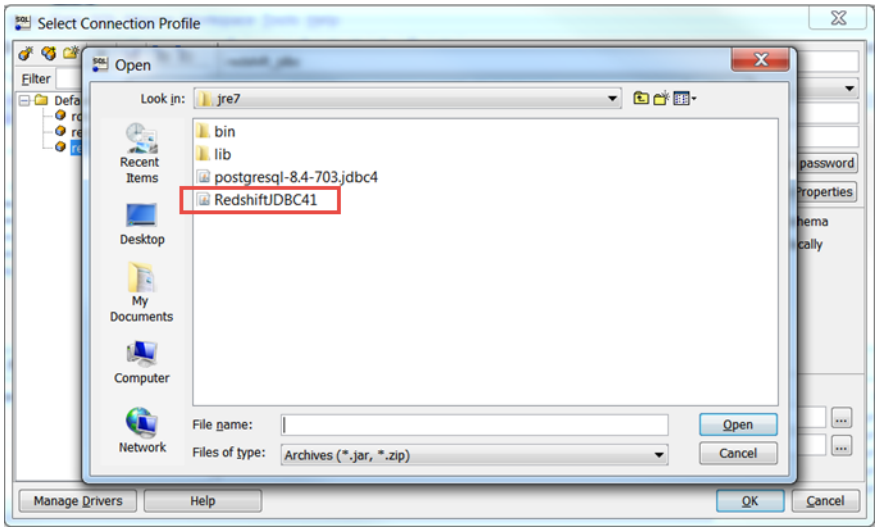
在执行此过程中的步骤之前，请确保您的客户端计算机或 Amazon EC2 实例安装了建议的 Amazon Redshift JDBC 驱动程序。有关下载最新驱动程序的链接，请参阅下载 Amazon Redshift JDBC 驱动程序版本 2.1 (p. 137)。另外，确保您已配置防火墙设置以允许访问集群。有关更多信息，请参阅步骤 4：授予集群的访问权限。

在 SQL Workbench/J 中使用 JDBC 连接

1. 打开 SQL Workbench/J。
2. 选择 File (文件)，然后选择 Connect window (连接窗口)。
3. 选择 Create a new connection profile。
4. 在 New profile 框中，键入配置文件的名称。例如，examplecluster_jdbc。
5. 选择 Manage Drivers。系统随即打开 Manage Drivers 对话框。在 Name (名称) 框中，键入驱动程序的名称。



选择 Library (库) 框旁边的文件夹图标，导航至该驱动程序所在位置，选中它，然后选择 Open (打开)。

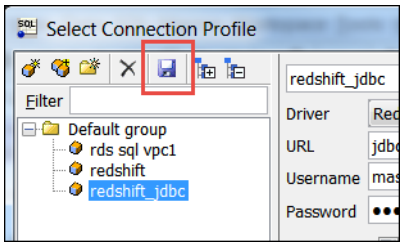


如果系统显示 Please select one driver 对话框，请选择 com.amazon.redshift.jdbc4.Driver 或 com.amazon.redshift.jdbc41.Driver，然后选择 OK。SQL Workbench/J 会自动填写 Classname 框。将 Sample URL 框留空，然后选择 OK。

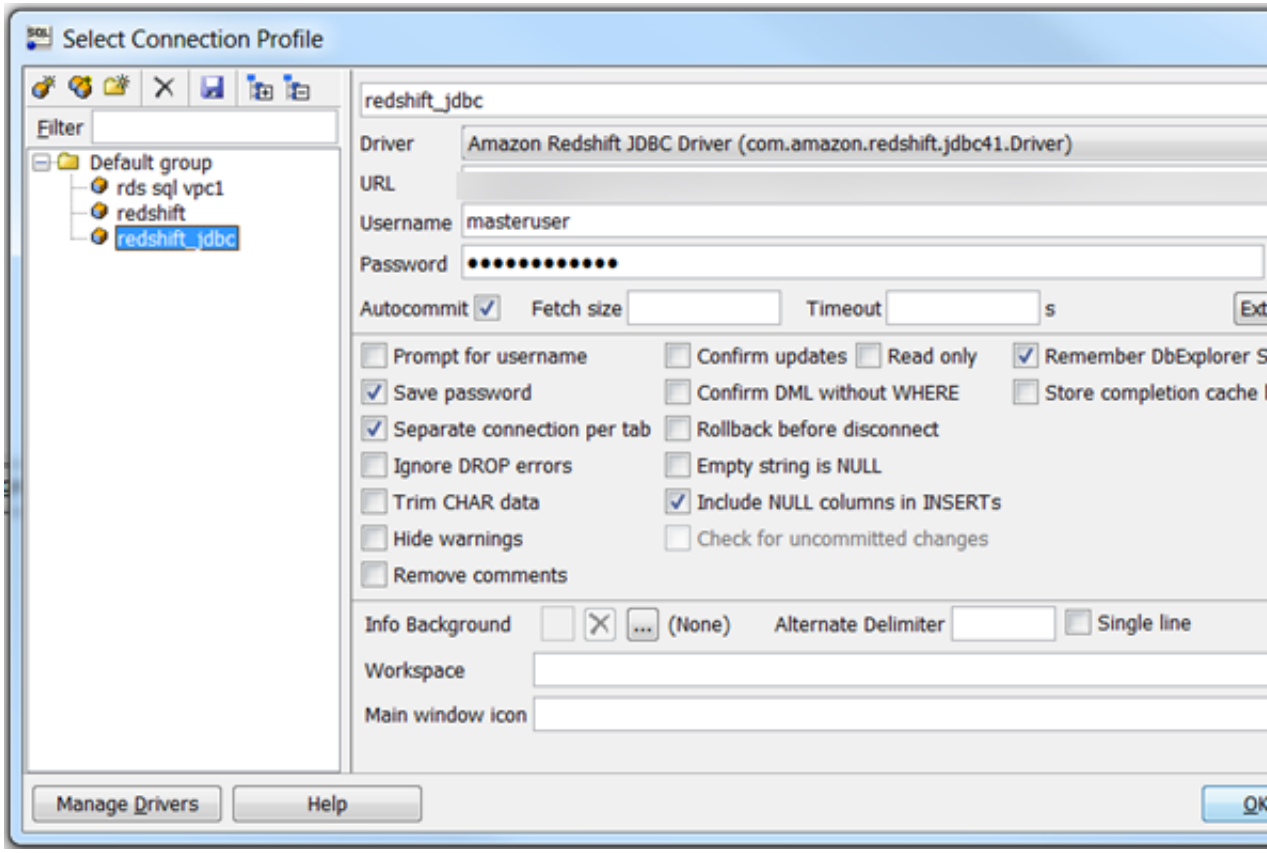
6. 在 Driver 框中，选择您刚刚添加的驱动程序。
7. 在 URL 中，从 Amazon Redshift 控制台中复制 JDBC URL 并将其粘贴到此处。

   有关查找 JDBC URL 的更多信息，请参阅为 Amazon Redshift 配置 JDBC 驱动程序版本 2.1 连接 (p. 136)。
8. 在 Username（用户名）中，键入管理员用户的名称。

   如果您正在遵循《Amazon Redshift 入门指南》，键入 *adminuser*。
9. 在 Password（密码）中，键入与管理员用户账户关联的密码。
10. 选择 Autocommit 框。
11. 选择 Save profile list 图标，如下所示：



12. 选择 OK（确定）。



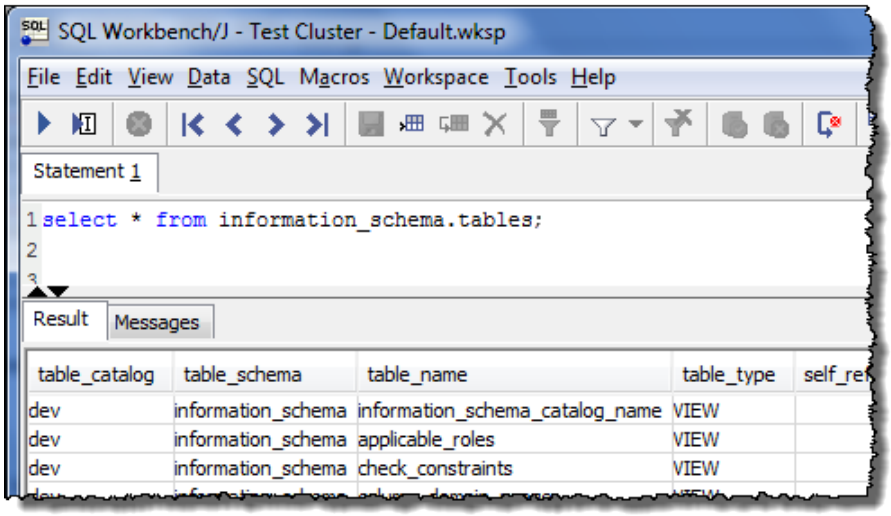
测试 SQL Workbench/J 连接

JDBC 或 ODBC 连接配置完成后，您可以通过运行查询示例测试连接。

1. 您可以使用以下查询来测试您的连接。

```
select * from information_schema.tables;
```

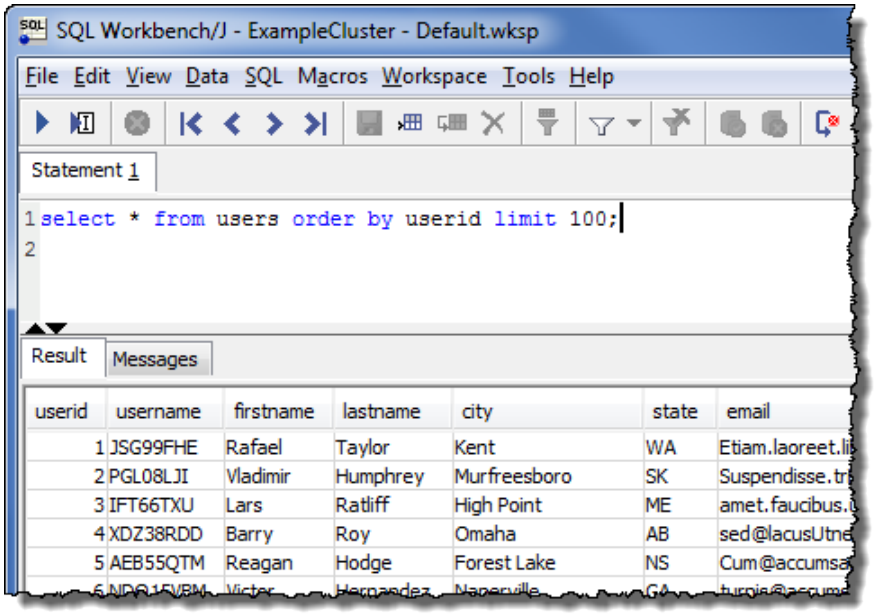
如果连接成功，Results（结果）选项卡中将显示一系列记录。



2. 或者，如果您已从 Amazon Redshift 入门指南中加载示例表和数据，则可通过在 Statement（语句）窗口中键入以下查询来测试您的连接：

```
select * from users order by userid limit 100;
```

如果连接成功，Results（结果）选项卡中将显示一系列记录。



使用 psql 工具连接到集群

创建 Amazon Redshift 集群后，您可以使用 psql 工具（PostgreSQL 中基于终端的前端）来查询集群中的数据。您能以交互方式键入查询，或从文件中读取查询。要通过 psql 进行连接，您必须指定集群端点、数据库和端口。

Note

Amazon Redshift 不提供 psql 工具；它随 PostgreSQL 一起安装。有关使用 psql 的信息，请转至 https://www.postgresql.org/docs/8.4/static/app-psql.html。有关安装 PostgreSQL 客户端工具的信息，请访问以下位置的 PostgreSQL 二进制文件下载页面并选择您的操作系统：https://www.postgresql.org/download/。
如果由于无效的 `client_encoding` 而无法从 Microsoft Windows 提示符中进行连接，请在运行 psql 之前将 `PGCLIENTENCODING` 环境变量设置为 UTF-8。

```
set PGCLIENTENCODING=UTF8
```

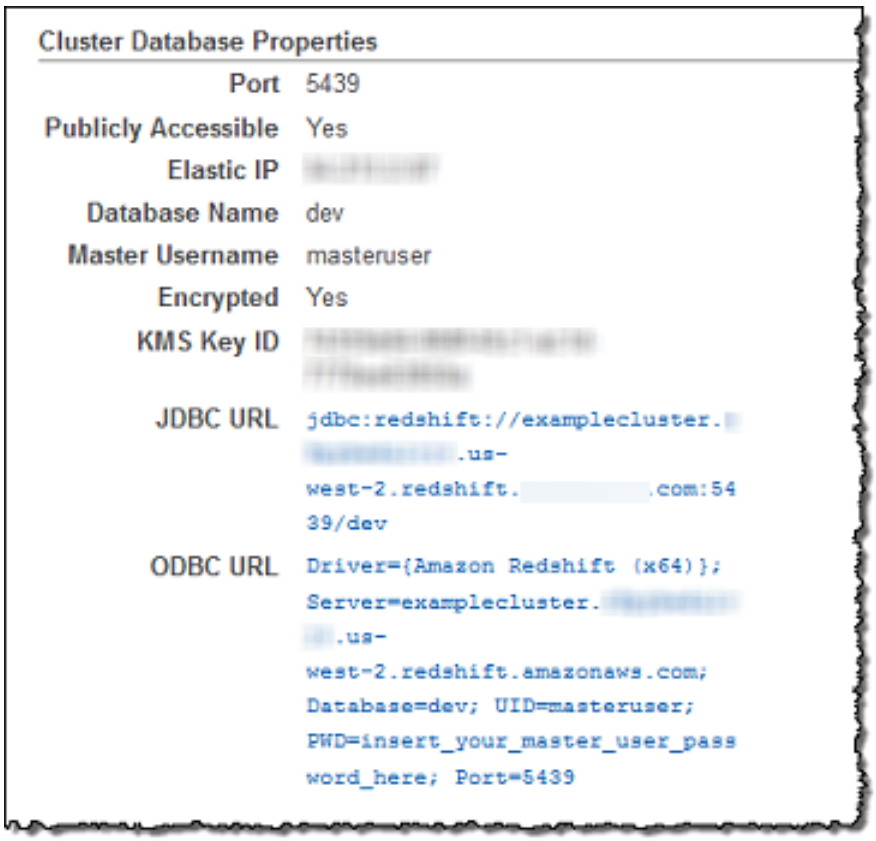
使用 psql 默认设置进行连接

预设情况下，psql 不会验证 Amazon Redshift 服务，但会使用安全套接字层 (SSL) 建立加密连接。

使用 psql 默认设置进行连接

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 根据您使用的 Amazon Redshift 控制台，选择以下其中一个步骤：
   - 在导航窗格中，选择 Clusters。然后，从列表中选择集群名称以打开其详细信息。在 Properties（属性）选项卡上的 Database configurations（数据库配置）部分中，记录 Database name（数据库名称）和 Port（端口）。查看 Connection details（连接详细信息）部分，并记录以下形式的 Endpoint（端点）：

     ```
     endpoint:port/databasename
     ```

   - 

3. 在命令提示符处，使用命令行参数或连接信息字符串来指定连接信息。使用以下参数：

```
psql -h <endpoint> -U <userid> -d <databasename> -p <port>
```

其中：

- *<endpoint>* 是您在上一步中记录的 Endpoint（端点）。
- *<userid>* 是有权连接到集群的用户 ID。
- *<databasename>* 是您在上一步中记录的 Database Name（数据库名称）。
- *<port>* 是您在上一步中记录的 Port（端口）。

例如：

```
psql -h examplecluster.<XXXXXXXXXXXX>.us-west-2.redshift.amazonaws.com -U adminuser -d
 dev -p 5439
```

4. 在 psql 密码提示符处，输入 *<userid>* 用户的密码。

您现已连接到集群，并能以交互方式输入命令。

使用证书进行连接

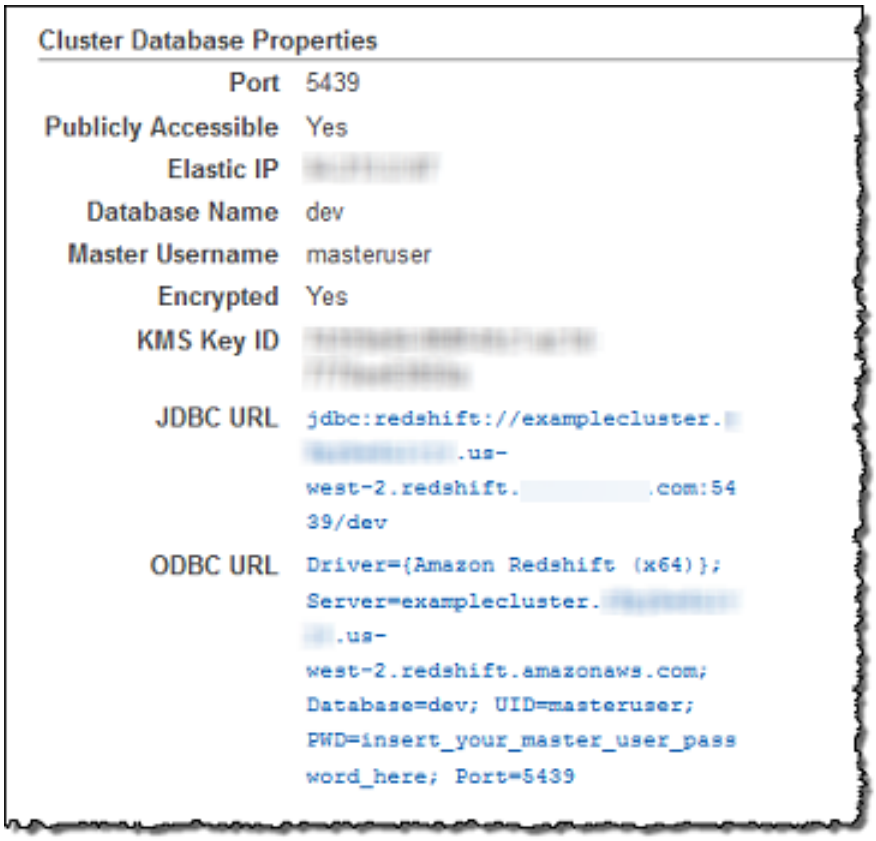
要控制 psql 是否要使用证书对服务进行身份验证，您必须使用连接信息字符串指定连接信息，并指定 `sslmode` 关键字。默认情况下，psql 采用的是 `sslmode=prefer`。要指定 psql 打开加密连接并使用 Amazon Redshift 证书验证服务，请将 Amazon Redshift 证书下载到您的计算机上。除非您不使用 DNS 别名，请指定 `verify-full`。如果您使用 DNS 别名，请选择 `verify-ca`。指定 `sslrootcert` 与证书的位置。有关 `sslmode` 的更多信息，请参阅 配置连接的安全选项 (p. 217)。

有关连接信息字符串参数的更多信息，请参阅 https://www.postgresql.org/docs/8.4/static/libpq-connect.html。

使用证书进行连接

1. 将 Amazon 信任证书颁发机构包 .crt 文件保存并下载到您的计算机中。有关下载信息，请参阅使用 SSL 进行连接 (p. 217)。如果您使用的是 Internet Explorer，要执行文件\另存为操作，请将文件类型指定为文本文件 (*.txt)，并删除 .txt 扩展名。例如，将其另存为文件 `C:\MyDownloads\amazon-trust-ca-bundle.crt`。
2. 根据您使用的 Amazon Redshift 控制台，选择以下其中一个步骤：
   - 在导航窗格中，选择 Clusters。然后，从列表中选择集群名称以打开其详细信息。在 Properties（属性）选项卡上的 Database configurations（数据库配置）部分中，记录 Database name（数据库名称）和 Port（端口）。查看 Connection details（连接详细信息）部分，并记录以下形式的 Endpoint（端点）：

     ```
     endpoint:port/databasename
     ```

- 

3. 在命令提示符处，使用连接信息字符串指定连接信息：

```
psql "host=<endpoint> user=<userid> dbname=<databasename> port=<port> sslmode=verify-ca
 sslrootcert=<certificate>"
```

其中：

- *<endpoint>* 是您在上一步中记录的 Endpoint（端点）。
- *<userid>* 是有权连接到集群的用户 ID。
- *<databasename>* 是您在上一步中记录的 Database Name（数据库名称）。
- *<port>* 是您在上一步中记录的 Port（端口）。
- *<certificate>* 是证书文件的完整路径。在 Windows 系统上，指定证书路径必须使用 Linux 式分隔符“/”而非 Windows 式分隔符“\”。

  在 Linux 和 macOS X 操作系统上，路径为

  ```
  ~/.postgresql/root.crt
  ```

  在 Microsoft Windows 上，路径为

  ```
  %APPDATA%/postgresql/root.crt
  ```

例如：

```
psql "host=examplecluster.<XXXXXXXXXXXX>.us-west-2.redshift.amazonaws.com
 user=adminuser dbname=dev port=5439 sslmode=verify-ca sslrootcert=C:/MyDownloads/
amazon-trust-ca-bundle.crt"
```

4. 在 psql 密码提示符处，输入 *<userid>* 用户的密码。

您现已连接到集群，并能以交互方式输入命令。

以编程方式连接到集群

此部分介绍了如何以编程方式连接到集群。如果您使用的应用程序（如 SQL Workbench/J）能够为您管理客户端连接，则可跳过这一部分。

使用 Java 连接到集群

当您使用 Java 来以编程方式连接到集群时，不管是否使用服务器身份验证均可实现。如果您计划使用服务器身份验证，请按照 配置连接的安全选项 (p. 217) 中的说明将 Amazon Redshift 服务器证书放入密钥存储库中。您可以通过在运行代码时指定属性来使用 keystore，如下所示：

```
-Djavax.net.ssl.trustStore=<path to keystore>
-Djavax.net.ssl.trustStorePassword=<keystore password>
```

Example ：使用 Java 连接到集群

以下示例可连接到集群，并会运行可返回系统表的示例查询。即使您的数据库中没有数据也可以使用此示例。

如果您要使用服务器证书对集群进行身份验证，则可还原使用密钥存储库但已被注释掉的行。

```
props.setProperty("ssl", "true");
```

有关服务器证书的更多信息，请参阅配置连接的安全选项 (p. 217)。

有关运行以下示例的分步说明，请参阅 使用 Eclipse 运行 Amazon Redshift 的 Java 示例 (p. 464)。

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
*/

// snippet-sourcedescription:[ConnectToClusterExample demonstrates how to connect to an
 Amazon Redshift cluster and run a sample query.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[Connect]
// snippet-keyword:[JDBC]
// snippet-sourcetype:[full-example]
```

```
// snippet-sourcedate:[2019-02-01]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.ConnectToCluster.complete]

package connection;

import java.sql.*;
import java.util.Properties;

public class ConnectToCluster {
    //Redshift driver: "jdbc:redshift://x.y.us-west-2.redshift.amazonaws.com:5439/dev";
    static final String dbURL = "***jdbc cluster connection string ****";
    static final String MasterUsername = "***master user name***";
    static final String MasterUserPassword = "***master user password***";

    public static void main(String[] args) {
        Connection conn = null;
        Statement stmt = null;
        try{
           //Dynamically load driver at runtime.
           //Redshift JDBC 4.1 driver: com.amazon.redshift.jdbc41.Driver
           //Redshift JDBC 4 driver: com.amazon.redshift.jdbc4.Driver
           Class.forName("com.amazon.redshift.jdbc.Driver");

           //Open a connection and define properties.
           System.out.println("Connecting to database...");
           Properties props = new Properties();

           //Uncomment the following line if using a keystore.
           //props.setProperty("ssl", "true");
           props.setProperty("user", MasterUsername);
           props.setProperty("password", MasterUserPassword);
           conn = DriverManager.getConnection(dbURL, props);

           //Try a simple query.
           System.out.println("Listing system tables...");
           stmt = conn.createStatement();
           String sql;
           sql = "select * from information_schema.tables;";
           ResultSet rs = stmt.executeQuery(sql);

           //Get the data from the result set.
           while(rs.next()){
              //Retrieve two columns.
              String catalog = rs.getString("table_catalog");
              String name = rs.getString("table_name");

              //Display values.
              System.out.print("Catalog: " + catalog);
              System.out.println(", Name: " + name);
           }
           rs.close();
           stmt.close();
           conn.close();
        }catch(Exception ex){
           //For convenience, handle all errors here.
           ex.printStackTrace();
        }finally{
           //Finally block to close resources.
           try{
              if(stmt!=null)
                 stmt.close();
           }catch(Exception ex){
           }// nothing we can do
           try{
              if(conn!=null)
```

```
                conn.close();
            }catch(Exception ex){
               ex.printStackTrace();
            }
        }
        System.out.println("Finished connectivity test.");
     }
}
// snippet-end:[redshift.java.ConnectToCluster.complete]
```

使用 .NET 连接到集群

当您使用 .NET (C#) 以编程方式连接到集群时，不管是否使用服务器身份验证均可实现。如果您计划使用服务器身份验证，请按照 配置连接的安全选项 (p. 217) 中的说明下载 Amazon Redshift 服务器证书，然后将证书转换成格式正确的 .NET 代码。

Example 使用 .NET 连接到集群

以下示例可连接到集群，并会运行可返回系统表的示例查询。它不会显示服务器身份验证。即使您的数据库中没有数据也可以使用此示例。该示例使用 System.Data.Odbc 命名空间，这是适用于 ODBC 的 .NET Framework 数据提供程序。

```
using System;
using System.Data;
using System.Data.Odbc;

namespace redshift.amazon.com.docsamples
{
    class ConnectToClusterExample
    {
        public static void Main(string[] args)
        {

            DataSet ds = new DataSet();
            DataTable dt = new DataTable();

            // Server, e.g. "examplecluster.xyz.us-west-2.redshift.amazonaws.com"
            string server = "***provide server name part of connection string****";

            // Port, e.g. "5439"
            string port = "***provide port***";

            // MasterUserName, e.g. "masteruser".
            string masterUsername = "***provide master user name***";

            // MasterUserPassword, e.g. "mypassword".
            string masterUserPassword = "***provide master user password***";

            // DBName, e.g. "dev"
            string DBName = "***provide name of database***";

            string query = "select * from information_schema.tables;";

            try
            {
                // Create the ODBC connection string.
                //Redshift ODBC Driver - 64 bits
                /*
                string connString = "Driver={Amazon Redshift (x64)};" +
                    String.Format("Server={0};Database={1};" +
                    "UID={2};PWD={3};Port={4};SSL=true;Sslmode=Require",
                    server, DBName, masterUsername,
                    masterUserPassword, port);
```

```
                */

                //Redshift ODBC Driver - 32 bits
                string connString = "Driver={Amazon Redshift (x86)};" +
                    String.Format("Server={0};Database={1};" +
                    "UID={2};PWD={3};Port={4};SSL=true;Sslmode=Require",
                    server, DBName, masterUsername,
                    masterUserPassword, port);

                // Make a connection using the psqlODBC provider.
                OdbcConnection conn = new OdbcConnection(connString);
                conn.Open();

                // Try a simple query.
                string sql = query;
                OdbcDataAdapter da = new OdbcDataAdapter(sql, conn);
                da.Fill(ds);
                dt = ds.Tables[0];
                foreach (DataRow row in dt.Rows)
                {
                    Console.WriteLine(row["table_catalog"] + ", " + row["table_name"]);
                }

                conn.Close();
                Console.ReadKey();
            }
            catch (Exception ex)
            {
                Console.Error.WriteLine(ex.Message);
            }

        }
    }
}
```

使用身份验证配置文件连接到 Amazon Redshift

如果您与 Amazon Redshift 有很多连接，则可能很难管理所有这些连接的设置。通常，每个 JDBC 或 ODBC 连接都使用特定的配置选项。借助身份验证配置文件，可以将连接选项存储在一起。这样，用户可以选择要连接的配置文件，避免管理单个选项的设置。配置文件可以应用于各种场景和用户类型。

创建身份验证配置文件后，用户可以将即用型配置文件添加到连接字符串。这样，他们即可使用针对每个角色和使用案例的正确设置连接到 Amazon Redshift。

有关 Amazon Redshift API 的信息，请参阅 CreateAuthenticationProfile。

创建身份验证配置文件

通过 Amazon CLI，您可以使用 `create-authentication-profile` 命令创建身份验证配置文件。这假定您已有一个 Amazon Redshift 集群和现有数据库。您的凭证必须具有连接到 Amazon Redshift 数据库的权限以及获取身份验证配置文件的权限。您可以将配置选项作为 JSON 字符串提供，或者引用包含 JSON 字符串的文件。

```
create-authentication-profile --authentication-profile-name<value: String> --
authentication-profile-content<value: String>
```

以下示例创建一个名为 `ExampleProfileName` 的配置文件。在这里，您可以将定义集群名称和其它选项设置的键和值作为 JSON 字符串添加。

```
create-authentication-profile --authentication-profile-name "ExampleProfileName"
 --authentication-profile-content "{\"AllowDBUserOverride\":\"1\",\"Client_ID
```

```
\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID\",\"AutoCreate\":false,
\"enableFetchRingBuffer\":true,\"databaseMetadataCurrentDbOnly\":true}"
}
```

此命令使用指定的 JSON 设置创建配置文件。返回以下内容，表示已创建配置文件。

```
{"AuthenticationProfileName": "ExampleProfileName",
"AuthenticationProfileContent": "{\"AllowDBUserOverride\":\"1\",\"Client_ID\":
\"ExampleClientID\",\"App_ID\":\"ExampleAppID\",\"AutoCreate\":false,
\"enableFetchRingBuffer\":true,\"databaseMetadataCurrentDbOnly\":true}" }
```

创建身份验证配置文件的限制和配额

每位客户的配额为十（10）个身份验证配置文件。

身份验证配置文件可能发生某些错误 例如，如果您使用现有名称创建新的配置文件，或者您是否超过了配置文件配额。有关更多信息，请参阅 CreateAuthenticationProfile。

您无法在身份验证配置文件存储中存储 JDBC、ODBC 和 Python 连接字符串的某些选项键和值：

- `AccessKeyID`
- `access_key_id`
- `SecretAccessKey`
- `secret_access_key_id`
- `PWD`
- `Password`
- `password`

对于 JDBC 或 ODBC 连接字符串，您不能在配置文件存储中存储键或值 `AuthProfile`。对于 Python 连接，您无法存储 `auth_profile`。

身份验证配置文件存储在 Amazon DynamoDB 中并由 Amazon 管理。

使用身份验证配置文件

创建身份验证配置文件后，您可以包含配置文件名称作为 JDBC 2.0 `AuthProfile` 版的连接选项。使用此连接选项可以检索存储的设置。

```
jdbc:redshift:iam://endpoint:port/database?AuthProfile=<Profile-Name>&AccessKeyID=<Caller-
Access-Key>&SecretAccessKey=<Caller-Secret-Key>
```

以下是 JDBC URL 字符串示例。

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
AuthProfile="ExampleProfile"&AccessKeyID="AKIAIOSFODNN7EXAMPLE"&SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

在 JDBC URL 中指定 `AccessKeyID` 和 `SecretAccessKey`，以及身份验证配置文件名称。

在下面的示例中，您还可以使用分号分隔符分隔配置选项，其中包括日志记录选项。

```
jdbc:redshift:iam://my_redshift_end_point:5439/dev?LogLevel=6;LogPath=/
tmp;AuthProfile=my_profile;AccessKeyID="AKIAIOSFODNN7EXAMPLE";SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

Note

请勿向身份验证配置文件中添加机密信息。例如，不要在身份验证配置文件中存储 AccessKeyID 或 SecretAccessKey 值。身份验证配置文件存储具有禁止存储密钥的规则。如果尝试存储与敏感信息相关的密钥和值，则会出错。

获取身份验证配置文件

要列出现有身份验证配置文件，请调用以下命令。

```
describe-authentication-profiles --authentication-profile-name <value: String>
```

下面的示例显示了两个检索配置文件。如果不指定配置文件名称，则返回所有配置文件。

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

解决 Amazon Redshift 中的连接问题

如果您在从 SQL 客户端工具连接到集群时遇到问题，可以从几个方面进行排查以缩小问题范围。如果您使用了 SSL 或服务器证书，请在开始排查连接问题之前将其删除以降低复杂性。然后，在找出解决方案之后再添加。有关更多信息，请参阅配置连接的安全选项 (p. 217)。

Important

Amazon Redshift 改变了我们管理 SSL 证书的方法。如果您在使用 SSL 连接时遇到问题，您可能需要更新当前的信任根 CA 证书。有关更多信息，请参阅将 SSL 连接过渡到 ACM 证书 (p. 220)。

以下部分提供了一些针对连接问题的示例错误消息和可能的解决方案。不同 SQL 客户端工具提供的错误消息不同，因此，虽然此非完整列表，但却是不错的问题排查切入点。

主题

- 从 Amazon EC2 外部连接防火墙超时问题 (p. 263)
- 连接被拒绝或失败 (p. 265)
- 客户端和驱动程序不兼容 (p. 266)
- 查询似乎挂起，有时无法连接到集群 (p. 266)

从 Amazon EC2 外部连接防火墙超时问题

问题示例

在运行 COPY 命令等较长的查询时，客户端到数据库的连接会挂起或超时。此时，您可能会发现，Amazon Redshift 控制台显示查询已完成，而客户端工具仍然显示正在运行查询。查询结果可能会丢失或不完整，具体取决于连接停止的时间。

可能的解决方案

当您从 Amazon EC2 实例以外的计算机连接到 Amazon Redshift 时，会发生此问题。在此情况下，空闲连接将在处于不活动状态一段时间后被防火墙等中间网络组件终止。当您从 Virtual Private Network（VPN）或本地网络登录时，通常会出现这种行为。

为避免出现此类超时，建议您执行以下更改：

- 提高用于处理 TCP/IP 超时的客户端系统值。在用来连接集群的计算机上进行这些更改。根据您的客户端和网络调整超时期限。有关更多信息，请参阅更改 TCP/IP 超时设置 (p. 264)。
- （可选）在 DSN 级别设置 Keepalive 行为。有关更多信息，请参阅更改 DSN 超时设置 (p. 265)。

更改 TCP/IP 超时设置

要更改 TCP/IP 超时设置，请根据您用来连接集群的操作系统配置超时设置。

- Linux — 如果您的客户端在 Linux 上运行，请以根用户身份运行以下命令来更改当前会话的超时设置：

```
/sbin/sysctl -w net.ipv4.tcp_keepalive_time=200 net.ipv4.tcp_keepalive_intvl=200
 net.ipv4.tcp_keepalive_probes=5
```

要保存设置，请使用以下值创建或修改文件 `/etc/sysctl.conf`，然后重新启动您的系统。

```
net.ipv4.tcp_keepalive_time=200
net.ipv4.tcp_keepalive_intvl=200
net.ipv4.tcp_keepalive_probes=5
```

- Windows — 如果您的客户端在 Windows 上运行，请在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ 下编辑以下注册表设置的值：
  - KeepAliveTime：30000
  - KeepAliveInterval：1000
  - TcpMaxDataRetransmissions：10

  这些设置使用 DWORD 数据类型。如果它们不在注册表路径下，您可以创建设置并指定这些建议值。有关编辑 Windows 注册表的更多信息，请参阅 Windows 文档。

  在设置好这些值之后，重启您的计算机以使更改生效。

- Mac — 如果您的客户端在 Mac 上运行，请运行以下命令来更改当前会话的超时设置：

```
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
```

要保存设置，请使用以下值创建或修改文件 `/etc/sysctl.conf`：

```
net.inet.tcp.keepidle=200000
net.inet.tcp.keepintvl=200000
net.inet.tcp.keepinit=200000
net.inet.tcp.always_keepalive=1
```

重新启动计算机，然后运行以下命令来验证值是否已设置。

```
sysctl net.inet.tcp.keepidle
sysctl net.inet.tcp.keepintvl
sysctl net.inet.tcp.keepinit
sysctl net.inet.tcp.always_keepalive
```

更改 DSN 超时设置

如果需要，您可以在 DSN 级别设置 Keepalive 行为。在 odbc.ini 文件中添加或修改以下参数即可实现：

KeepAlivesCount

连接被视为断开前可能丢失的 TCP keepalive 包的数量。

KeepAlivesIdle

驱动程序发送 TCP Keepalive 包前处于不活动状态的秒数。

KeepAlivesInterval

两次传输 TCP keepalive 间隔的秒数。

在 Windows 上，您可以通过在 HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI*your_DSN* 中添加或更改密钥来修改注册表中的这些参数。在 Linux 和 macOS 上，您可以直接在 odbc.ini 文件中添加或修改目标 DSN 条目中的这些参数。有关在 Linux 和 macOS 计算机上修改 odbc.ini 文件的更多信息，请参阅使用 ODBC 驱动程序管理器在 Linux 和 macOS X 操作系统上配置驱动程序 (p. 212)。

如果这些参数不存在，或者其值为 0，则系统将使用为 TCP/IP 指定的 Keepalive 参数来确定 DSN Keepalive 行为。在 Windows 上，您可以在注册表中的 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\` 中查找 TCP/IP 参数。在 Linux 和 macOS 上，可以在 sysctl.conf 文件中查找 TCP/IP 参数。

连接被拒绝或失败

错误示例

- “无法建立到 *<endpoint>* 的连接。”
- “无法连接到服务器：连接超时。服务器是否在主机 *'<endpoint>'* 上运行，是否接受端口 *'<port>'* 上的 TCP/IP 连接？”
- “连接被拒。请检查主机名和端口是否正确无误，以及邮件管理员是否接受 TCP/IP 连接。”

可能的解决方案

当您收到提示连接建立失败的错误消息时，通常是因为您没有访问集群的权限。

要从集群所在的网络外部的客户端工具连接到集群，请添加入口规则。将规则添加到要从其连接的 CIDR/IP 的集群安全组中：

- 如果您已在 Virtual Private Cloud (VPC) 中创建基于 Amazon VPC 的 Amazon Redshift 集群，则需要将您的客户端 CIDR/IP 地址添加到 Amazon VPC 中的 VPC 安全组。有关为集群配置 VPC 安全组的更多信息，请参阅在 VPC 中管理集群 (p. 92)。
- 如果您已在 VPC 外部创建 Amazon VPC 集群，则需要将您的客户端 CIDR/IP 地址添加到 Amazon Redshift 中的集群安全组。有关配置集群安全组的更多信息，请参阅Amazon Redshift 集群安全组 (p. 458)。

如果您尝试从 Amazon EC2 实例中的客户端工具连接到集群，也需要添加入口规则。在此情况下，需要将规则添加到与 Amazon EC2 实例关联的 Amazon EC2 安全组的集群安全组。有关配置集群安全组的更多信息，请参阅Amazon Redshift 集群安全组 (p. 458)。

在某些情况下，客户端和服务器之间可能有一个层，例如防火墙。在这些情况下，请确保防火墙接受通过为集群配置的端口的入站连接。

客户端和驱动程序不兼容

错误示例

“指定的 DSN 中包含驱动程序与应用程序之间的架构不匹配。”

可能的解决方案

如果您在尝试连接时收到架构不匹配的错误，则说明客户端工具与驱动程序不兼容。此情况是由于其系统架构不匹配导致的。例如，如果您在 32 位客户端工具上安装 64 位驱动程序版本，便会发生这种情况。有时，64 位客户端工具可以使用 32 位驱动程序，但无法在 32 位应用程序上使用 64 位驱动程序。请确保驱动程序和客户端工具使用的是相同版本的系统架构。

查询似乎挂起，有时无法连接到集群

问题示例

您在完成查询时遇到问题，即在 SQL 客户端工具中，查询显示为正在进行，但实则处于挂起状态。有时，查询无法显示在集群中，如系统表或 Amazon Redshift 控制台中。

可能的解决方案

此问题可能是由于数据包丢失导致的。在此情况下，两个 Internet 协议 (IP) 主机在网络路径中的最大传输单位 (MTU) 大小不同。MTU 大小用于确定可通过网络连接在单个以太网帧中传输的数据包的最大大小（以字节为单位）。在 Amazon 中，一些 Amazon EC2 实例类型支持 1500 MTU（以太网 v2 帧），其他实例类型支持 9001 MTU（TCP/IP 巨型帧）。

为避免因 MTU 大小不同可能导致的各种问题，建议您执行以下操作之一：

- 如果集群使用 EC2-VPC 平台，则使用将返回 `Destination Unreachable` 的入站自定义 互联网 控制消息协议 (ICMP) 规则配置 Amazon VPC 安全组。因此，该规则指示原始主机沿网络路径使用最小的 MTU 大小。有关此方法的详细信息，请参阅配置安全组以允许 ICMP“无法到达目标” (p. 266)。
- 如果您的集群使用 EC2-Classic 平台，或者您无法允许 ICMP 入站规则，请禁用 TCP/IP 巨型帧以便使用以太网 v2 帧。有关此方法的详细信息，请参阅配置实例的 MTU (p. 266)。

配置安全组以允许 ICMP“无法到达目标”

当两个主机在网络中的 MTU 大小存在差异时，请先确保您的网络设置不会阻止路径 MTU 发现 (PMTUD)。PMTUD 使接收主机能够使用以下 ICMP 消息响应原始主机：`Destination Unreachable: fragmentation needed and DF set (ICMP Type 3, Code 4)`。此消息将指示原始主机在网络路径中使用最低 MTU 大小重新发送请求。若无此协商，当请求过大，导致接收主机无法接收时，数据包可能会丢失。有关此 ICMP 消息的更多信息，请转至 国际互联网工程任务组 (IETF) 网站上的 RFC792。

如果您没有为 Amazon VPC 安全组明确配置此 ICMP 入站规则，PMTUD 则将被阻止。在 Amazon 中，安全组是虚拟防火墙，用于为到实例的入站和出站流量指定规则。有关 Amazon Redshift 集群安全组的信息，请参阅 Amazon Redshift 集群安全组 (p. 458)。对于使用 EC2-VPC 平台的集群，Amazon Redshift 将使用 VPC 安全组来允许或拒绝到集群的流量。默认情况下，安全组处于锁定状态，会拒绝所有入站流量。有关如何为 EC2-Classic 或 EC2-VPC 实例设置入站和出站规则的信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中的 EC2-Classic 与 VPC 中的实例间的差异。

有关如何向 VPC 安全组添加规则的更多信息，请参阅管理集群的 VPC 安全组 (p. 94)。有关此规则中需要的特定 PMTUD 设置的更多信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中的路径 MTU 发现。

配置实例的 MTU

在某些情况下，您的集群可能会使用 EC2-Classic 平台，或者您不能允许对入站流量使用自定义 ICMP 规则。在这些情况下，建议您在从中连接到 Amazon Redshift 集群的 EC2 实例的网络接口 (NIC) 上将 MTU 调

整为 1500。此调整将禁用 TCP/IP 巨型帧，以确保连接始终使用同一数据包大小。但是，此选项将从整体上降低实例的最大网络吞吐量，而不仅仅是到 Amazon Redshift 的连接。有关更多信息，请参阅以下流程。

在 Microsoft Windows 操作系统上设置 MTU

如果客户端在 Microsoft Windows 操作系统上运行，则可使用 `netsh` 命令查看和设置以太网适配器的 MTU 值。

1. 运行以下命令可确定当前 MTU 值：

```
netsh interface ipv4 show subinterfaces
```

2. 在输出中查看 `MTU` 适配器的 `Ethernet` 值。
3. 如果值不是 `1500`，则运行以下命令设置它：

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500 store=persistent
```

设置好此值后，重启您的计算机以使更改生效。

在 Linux 操作系统上设置 MTU

如果客户端在 Linux 操作系统上运行，则可使用 `ip` 命令查看和设置 MTU 值。

1. 运行以下命令可确定当前 MTU 值：

```
$ ip link show eth0
```

2. 查看输出中 `mtu` 后面的值。
3. 如果值不是 `1500`，则运行以下命令设置它：

```
$ sudo ip link set dev eth0 mtu 1500
```

在 Mac 操作系统上设置 MTU

- 请按照 MacOS 支持网站上关于 `How to change the MTU for troubleshooting purposes` 的说明。有关详细信息，请搜索 支持网站。

使用 Amazon Redshift 数据 API

您可以使用内置的 Amazon Redshift 数据 API 访问您的 Amazon Redshift 数据库。使用此 API，您可以通过基于 Web 服务的应用程序（包括 Amazon Lambda、Amazon SageMaker 笔记本和 Amazon Cloud9）访问 Amazon Redshift 数据。有关这些应用程序的更多信息，请参阅 Amazon Lambda、Amazon SageMaker 和 Amazon Cloud9。

数据 API 不需要与集群的持久连接。相反，它提供了安全 HTTP 终端节点以及与 Amazon 开发工具包的集成。您可以使用终端节点运行 SQL 语句，而无需管理连接。对数据 API 的调用是异步的。

数据 API 使用存储在 Amazon Secrets Manager 中的凭证或临时数据库凭证。您无需使用任何一种授权方法在 API 调用中传递密码。有关 Amazon Secrets Manager 的更多信息，请参阅 Amazon Secrets Manager 用户指南中的什么是 Amazon Secrets Manager？

有关数据 API 操作的更多信息，请参阅 Amazon Redshift 数据 API 参考。

使用 Amazon Redshift 数据 API

在您使用 Amazon Redshift 数据 API 之前，请查看以下步骤：

1. 确定您作为数据 API 的调用者是否获得授权。有关 授权的更多信息，请参阅授予对 Amazon Redshift 数据 API 的访问权限 (p. 270)。
2. 确定是否计划使用来自 Secrets Manager 的身份验证凭据或临时凭证调用数据 API。有关更多信息，请参阅在调用 Amazon Redshift 数据 API 时选择身份验证凭证 (p. 268)。
3. 如果您将 Secrets Manager 用于身份验证凭证，请设置密码。有关更多信息，请参阅在 Amazon Secrets Manager 中存储数据库凭证 (p. 271)。
4. 查看调用数据 API 时的注意事项和限制。有关更多信息，请参阅调用 Amazon Redshift 数据 API 时的注意事项 (p. 268)。
5. 从 Amazon Command Line Interface (Amazon CLI)、您自己的代码中调用数据 API，或使用 Amazon Redshift 控制台中的查询编辑器。有关从 Amazon CLI 进行调用的示例，请参阅调用 Data API (p. 273)。

调用 Amazon Redshift 数据 API 时的注意事项

调用数据 API 时，请注意以下事项：

- 有关提供了数据 API 的 Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中为 Redshift 数据 API 列出的端点。
- 查询的最长持续时间为 24 小时。
- 每个 Amazon Redshift 集群的活动查询（`STARTED` 和 `SUBMITTED` 查询）最大数为 200 个。
- 查询结果的最大大小为 100 MB。如果调用返回的响应数据超过 100 MB，则调用将结束。
- 查询结果的最长保留时间为 24 小时。
- 最大查询语句大小为 100 KB。
- 数据 API 可用于查询以下节点类型的单节点和多节点集群：
  - dc2.large
  - dc2.8xlarge
  - ds2.xlarge
  - ds2.8xlarge
  - ra3.xlplus
  - ra3.4xlarge
  - ra3.16xlarge
- 集群必须在基于 Amazon VPC 服务的 Virtual Private Cloud (VPC) 中。
- 预设情况下，具有与 `ExecuteStatement` 或者 `BatchExecuteStatement` API 操作运行者相同的 IAM 角色或 IAM 用户的用户可以使用 `CancelStatement`、`DescribeStatement`、`GetStatementResult` 和 `ListStatements` API 操作对同一个语句进行操作。要从另一个 IAM 用户对同一 SQL 语句执行操作，该用户必须能够代入运行 SQL 语句的用户的 IAM 角色。有关如何代入角色的更多信息，请参阅授予对 Amazon Redshift 数据 API 的访问权限 (p. 270)。
- `BatchExecuteStatement` API 操作的 `Sqls` 参数中的 SQL 语句将作为单个事务运行。它们按数组的顺序连续运行。后续的 SQL 语句要等到数组中的前一条语句完成后才会开始。如果任何 SQL 语句失败，由于它们作为一个事务运行，所有工作都将回滚。

在调用 Amazon Redshift 数据 API 时选择身份验证凭证

当您调用数据 API 时，您对某些 API 操作使用以下身份验证方法之一。每种方法都需要不同的参数组合。

Amazon Secrets Manager

使用此方法，提供存储在 Amazon Secrets Manager 中的 `secret-arn` 密钥值。指定的密钥包含用于连接到您指定的 `database` 的凭证。在连接到集群时，还可以提供数据库名称以及与密钥中的集群匹配的集群标识符。在连接到无服务器工作组时，也要提供数据库名称。

临时凭证

利用此方法，在连接到集群时，需要指定集群标识符、数据库名称和数据库用户名。此外，需具有调用 `redshift:GetClusterCredentials` 操作的权限。在连接到无服务器工作组时，需指定数据库名称。

使用任何一种方法，您还可以提供 `region` 值，该值指定您的集群所在的 Amazon 区域。

调用 Amazon Redshift 数据 API 时映射 JDBC 数据类型

下表将 Java 数据库连接 (JDBC) 数据类型映射到您在数据 API 调用中指定的数据类型。

JDBC 数据类型	Data API 数据类型
`INTEGER, TINYINT, SMALLINT, BIGINT`	`LONG`
`FLOAT, REAL, DOUBLE`	`DOUBLE`
`DECIMAL`	`STRING`
`BOOLEAN, BIT`	`BOOLEAN`
`BLOB, BINARY, LONGVARBINARY, VARBINARY`	`BLOB`
`CLOB`	`STRING`
其他类型（包括与日期和时间有关的类型）	`STRING`

字符串值将传递到 Amazon Redshift 数据库并隐式转换为数据库数据类型。

Note

目前，数据 API 不支持通用唯一标识符 (UUID) 的数组。

在调用 Amazon Redshift 数据 API 时运行带有参数的 SQL 语句

您可以通过使用 SQL 语句部分的参数调用数据 API 操作来控制提交到数据库引擎的 SQL 文本。命名参数提供了一种灵活的方式来传入参数，而无需在 SQL 文本中对参数进行硬编码。它们可以帮助您重复使用 SQL 文本并避免 SQL 注入问题。

以下示例显示 `execute statement` Amazon CLI 命令的 `parameters` 字段的命名参数。

```
--parameters "[{\"name\": \"id\", \"value\": \"1\"},{\"name\": \"address\", \"value\":
 \"Seattle\"}]"
```

使用命名参数时，请注意以下事项：

- 命名参数可以按任意顺序排列，并且参数可以在 SQL 文本中多次使用。前面示例中显示的参数选项，值 `1` 和 `Seattle` 插入到表列 `id` 和 `address` 中。在 SQL 文本中，您可以按如下方式指定命名参数：

```
--sql "insert into mytable values (:id, :address)"
```

- SQL 运行时，数据将隐式转换为数据类型。有关数据类型转换的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的数据类型。
- 您不能将值设置为 NULL。数据 API 将其解释为文本字符串 `NULL`。以下示例将 `id` 替换为文本字符串 `null`。不是 SQL NULL 值。

```
--parameters "[{\"name\": \"id\", \"value\": \"null\"}]"
```

- 无法设置零长度值。数据 API SQL 语句失败。下面的示例尝试设置 `id` 长度值为零，导致 SQL 语句失败。

```
--parameters "[{\"name\": \"id\", \"value\": \"\"}]"
```

- 不能在带有参数的 SQL 语句中设置表名。数据 API 遵循 JDBC `PreparedStatement` 的规则。
- `describe statement` 操作的输出返回 SQL 语句的查询参数。
- 仅 `execute-statement` 操作支持带有参数的 SQL 语句。

授予对 Amazon Redshift 数据 API 的访问权限

用户必须获得授权才能访问数据 API。您可以通过将托管策略（预定义的 Amazon Identity and Access Management (IAM) policy）添加给用户，授予该用户访问数据 API 的权限。要查看托管策略允许和拒绝的权限，请参阅 IAM 控制台 (https://console.aws.amazon.com/iam/)。

Amazon Redshift 提供 `AmazonRedshiftDataFullAccess` 托管策略。此策略提供了对 Amazon Redshift 数据 API 操作的完全访问。此策略还允许在范围内访问特定的 Amazon Redshift、Amazon Secrets Manager 以及对 Amazon Redshift 集群进行身份验证和访问所需的 IAM API 操作。

此外，您还可以创建自己的 IAM policy，以允许对特定资源的访问。要创建策略，请使用 `AmazonRedshiftDataFullAccess` 策略作为起始模板。在创建策略后，将该策略添加到需要访问数据 API 的每个用户。

考虑与 IAM 用户关联的 IAM policy 的以下要求：

- 如果您使用 Amazon Secrets Manager 进行身份验证，请确认策略允许使用 `secretsmanager:GetSecretValue` 操作来检索使用键 `RedshiftDataFullAccess` 标记的密钥。
- 如果您使用临时凭证对集群进行身份验证，请确认该策略允许将 `redshift:GetClusterCredentials` 操作用于集群中任何数据库的数据库用户名 `redshift_data_api_user`。此用户名必须已在数据库中创建。
- 如果您使用临时凭证对无服务器工作组进行身份验证，请确认该策略允许使用 `redshift-serverless:GetCredentials` 操作来检索使用键 `RedshiftDataFullAccess` 标记的工作组。数据库用户按 1:1 的比例映射到源 Amazon Identity and Access Management (IAM) 身份。例如，IAM 用户 foo 映射到数据库用户 `IAM:foo`，IAM 角色栏映射到 `IAMR:bar`。有关 IAM 身份的更多信息，请参阅《IAM 用户指南》中的 IAM 身份（用户、组和角色）。

要对其他账户拥有的集群运行查询，拥有账户必须提供一个 IAM 角色，数据 API 可以在调用账户时代入该角色。例如，假设账户 B 拥有账户 A 需要访问的集群。账户 B 可以将 Amazon 托管策略 `AmazonRedshiftDataFullAccess` 附加到账户 B 的 IAM 角色。然后，账户 B 使用信任策略信任账户 A，如下所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
```

```
            "arn:aws:iam::accountID-of-account-A:role/someRoleA"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

最后，账户 A 的 IAM 角色需要能够代入账户 B 的 IAM 角色。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::accountID-of-account-B:role/someRoleB"
  }
}
```

以下链接提供了 IAM 用户指南中有关 Amazon Identity and Access Management 的更多信息。

- 有关创建 IAM 角色的信息，请参阅创建 IAM 角色。
- 有关创建 IAM policy 的更多信息，请参阅创建 IAM policy。
- 有关将 IAM policy 添加到用户的信息，请参阅添加和删除 IAM 身份权限。

在 Amazon Secrets Manager 中存储数据库凭证

在调用数据 API 时，您可以使用 Amazon Secrets Manager 中的密钥传递集群或无服务器工作组的凭证。要通过此方式传递凭证，您需要指定密钥的名称或密钥的 Amazon Resource Name (ARN)。

要使用 Secrets Manager 存储凭证，您需要 `SecretManagerReadWrite` 托管策略权限。有关最低权限的更多信息，请参阅 Amazon Secrets Manager 用户指南中的使用 Amazon Secrets Manager 创建和管理密钥。

要将凭证存储在 Amazon Redshift 集群的密钥中

1. 使用 Amazon Secrets Manager 控制台创建包含集群凭证的密钥：

   - 当您选择 Store a new secret（存储新密钥）时，选择 Credentials for Redshift cluster（Redshift 集群的凭证）。
   - 将 User name（用户名）（数据库用户）、Password（密码）和 DB cluster （数据库集群）（集群标识符）的值存储在您的密钥中。
   - 使用键 `RedshiftDataFullAccess` 标记密钥。Amazon 托管策略 `AmazonRedshiftDataFullAccess` 只允许对使用键 `RedshiftDataFullAccess` 进行标记的密钥执行操作 `secretsmanager:GetSecretValue`。

   有关说明，请参阅 Amazon Secrets Manager 用户指南中的创建基本密钥。
2. 使用 Amazon Secrets Manager 控制台查看您创建的密钥的详细信息，或运行 `aws secretsmanager describe-secret` Amazon CLI 命令。

   记下密钥的名称和 ARN。您可以将其用于对数据 API 的调用中。

将凭证存储在无服务器工作组的密钥中

1. 使用 Amazon Secrets Manager Amazon CLI 命令存储包含无服务器工作组凭证的密钥：

- 在文件中创建密钥，例如名为 `mycreds.json` 的 JSON 文件。在文件中提供 User name（用户名）（数据库用户）和 Password（密码）的值。

```
{
      "username": "myusername",
      "password": "mypassword"
}
```

- 将值存储在密钥中，并使用键 `RedshiftDataFullAccess` 标记密钥。

```
aws secretsmanager create-secret --name MyRedshiftSecret  --tags
 Key="RedshiftDataFullAccess",Value="serverless" --secret-string file://mycreds.json
```

下面显示了输出。

```
{
    "ARN": "arn:aws:secretsmanager:region:accountId:secret:MyRedshiftSecret-mvLHxf",
    "Name": "MyRedshiftSecret",
    "VersionId": "a1603925-e8ea-4739-9ae9-e509eEXAMPLE"
}
```

有关更多信息，请参阅《Amazon Secrets Manager 用户指南》中的使用 Amazon CLI 创建基本密钥。

2. 使用 Amazon Secrets Manager 控制台查看您创建的密钥的详细信息，或运行 `aws secretsmanager describe-secret` Amazon CLI 命令。

   记下密钥的名称和 ARN。您可以将其用于对数据 API 的调用中。

为数据 API 创建 Amazon VPC 终端节点 (Amazon PrivateLink)

借助 Amazon Virtual Private Cloud (Amazon VPC)，您可以在 Virtual Private Cloud (VPC) 中启动 Amazon 资源（例如 Amazon Redshift 集群和应用程序）。Amazon PrivateLink 在亚马逊网络上提供了 Virtual Private Cloud (VPC) 和 Amazon 服务之间的私有连接。通过使用 Amazon PrivateLink，您可以创建 VPC 终端节点，这可让您根据 Amazon VPC 跨不同的账户和 VPC 连接到服务。有关 Amazon PrivateLink 的更多信息，请参阅 Amazon Virtual Private Cloud 用户指南中的 VPC 终端节点服务 (Amazon PrivateLink)。

您可以使用 Amazon VPC 终端节点调用数据 API。使用 Amazon VPC 终端节点可保留 Amazon VPC 中应用程序间的流量与Amazon网络中的 Data API，而无需使用公有 IP 地址。Amazon VPC 终端节点可帮助您遵守与管理公共互联网连接有关的合规性和法规要求。例如，如果您使用 Amazon VPC 终端节点，则可保持 Amazon EC2 实例上运行的应用程序和包含终端节点的 VPC 中的 Data API 之间的流量。

创建 Amazon VPC 终端节点后，便能开始使用此终端节点，而无需在应用程序中进行任何代码或配置更改。

为 Data API 创建 Amazon VPC 终端节点

1. 登录到Amazon Web Services Management Console并打开 Amazon VPC 控制台，网址：https://console.aws.amazon.com/vpc/。
2. 选择 Endpoints (终端节点)，然后选择 Create Endpoint (创建终端节点)。
3. 在 Create Endpoint (创建终端节点) 页面上，为 Service category (服务类别) 选择 Amazon services (亚马逊云科技服务)。对于 Service Name（服务名称），选择 redshift-data (`com.amazonaws.region.redshift-data`)。
4. 对于 VPC，选择要在其中创建终端节点的 VPC。

   选择包含用于进行 Data API 调用的应用程序的 VPC。
5. 对于 Subnets（子网），请为运行应用程序的 Amazon 服务所使用的每个可用区 (AZ) 选择子网。

要创建 Amazon VPC 终端节点，请指定端点可在其中访问的私有 IP 地址范围。为此，请为每个可用区选择子网。执行此操作会将 VPC 终端节点限制为特定于每个可用区的私有 IP 地址范围，并且还会在每个可用区中创建一个 Amazon VPC 终端节点。

6. 对于 Enable DNS Name (启用 DNS 名称)，选择 Enable for this endpoint (为此终端节点启用)。

   私有 DNS 会将标准 Data API DNS 主机名 (`https://redshift-data.region.amazonaws.com`) 解析为与特定于 Amazon VPC 终端节点的 DNS 主机名关联的私有 IP 地址。因此，您可以使用 Amazon CLI 或 Amazon 开发工具包访问 Data API VPC 终端节点，而无需进行任何代码或配置更改来更新 Data API 终端节点 URL。

7. 对于 Security group (安全组)，选择要与 Amazon VPC 终端节点关联的安全组。

   选择允许访问运行应用程序的 Amazon 服务的安全组。例如，如果 Amazon EC2 实例正在运行您的应用程序，请选择允许访问 Amazon EC2 实例的安全组。利用安全组，您可以控制从 VPC 中的资源发送到 Amazon VPC 终端节点的流量。

8. 选择Create endpoint。

创建终端节点后，选择 Amazon Web Services Management Console中的链接以查看终端节点详细信息。

终端节点 Details (详细信息) 选项卡将显示在创建 Amazon VPC 终端节点时生成的 DNS 主机名。

您可以使用标准终端节点 (`redshift-data.region.amazonaws.com`) 或特定于 VPC 的终端节点之一来调用 Amazon VPC 中的 Data API。标准 Data API 终端节点将自动路由到 Amazon VPC 终端节点。发生此路由的原因是，在创建 Amazon VPC 终端节点时启用了私有 DNS 主机名。

在 Data API 调用中使用 Amazon VPC 终端节点时，应用程序和 Data API 之间的所有流量将在包含它们的 Amazon VPC 中保留。可以将 Amazon VPC 终端节点用于任何类型的 Data API 调用。有关调用 Data API 的信息，请参阅调用 Amazon Redshift 数据 API 时的注意事项 (p. 268)。

调用 Data API

您可以调用数据 API 或 Amazon CLI 以在集群或无服务器工作组上运行 SQL 语句。运行 SQL 语句的主要操作是《Amazon Redshift 数据 API 参考》中的 `ExecuteStatement` 和 `BatchExecuteStatement`。数据 API 支持 Amazon 开发工具包所支持的编程语言。有关它们的更多信息，请参阅用于在 Amazon 上构建的工具。

要查看调用 Data API 的代码示例，请参阅 GitHub 中的 Redshift 数据 API入门。此存储库包含使用 Amazon Lambda 从 Amazon EC2、Amazon Glue Data Catalog 和 Amazon SageMaker 访问 Amazon Redshift 数据的示例。示例编程语言包括 Python、Go、Java 和 Javascript。

您可以使用 Amazon CLI 调用 Data API。

以下示例使用 Amazon CLI 调用数据 API。要运行示例，请编辑参数值以匹配您的环境。在许多示例中，会提供 `cluster-identifier` 以针对集群运行。在针对无服务器工作组运行时，需改为提供 `workgroup-name`。这些示例演示了一些数据 API 操作。有关更多信息，请参阅 Amazon CLI 命令参考。

以下示例中的命令已被拆分和格式化以便于阅读。

运行 SQL 语句

要运行 SQL 语句，请使用 `aws redshift-data execute-statement` Amazon CLI 命令。

以下 Amazon CLI 命令针对集群运行一个 SQL 语句，并返回一个标识符来获取结果。此示例使用 Amazon Secrets Manager 身份验证方法。

```
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
```

以下为响应示例。

```
{
    "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"
}
```

以下 Amazon CLI 命令针对集群运行一个 SQL 语句，并返回一个标识符来获取结果。此示例使用临时凭证身份验证方法。

```
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"
```

以下为响应示例。

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

以下 Amazon CLI 命令针对无服务器工作组运行一个 SQL 语句，并返回一个标识符来获取结果。此示例使用临时凭证身份验证方法。

```
aws redshift-data execute-statement
    --database dev
    --workgroup-name myworkgroup
    --sql "select 1;"
```

以下为响应示例。

```
{
 "CreatedAt": "2022-02-11T06:25:28.748000+00:00",
 "Database": "dev",
 "DbUser": "IAMR:RoleName",
 "Id": "89dd91f5-2d43-43d3-8461-f33aa093c41e",
 "WorkgroupName": "myworkgroup"
}
```

运行带有参数的 SQL 语句

要运行 SQL 语句，请使用 `aws redshift-data execute-statement` Amazon CLI 命令。

以下 Amazon CLI 命令针对集群运行一个 SQL 语句，并返回一个标识符来获取结果。此示例使用 Amazon Secrets Manager 身份验证方法。SQL 文本具有命名参数 `colname` 和 `distance`。在这种情况下，表中的列名为 `ratecode` 并且谓词中使用的距离是 `5`。SQL 语句的命名参数值在 `parameters` 选项中指定。

```
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 :colname, COUNT(*) FROM demo_table WHERE trip_distance > :distance"
    --parameters "[{\"name\": \"colname\", \"value\": \"ratecode\"}, \ {\"name\":
 \"distance\", \"value\": \"5\"}]"
    --database dev
```

以下为响应示例。

```
{
    "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"
}
```

以下示例使用示例数据库中的 `EVENT` 表。有关 COPY 语法的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 EVENT 表。

如果您的数据库中没有 `EVENT` 表，则可以使用数据 API 创建一个，如下所示：

```
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)"
```

以下命令将一个行插入 `EVENT` 表。

```
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\"}]"
```

以下命令将另一个行插入 `EVENT` 表。该示例演示以下内容：

- 名为 id 参数在 SQL 文本中使用了四次。
- 插入参数 starttime 时自动应用隐式类型转换。
- venueid 列是转换为 SMALINT 数据类型的类型。
- 表示 DATE 数据类型的字符串将隐式转换为 TIMESTAMP 数据类型。
- 注释可以在 SQL 文本中使用。

```
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\"}]"
```

下面显示了两个插入的行：

```
 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
```

以下命令使用 WHERE 子句中的命名参数来检索 eventid 为 1 的行。

```
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\"}]"
```

运行以下命令以获取上一个 SQL 语句的 SQL 结果：

```
aws redshift-data get-statement-result --id 7529ad05-b905-4d71-9ec6-8b333836eb5a
```

提供以下结果：

```
{
    "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
}
```


要运行多个 SQL 语句

要使用一个命令运行多个 SQL 语句，请使用 `aws redshift-data batch-execute-statement` Amazon CLI 命令。

以下 Amazon CLI 命令针对集群运行三个 SQL 语句，并返回一个标识符来获取结果。此示例使用临时凭证身份验证方法。

```
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"
```

以下为响应示例。


```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

要列出有关 SQL 语句的元数据

要列出有关 SQL 语句的元数据，请使用 `aws redshift-data list-statements` Amazon CLI 命令。运行此命令的授权基于调用者的 IAM 权限。

以下 Amazon CLI 命令列出了运行的 SQL 语句。

```
aws redshift-data list-statements
    --region us-west-2
    --status ALL
```

以下为响应示例。

```
{
    "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
        }
    ]
}
```

描述有关 SQL 语句的元数据

要获取 SQL 语句的元数据描述，请使用 `aws redshift-data describe-statement` Amazon CLI 命令。运行此命令的授权基于调用者的 IAM 权限。

以下 Amazon CLI 命令描述 SQL 语句。

```
aws redshift-data describe-statement
    --id d9b6c0c9-0747-4bf4-b142-e8883122f766
    --region us-west-2
```

以下为响应示例。

```
{
    "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
}
```

以下是使用多个 SQL 语句运行 `batch-execute-statement` 命令后的 `describe-statement` 响应示例。

```
{
    "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
}
```

获取 SQL 语句的结果

要从运行的 SQL 语句中获取结果，请使用 `redshift-data get-statement-result` Amazon CLI 命令。您可以提供响应 `execute-statement` 或者 `batch-execute-statement` 而收到的 `Id`。可以在 `describe-statement` 的结果中检索 `batch-execute-statement` 运行的 SQL 语句的 `Id` 值，并以

冒号和 b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2 等序号为该值添加后缀。如果使用 batch-execute-statement 运行多个 SQL 语句，则每个 SQL 语句都有一个 Id 值，如 describe-statement 中所示。运行此命令的授权基于调用者的 IAM 权限。

以下语句返回 execute-statement 运行的 SQL 语句的结果。

```
aws redshift-data get-statement-result
    --id d9b6c0c9-0747-4bf4-b142-e8883122f766
    --region us-west-2
```

以下语句返回 batch-execute-statement 运行的第二个 SQL 语句的结果。

```
aws redshift-data get-statement-result
    --id b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2
    --region us-west-2
```

以下是 get-statement-result 调用的响应的示例。

```
{
    "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
}
```

要描述表

要获取描述表的元数据，请使用 `aws redshift-data describe-table` Amazon CLI 命令。

以下 Amazon CLI 命令针对集群运行一个 SQL 语句，并返回描述表的元数据。此示例使用 Amazon Secrets Manager 身份验证方法。

```
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
```

以下为响应示例。

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

以下 Amazon CLI 命令针对集群运行一个 SQL 语句来描述表。此示例使用临时凭证身份验证方法。

```
aws redshift-data describe-table
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --schema information_schema
    --table sql_features
```

以下为响应示例。

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

要列出集群中的数据库

要列出集群中的数据库，请使用 `aws redshift-data list-databases` Amazon CLI 命令。

以下 Amazon CLI 命令针对集群运行一个 SQL 语句来列出数据库。此示例使用 Amazon Secrets Manager 身份验证方法。

```
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
```

以下为响应示例。

```
{
    "Databases": [
        "dev"
    ]
}
```

以下 Amazon CLI 命令针对集群运行一个 SQL 语句来列出数据库。此示例使用临时凭证身份验证方法。

```
aws redshift-data list-databases
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
```

以下为响应示例。

```
{
    "Databases": [
        "dev"
    ]
}
```

要列出数据库中的 schema

要列出数据库中的 schema，请使用 `aws redshift-data list-schemas` Amazon CLI 命令。

以下 Amazon CLI 命令针对集群运行一个 SQL 语句来列出数据库中的架构。此示例使用 Amazon Secrets Manager 身份验证方法。

```
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
```

以下为响应示例。

```
{
    "Schemas": [
        "information_schema",
        "pg_catalog",
        "pg_internal",
        "public"
    ]
}
```

以下 Amazon CLI 命令针对集群运行一个 SQL 语句来列出数据库中的架构。此示例使用临时凭证身份验证方法。

```
aws redshift-data list-schemas
    --region us-west-2
    --db-user mysuser
    --cluster-identifier mycluster-test
    --database dev
```

以下为响应示例。

```
{
    "Schemas": [
        "information_schema",
        "pg_catalog",
        "pg_internal",
        "public"
    ]
}
```

要列出数据库中的表

要列出数据库中的表，请使用 `aws redshift-data list-tables` Amazon CLI 命令。

以下 Amazon CLI 命令针对集群运行一个 SQL 语句来列出数据库中的表。此示例使用 Amazon Secrets Manager 身份验证方法。

```
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
```

以下为响应示例。

```
{
    "Tables": [
        {
            "name": "sql_features",
            "schema": "information_schema",
```

```
            "type": "SYSTEM TABLE"
        },
        {
            "name": "sql_implementation_info",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        }
}
```

以下 Amazon CLI 命令针对集群运行一个 SQL 语句来列出数据库中的表。此示例使用临时凭证身份验证方法。

```
aws redshift-data list-tables
     --region us-west-2
     --db-user myuser
     --cluster-identifier mycluster-test
     --database dev
     --schema information_schema
```

以下为响应示例。

```
{
    "Tables": [
        {
            "name": "sql_features",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        },
        {
            "name": "sql_implementation_info",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        }
    ]
}
```

Amazon Redshift 数据 API 的问题排查

使用以下部分（标题为常见错误消息）帮助解决 Data API 问题。

主题

- 用于查询的包太大 (p. 289)
- 数据库响应超出大小限制 (p. 289)

用于查询的包太大

如果您看到一条错误，指示查询的数据包过大，则为行返回的结果集通常过大。数据库返回的结果集中的 Data API 大小限制为每行 64 KB。

要解决此问题，请确保结果集中的每一行都小于或等于 64 KB。

数据库响应超出大小限制

如果您看到一条错误，指示数据库响应超出了大小限制，则数据库返回的结果集的大小通常太大。数据库返回的结果集中的数据 API 限制为 100 MB。

要解决此问题，请确保对数据 API 的调用返回 100 MB 或更少数据。如果需要返回 100 MB 以上的数据，您可以在查询中将多个语句调用与 `LIMIT` 子句结合使用。

使用 Amazon EventBridge 计划 Amazon Redshift 数据 API 操作

Amazon EventBridge 可帮助您响应您 Amazon 资源的状态更改。当您的资源的状态发生变化时，会自动向事件流发送事件。事件将发送到包含 Amazon Redshift 数据库的账户。您可以创建规则来匹配流中的选定事件并将它们路由到目标以采取操作。此外，您还可以使用规则对预定的计划采取操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。

要使用 EventBridge 计划数据 API 操作，关联的 IAM 角色必须信任 CloudWatch Events (events.amazonaws.com) 的委托人。此角色应附加相当于托管策略 `AmazonEventBridgeFullAccess` 的策略。它还应具有 `AmazonRedshiftDataFullAccess` 策略权限，这些权限由数据 API 管理。您可以在 IAM 控制台上创建具有这些权限的 IAM 角色。在 IAM 控制台上创建角色时，为 CloudWatch Events 选择 Amazon 服务可信任实体。有关创建 IAM 角色的更多信息，请参阅 IAM 用户指南中的为 Amazon 服务（控制台）创建一个角色。

以下示例使用 Amazon CLI 创建用于运行 SQL 语句的 EventBridge 规则。

```
aws events put-rule
--name test-redshift-data
--schedule-expression "rate(1 minute)"
```

然后创建一个 EventBridge 目标，以按照规则中指定的计划运行。

```
aws events put-targets
--cli-input-json file://data.json
```

输入 data.json 文件如下。

```
{
    "Rule": "test-redshift-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-scheduler-statement",
                "WithEvent": true
            }
        }
    ]
}
```

监控数据 API

监控是保持数据 API 和您的其他 Amazon 解决方案的可靠性、可用性和性能的重要方面。Amazon 提供了以下一些监控工具来监控数据 API、在出现错误时进行报告并适时自动采取措施：

- 您可以使用 Amazon EventBridge 自动执行您的 Amazon 服务并自动响应系统事件，例如应用程序可用性问题或资源更改。Amazon 服务中的事件将近乎实时地传输到 EventBridge。您可以编写简单的规则

来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。

- Amazon CloudTrail 捕获由您的 Amazon 账户或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Simple Storage Service（Amazon S3）存储桶。您可以标识哪些用户和账户调用了 Amazon、从中发出调用的源 IP 地址以及调用的发生时间。要了解有关 Amazon Redshift 如何与 Amazon CloudTrail 集成的更多信息，请参阅使用 Cloudtrail 进行日志记录。有关 CloudTrail 的更多信息，请参阅《Amazon CloudTrail 用户指南》。

主题

- 在 Amazon EventBridge 中监控 Amazon Redshift 数据 API 的事件 (p. 291)

在 Amazon EventBridge 中监控 Amazon Redshift 数据 API 的事件

您可以在 EventBridge 中监控数据 API，这将从您自己的应用程序、软件即服务 (SaaS) 应用程序和 Amazon 服务传输实时数据流。EventBridge 将该数据路由到诸如 Amazon Lambda 和 Amazon SNS 之类的目标。这些事件与 CloudWatch Events 中出现的事件相同，可提供近乎实时的系统事件流，这些系统事件描述 Amazon 资源的变化。事件将发送到包含 Amazon Redshift 数据库的账户。例如，如果您担任另一个账户中的角色，则事件将发送到该帐户。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 事件。

当 `ExecuteStatement` 或 `BatchExecuteStatement` API 操作将 `WithEvent` 选项设置为 `true` 时，将发送数据 API 事件。事件的 `state` 字段包含以下值之一：

- 中止 – 用户停止了查询运行。
- FAILED – 查询运行失败。
- FINISHED – 查询已完成运行。

事件会确保送达。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 Events from Amazon services。

数据 API 完成事件示例

以下示例在 `ExecuteStatement` API 操作完成时显示数据 API 的一个事件。在以下示例中，名为 `test.testtable` 的语句运行完成。

```
{
    "version": "0",
    "id": "18e7079c-dd4b-dd64-caf9-e2a31640dab0",
    "detail-type": "Redshift Data Statement Status Change",
    "source": "aws.redshift-data",
    "account": "123456789012",
    "time": "2020-10-01T21:14:26Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:redshift:us-east-1:123456789012:cluster:redshift-cluster-1"
    ],
    "detail": {
        "principal": "arn:aws:iam::123456789012:user/myuser",
        "statementName": "test.testtable",
        "statementId": "dd2e1ec9-2ee3-49a0-819f-905fa7d75a4a",
        "redshiftQueryId": -1,
        "state": "FINISHED",
        "rows": 1,
        "expireAt": 1601673265
    }
```

```
}
```

Amazon Redshift 中的增强型 VPC 路由

在使用 Amazon Redshift 增强型 VPC 路由时，Amazon Redshift 会强制通过基于 Amazon VPC 服务的 Virtual Private Cloud (VPC) 路由集群和数据存储库之间的所有 COPY 和 UNLOAD 流量。通过使用增强型 VPC 路由，您可以使用标准 VPC 功能，例如 VPC 安全组、网络访问控制列表 (ACL)、VPC 终端节点、VPC 终端节点策略、互联网 网关和域名系统 (DNS) 服务器，如 Amazon VPC 用户指南中所述。您可以使用这些功能来严格管理 Amazon Redshift 集群与其他资源之间的数据流。在使用增强型 VPC 路由以通过 VPC 路由流量时，您还可以使用 VPC 流日志监视 COPY 和 UNLOAD 流量。

如果未启用增强型 VPC 路由，则 Amazon Redshift 会通过 互联网 路由流量，包括至 Amazon 网络中的其他服务的流量。

> Important
>
> 由于增强型 VPC 路由影响 Amazon Redshift 访问其他资源的方式，除非您正确配置了 VPC，否则 COPY 和 UNLOAD 命令可能会失败。您必须专门在集群的 VPC 和数据资源之间创建网络路径，如下所述。

在对启用了增强型 VPC 路由的集群运行 COPY 或 UNLOAD 命令时，VPC 使用最严格或最具体的可用网络路径将流量路由到指定的资源。

例如，可以在您的 VPC 中配置以下路径：

- VPC 终端节点 – 对于传输到集群所在 Amazon 区域中的 Simple Storage Service（Amazon S3）存储桶的流量，您可以创建 VPC 终端节点来将流量直接传送到该存储桶。在使用 VPC 终端节点时，您可以附加端点策略来管理对 Simple Storage Service（Amazon S3）的访问。有关将端点与 Amazon Redshift 结合使用的更多信息，请参阅使用 VPC 终端节点 (p. 294)。如果您使用的是 Lake Formation，则可以在 Amazon Lake Formation 和接口 VPC 端点 (Amazon PrivateLink) 中找到有关在 VPC 和 Amazon Lake Formation 之间建立私有连接的更多信息。
- NAT 网关 – 您可以连接到另一个 Amazon 区域中的 Simple Storage Service（Amazon S3）存储桶，并且可以连接到 Amazon 网络中的另一个服务。您还可以访问 Amazon 网络外部的主机实例。为此，请配置网络地址转换 (NAT) 网关，如 Amazon VPC 用户指南中所述。
- 互联网网关 – 要连接到 VPC 外部的 Amazon 服务，您可以将互联网网关附加到您的 VPC 子网，如 Amazon VPC 用户指南中所述。要使用 Internet 网关，您的集群必须具有一个公有 IP 来允许其他服务与您的集群进行通信。

有关更多信息，请参阅 Amazon VPC 用户指南中的 VPC 终端节点。

使用增强型 VPC 路由不会产生任何额外的费用。您可能需要为某些操作支付额外的数据传输费用。其中包括在不同 Amazon 区域中 UNLOAD 到 Simple Storage Service（Amazon S3）之类的操作。使用公有 IP 地址从 Amazon EMR 或安全外壳 (SSH) 执行 COPY。有关定价的更多信息，请参阅 Amazon EC2 定价。

主题

- 使用 VPC 终端节点 (p. 294)
- 启用增强型 VPC 路由 (p. 294)
- 将 Amazon Redshift Spectrum 与增强型 VPC 路由一起使用 (p. 295)

使用 VPC 终端节点

您可以使用 VPC 终端节点创建 VPC 中的 Amazon Redshift 集群与 Amazon Simple Storage Service（Amazon S3）之间的托管连接。在执行此操作时，您的集群与 Simple Storage Service（Amazon S3）数据之间的 COPY 和 UNLOAD 流量将保留在您的 Amazon VPC 中。可以将终端节点策略附加到您的终端节点，以便更严格地管理对数据的访问。例如，可以向 VPC 终端节点添加策略以仅允许将数据上载到您账户中的特定 Simple Storage Service（Amazon S3）存储桶。

> Important
>
> 目前，Amazon Redshift 仅支持连接到 Simple Storage Service（Amazon S3）的 VPC 终端节点。当 Amazon VPC 添加对其他 Amazon 服务的支持以使用 VPC 终端节点时，Amazon Redshift 也将支持这些 VPC 终端节点连接。要使用 VPC 终端节点连接到 Simple Storage Service（Amazon S3）存储桶，该 Amazon Redshift 集群与其连接到的 Simple Storage Service（Amazon S3）存储桶必须在同一个 Amazon 区域。

要使用 VPC 终端节点，请为集群所在的 VPC 创建 VPC 终端节点，然后为集群启用增强型 VPC 路由。可以在 VPC 中创建集群时启用增强型 VPC 路由，也可以修改 VPC 中的集群以使用增强型 VPC 路由。

VPC 终端节点使用路由表来控制 VPC 中的集群和 Simple Storage Service（Amazon S3）之间的流量路由。与指定路由表关联的子网中的所有集群会自动使用该终端节点来访问服务。

您的 VPC 使用与集群流量匹配的最具体的/最严格的路由来决定路由流量的方式。例如，假设路由表中有一条路由用于所有指向互联网网关和 Simple Storage Service（Amazon S3）端点的互联网流量 (0.0.0.0/0)。在这种情况下，对所有传送到 Simple Storage Service（Amazon S3）的流量优先使用端点路由。这是因为 Simple Storage Service（Amazon S3）服务的 IP 地址范围比 0.0.0.0/0 更具体。在此示例中，所有其他互联网流量（包括定位到其他 Amazon 区域内的 Simple Storage Service（Amazon S3）存储桶的流量）将流向互联网网关。

有关创建端点的更多信息，请参阅《Amazon VPC 用户指南》中的创建 VPC 端点。

您使用端点策略控制从集群到包含数据文件的 Simple Storage Service（Amazon S3）存储桶的访问。要实现更具体的控制，您可以选择附加一个自定义终端节点策略。有关更多信息，请参阅 Amazon PrivateLink 指南中的使用端点策略控制对服务的访问权限。

使用终端节点不收取任何额外费用。采用标准的数据传输和资源使用计费方式。有关定价的更多信息，请参阅 Amazon EC2 定价。

启用增强型 VPC 路由

您可以在创建集群时启用增强型 VPC 路由，也可以修改现有集群以启用增强型 VPC 路由。

要使用增强型 VPC 路由，集群必须满足以下要求和约束：

- 集群必须在 VPC 中。

  如果您附加一个 Simple Storage Service（Amazon S3）VPC 终端节点，则集群仅使用该 VPC 终端节点来访问同一 Amazon 区域中的 Simple Storage Service（Amazon S3）存储桶。要访问其他 Amazon 区域中的存储桶（不使用 VPC 终端节点）或访问其他Amazon服务，请使您的集群可公开访问，或者使用网络地址转换 (NAT) 网关。有关更多信息，请参阅在 VPC 中创建集群 (p. 93)。
- 您必须在 VPC 中启用域名服务 (DNS) 解析。或者，如果您使用自己的 DNS 服务器，请确保将针对 Simple Storage Service（Amazon S3）的 DNS 请求正确解析为 Amazon 维护的 IP 地址。有关更多信息，请参阅 Amazon VPC 用户指南中的在您的 VPC 中使用 DNS。
- 必须在 VPC 中启用 DNS 主机名。DNS 主机名默认处于启用状态。
- 您的 VPC 终端节点策略必须允许访问用于 Amazon Redshift 中的 COPY、UNLOAD 或 CREATE LIBRARY 调用的任何 Simple Storage Service（Amazon S3）存储桶，包括访问涉及的任何清单文件。

对于从远程主机执行的 COPY 操作，您的终端节点策略必须允许访问每台主机。有关更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 COPY、UNLOAD 和 CREATE LIBRARY 的 IAM 权限。

创建具有增强型 VPC 路由的集群

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后选择 Create cluster（创建集群）并输入 Cluster details（集群详细信息）属性。
3. 要显示 Additional configurations (其他配置) 部分，请选择关闭 Use defaults (使用默认值)。
4. 要启用 Enhanced VPC routing (增强型 VPC 路由)，请选择 Enabled (启用) 以强制通过 VPC 的集群流量。
5. 选择 Create cluster (创建集群) 以创建集群。集群可能需要几分钟才可以使用。

您可以在 Amazon Redshift 中使用以下 Amazon Command Line Interface (Amazon CLI) 操作以启用增强型 VPC 路由：

- create-cluster ()
- modify-cluster

您可以使用以下 Amazon Redshift API 操作以启用增强型 VPC 路由：

- CreateCluster
- ModifyCluster

将 Amazon Redshift Spectrum 与增强型 VPC 路由一起使用

Amazon Redshift 增强型 VPC 路由通过 VPC 路由特定的流量。集群与 Simple Storage Service（Amazon S3）存储桶之间的所有流量都强制通过您的 Amazon VPC 传送。Redshift Spectrum 在 Amazon Redshift 拥有的 Amazon 托管资源上运行。由于这些资源位于 VPC 外部，Redshift Spectrum 不使用增强型 VPC 路由。

在集群配置为使用增强型 VPC 路由时，将通过 VPC 外部的 Amazon 私有网络安全地路由 Redshift Spectrum 和 Simple Storage Service（Amazon S3）之间的流量。使用 Amazon 签名版本 4 协议 (SIGv4) 签署正在传输的流量并使用 HTTPS 对该流量加密。此流量基于附加到 Amazon Redshift 集群的 IAM 角色进行授权。要进一步管理 Redshift Spectrum 流量，您可以修改集群的 IAM 角色以及附加到 Simple Storage Service（Amazon S3）存储桶的策略。您可能还需要配置 VPC 以允许集群访问 Amazon Glue 或 Athena，如下详述。

请注意，由于增强型 VPC 路由影响 Amazon Redshift 访问其他资源的方式，除非您正确配置了 VPC，否则查询可能会失败。有关更多信息，请参阅Amazon Redshift 中的增强型 VPC 路由 (p. 293)，其中更详细地讨论了如何创建 VPC 端点、NAT 网关和其他联网资源以将流量引导到 Amazon S3 存储桶。

在 Redshift Spectrum 中使用增强型 VPC 路由的注意事项

以下是使用 Redshift Spectrum 增强型 VPC 路由时的注意事项：

- 存储桶访问策略 (p. 296)

- 集群 IAM 角色 (p. 296)
- 记录和审计 Simple Storage Service（Amazon S3）访问 (p. 297)
- 访问 Amazon Glue 或 Amazon Athena (p. 297)

存储桶访问策略

您可以使用附加到存储桶的存储桶策略以及使用连接到集群的 IAM 角色来控制对 Simple Storage Service（Amazon S3）存储桶中数据的访问。

Redshift Spectrum 无法访问存储在下面这样的 Simple Storage Service（Amazon S3）存储桶中的数据：此类存储桶使用的存储桶策略限制仅访问指定的 VPC 终端节点。相反，应使用限制仅访问特定委托人（例如特定Amazon账户或特定用户）的存储桶策略。

对于被授予存储桶访问权限的 IAM 角色，请使用允许仅由 Amazon Redshift 服务委托人代入该角色的信任关系。该角色附加到集群时，只能在 Amazon Redshift 的上下文中使用，并且不能在集群外部共享。有关更多信息，请参阅限制对 IAM 角色的访问 (p. 426)。

要使用 Redshift Spectrum，不能制定任何阻止使用预签名 URL 的 IAM policy。

以下示例存储桶策略仅允许从Amazon账户 `123456789012` 拥有的 Redshift Spectrum 发起的流量访问指定存储桶。

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "BucketPolicyForSpectrum",
  "Effect": "Allow",
  "Principal": {
   "AWS": ["arn:aws:iam::123456789012:root"]
  },
  "Action": ["s3:GetObject", "s3:List*"],
  "Resource": ["arn:aws:s3:::examplebucket/*"],
  "Condition": {
   "StringEquals": {
    "aws:UserAgent": "AWS Redshift/Spectrum"
   }
  }
 }]
}
```

集群 IAM 角色

附加到集群的角色应该具有信任关系，只允许 Amazon Redshift 服务代入它，如下所示。

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

您可以向集群角色添加策略，以防止 COPY 和 UNLOAD 访问特定存储桶。以下策略仅允许从 Redshift Spectrum 到指定存储桶的流量。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["s3:Get*", "s3:List*"],
        "Resource": "arn:aws:s3:::myBucket/*",
                "Condition": {"StringEquals": {"aws:UserAgent": "AWS Redshift/Spectrum"}}
    }]
}
```

有关更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 Amazon Redshift Spectrum 的 IAM policy。

记录和审计 Simple Storage Service（Amazon S3）访问

使用 Amazon Redshift 增强型 VPC 路由的一个好处是，在 VPC 流日志中记录所有 COPY 和 UNLOAD 流量。源自 Redshift Spectrum 且传入 Simple Storage Service（Amazon S3）的流量不会通过您的 VPC，因此它不会记录在 VPC 流日志中。当 Redshift Spectrum 访问 Simple Storage Service（Amazon S3）中的数据时，它会在 Amazon 账户和相应角色权限的上下文中执行这些操作。您可以使用 Amazon CloudTrail 和 Simple Storage Service（Amazon S3）中的服务器访问日志记录来记录和审计 Simple Storage Service（Amazon S3）访问。

确保将 S3 IP 范围添加到您的允许列表中。要了解有关所需 S3 IP 范围的更多信息，请参阅 Network isolation（网络隔离）。

Amazon CloudTrail 日志

要跟踪 Simple Storage Service（Amazon S3）中对象的所有访问，包括 Redshift Spectrum 访问，请为 Simple Storage Service（Amazon S3）对象启用 CloudTrail 日志记录。

您可以使用 CloudTrail 来查看、搜索、下载、归档、分析和响应您的 Amazon 基础设施中的账户活动。有关更多信息，请参阅 CloudTrail 入门。

预设情况下，CloudTrail 仅跟踪存储桶级别的操作。要跟踪对象级别的操作（例如 `GetObject`），请为每个已记录的存储桶启用数据和管理事件。

Amazon S3 服务器访问日志记录

服务器访问日志记录详细地记录对存储桶提出的各种请求。访问日志信息可能在安全和访问审计方面十分有用。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的如何启用服务器访问日志记录。

有关更多信息，请参阅 Amazon 安全博客文章如何使用存储桶策略并应用深度防御来帮助保护您的 Simple Storage Service（Amazon S3）数据。

访问 Amazon Glue 或 Amazon Athena

Redshift Spectrum 访问您在 Amazon Glue 或 Athena 中的数据目录。另一种选择是为您的数据目录使用专用的 Hive 元存储。

要允许访问 Amazon Glue 或 Athena，请使用互联网网关或 NAT 网关配置 VPC。配置 VPC 安全组以允许 Amazon Glue 和 Athena 的公有端点的出站流量。或者，您可以为 Amazon Glue 配置接口 VPC 终端节点以访问您的 Amazon Glue Data Catalog。当您使用 VPC 接口端点时，您的 VPC 与 Amazon Glue 之间的通信会在 Amazon 网络内进行。有关更多信息，请参阅创建接口终端节点。

可以在您的 VPC 中配置以下通道：

- 互联网网关 – 要连接到 VPC 外部的 Amazon 服务，您可以将互联网网关附加到您的 VPC 子网，如 Amazon VPC 用户指南中所述。要使用 Internet 网关，您的集群必须具有一个公有 IP 地址来允许其他服务与您的集群进行通信。

- NAT 网关 – 要连接到另一个 Amazon 区域中的 Simple Storage Service（Amazon S3）存储桶或 Amazon 网络中的另一种服务，可以配置网络地址转换（NAT）网关，如 Amazon VPC 用户指南中所述。使用此配置还可以访问 Amazon 网络外部的主机实例。

有关更多信息，请参阅Amazon Redshift 中的增强型 VPC 路由 (p. 293)。

Amazon Redshift 参数组

概览

在 Amazon Redshift 中，您可以将参数组与创建的每个集群相关联。参数组是一组适用于您在集群中创建的所有数据库的参数。这些参数可用于配置数据库设置，例如查询超时和日期样式。

关于参数组

每个参数组都拥有几个可用于配置数据库设置的参数。可用参数列表取决于参数组所属的参数组系列。参数组系列是参数组中的参数所适用的 Amazon Redshift 引擎版本。参数组系列名称的格式为 `redshift-version`，其中 *version* 是引擎版本。例如，最新的引擎版本为 `redshift-1.0`。

Amazon Redshift 为每个参数组系列提供一个默认的参数组。默认参数组中的每个参数都有预设值，并且无法修改。默认参数组名称的格式为 `default.parameter_group_family`，其中 *parameter_group_family* 是参数组所属引擎的版本。例如，`redshift-1.0` 版本的默认参数组的名称为 `default.redshift-1.0`。

> **Note**
>
> 目前，`redshift-1.0` 是 Amazon Redshift 引擎的唯一版本。因此，`default.redshift-1.0` 是唯一的默认参数组。

如果您想要使用与默认参数组不同的参数值，则必须创建自定义参数组，然后将其与您的集群相关联。最初，自定义参数组中的参数值与默认参数组中的参数值相同。由于值由 Amazon Redshift 预先设置，因此所有参数的初始 `source` 均为 `engine-default`。在您更改参数值之后，`source` 将变为 `user`，表明默认值被修改为现在的值。

> **Note**
>
> Amazon Redshift 控制台不会显示每个参数的 `source`。您必须使用Amazon Redshift API、Amazon CLI、或其中一个 Amazon 开发工具包才能查看 `source`。

对于您创建的参数组，您可以随时修改参数值，也可以将所有参数值重置为默认值。您还可以将其他参数组与某个集群相关联。在某些情况下，您可以修改与集群关联的参数组中的参数值，或者将其他参数组与集群关联。在这些情况下，您可能需要重新启动集群以使更新后的参数值生效。如果该集群发生故障并由 Amazon Redshift 重新启动，那么系统将在此时应用您所做的更改。如果集群在维护期间重启，则无法应用更改。有关更多信息，请参阅WLM 动态和静态属性 (p. 301)。

默认参数值

您可以通过下面的表一目了然地了解默认的参数值，并借助提供的相应链接详细了解每个参数。下面显示的是 `redshift-1.0` 参数组系列的默认值。

参数名称	值	更多信息
auto_analyze	true	Amazon Redshift 数据库开发人员指南中的 auto_analyze
datestyle	ISO、MDY	Amazon Redshift 数据库开发人员指南中的 datestyle

参数名称	值	更多信息
enable_case_sensitive_identifier	false	Amazon Redshift 数据库开发人员指南中的 enable_case_sensitive_identifier
enable_user_activity_logging	false	本指南中的数据库审计日志记录 (p. 443)
extra_float_digits	0	Amazon Redshift 数据库开发人员指南中的 extra_float_digits
max_concurrency_scaling_clusters	1	Amazon Redshift 数据库开发人员指南中的 max_concurrency_scaling_clusters
query_group	默认值	Amazon Redshift 数据库开发人员指南中的 query_group
require_ssl	false	本指南中的配置连接的安全选项 (p. 217)
search_path	$user、public	Amazon Redshift 数据库开发人员指南中的 search_path
statement_timeout	0	Amazon Redshift 数据库开发人员指南中的 statement_timeout
wlm_json_configuration	[{"auto_wlm":true}]	本指南中的配置工作负载管理 (p. 301)
use_fips_ssl	false	仅在您的系统需要与 FIPS 兼容时才启用与 FIPS 兼容的 SSL 模式。
auto_mv	true	《Amazon Redshift 数据库开发人员指南》中的自动具体化视图

Note

`max_cursor_result_set_size` 参数已弃用。有关游标结果集大小的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的游标约束。

您可以使用数据库中的 `SET` 命令临时覆盖参数。`SET` 命令仅覆盖当前会话持续时间内的参数。除了上表中列出的参数之外，您还可以通过在数据库中设置 `wlm_query_slot_count` 来临时调整槽位计数。`wlm_query_slot_count` 参数不适用于参数组中的配置。有关调整槽数的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 wlm_query_slot_count。有关临时覆盖其他参数的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的修改服务器配置。

使用 Amazon CLI 配置参数值

要使用 Amazon CLI 配置 Amazon Redshift 参数，您可以对特定的参数组使用 `modify-cluster-parameter-group` 命令。您可以在 `parameter-group-name` 中指定要修改的参数组。您可以使用 `parameters` 参数（针对 `modify-cluster-parameter-group` 命令）指定希望在参数组中修改的每个参数的名称/值对。

Note

这些是使用 Amazon CLI 配置 `wlm_json_configuration` 参数时需要考虑的一些特殊注意事项。此部分中的示例适用于除 `wlm_json_configuration` 之外的所有参数。有关使用 Amazon CLI 配置 `wlm_json_configuration` 的更多信息，请参阅配置工作负载管理 (p. 301)。

修改参数值之后，您必须重新启动与修改后的参数组相关联的所有集群。当系统正在应用值时，集群状态将针对 `ParameterApplyStatus` 显示 `applying`；当应用了这些值之后，该状态则变为 `pending-`

reboot。重新启动之后，您集群中的数据库便开始使用新的参数值。有关重新启动集群的更多信息，请参阅重新引导集群 (p. 87)。

Note

wlm_json_configuration 参数中包含一些动态属性，您无需重新启动相关联的集群即可应用更改。有关动态属性和静态属性的更多信息，请参阅 WLM 动态和静态属性 (p. 301)。

语法

下面的语法显示了如何使用 modify-cluster-parameter-group 命令配置参数。您可以指定 *parameter_group_name*，并使用实际参数来替换 *parameter_name* 和 *parameter_value*，以修改相应参数的值。如果您想同时修改多个参数，请使用空格将每个参数和值集合彼此分隔开来。

```
aws redshift modify-cluster-parameter-group --parameter-group-name parameter_group_name --
parameters ParameterName=parameter_name,ParameterValue=parameter_value
```

示例

下面的示例显示了如何配置 myclusterparametergroup 参数组的 statement_timeout 和 enable_user_activity_logging 参数。

Note

为了便于阅读，该示例分为多行显示出来；但在实际的 Amazon CLI 中，该示例显示为一行。

```
aws redshift modify-cluster-parameter-group
--parameter-group-name myclusterparametergroup
--parameters ParameterName=statement_timeout,ParameterValue=20000
 ParameterName=enable_user_activity_logging,ParameterValue=true
```

您可以使用控制台管理参数组。有关更多信息，请参阅使用控制台管理参数组 (p. 310)。

配置工作负载管理

在 Amazon Redshift 中，您可以使用工作负载管理 (WLM) 来定义可用的查询队列的数量，并定义如何将查询路由至这些队列以进行处理。WLM 是参数组配置的一部分。集群使用其关联的参数组中指定的 WLM 配置。

当您创建参数组时，默认 WLM 配置中包含一个队列，该队列最多可并发运行五个查询。如果您想要更好地控制查询处理，则可以添加更多队列并在每个队列中配置 WLM 属性。除非对其属性进行配置，否则您添加的每个队列都具有相同的默认 WLM 配置。

当您添加更多队列时，配置中的最后一个队列是默认队列。除非根据 WLM 配置中的标准将查询路由至另一个队列，否则该查询将由默认队列进行处理。您可以为默认队列指定模式和并发级别（查询槽），但不能为默认队列指定用户组或查询组。

与其他参数一样，您无法修改默认参数组中的 WLM 配置。与默认参数组相关联的集群始终使用默认的 WLM 配置。要修改 WLM 配置，请创建一个新的参数组，然后将该参数组与需要自定义 WLM 配置的所有集群相关联。

WLM 动态和静态属性

WLM 配置属性可以是动态的，也可以是静态的。您可以将动态属性应用于数据库而无需重新启动集群，但静态属性需要重新启动集群才能够使更改生效。有关静态和动态属性的更多信息，请参阅 WLM 动态和静态配置属性。

wlm_json_configuration 参数的属性

您可以使用 Amazon Redshift 控制台、Amazon CLI、Amazon Redshift API 或 Amazon 开发工具包之一配置 WLM。WLM 配置使用多个用于定义队列行为的属性，例如队列之间的内存分配、队列中可以并发运行的查询数量等。

Note

下列属性和其 Amazon Redshift 控制台名称一起显示，具体说明中提供了对应的 JSON 属性名称。

下表总结属性是适用于自动 WLM 还是手动 WLM。

WLM 属性	自动 WLM	手动 WLM
自动 WLM	是	是
启用短查询加速	是	是
短查询的最大运行时间	是	是
优先级	是	否
队列类型	是	是
队列名称	是	是
并发扩展模式	是	是
并发	否	是
用户组	是	是
用户组通配符	是	是
查询组	是	是
查询组通配符	是	是
Timeout	否	弃用
内存	否	是
查询监控规则	是	是

下面的列表介绍了可为每个队列配置的 WLM 属性。

自动 WLM

自动 WLM 设置为 `true` 以启动自动 WLM。自动 WLM 将 Concurrency on main（主集群上的并发）和 Memory (%)（内存 (%)）的值设置为 `Auto`。Amazon Redshift 管理查询并发性和内存分配。默认为 `true`。

JSON 属性：`auto_wlm`

启用短查询加速

短查询加速 (SQA) 让选定的短时查询优先于长时查询。SQA 在专用空间中执行短时查询，因此 SQA 查询不会被迫排在队列中的长时查询后面等待。使用 SQA，短时查询会更快地开始执行，用户会更快地看到结果。当您启用 SQA 时，还可以为短时查询指定最大运行时间。要启用 SQA，请指定 `true`。默认为 `false`。

JSON 属性：`short_query_queue`

短查询的最大运行时间

当您启用 SQA 时，可以指定 0 以允许 WLM 动态设置短查询的最大运行时间。或者，您也可以指定一个介于 1 到 20 秒之间的值（以毫秒为单位）。原设定值为 0。

JSON 属性：max_execution_time

Priority

优先级设置队列中运行的查询的优先级。要设置优先级，WLM mode (WLM 模式) 必须设置为 Auto WLM (自动 WLM)；也即 auto_wlm 必须为 true。优先级值可以是 highest、high、normal、low 和 lowest。默认为 normal。

JSON 属性：priority

队列类型

队列类型指定 Auto WLM (自动 WLM) 或 Manual WLM (手动 WLM) 使用的队列。将 queue_type 设置为 auto 或 manual。如果未指定，则默认值为 manual。

JSON 属性：queue_type

队列名称

队列的名称。可以根据业务需求设置队列的名称。队列名称在 WLM 配置中必须唯一，最多为 64 个字母数字字符、下划线或空格，并且不能包含引号。例如，如果您有一个 ETL 查询队列，则可将该队列命名为 ETL queue。此名称在指标、系统表值和 Amazon Redshift 控制台中用来标识队列。使用这些源中的名称的查询和报表需要能够处理名称的更改。以前，队列名称由 Amazon Redshift 生成。队列的默认名称为 Queue 1、Queue 2，依此类推，直至最后一个名为 Default queue 的队列。

Important

如果您更改队列名称，则 WLM 队列指标（例如 WLMQueueLength、WLMQueueWaitTime、WLMQueriesCompletedPerSecond、WLMQueryDuration、WLMR
等）的 QueueName 维度值也会发生更改。因此，如果您更改队列的名称，则可能需要更改已设置的 CloudWatch 警报。

JSON 属性：name

并发扩展模式

要在队列上启用并发扩展，请将 Concurrency Scaling mode (并发扩展模式) 设置为 auto。当路由到队列的查询数超过队列的已配置并发数时，符合条件的查询将转到扩展集群。当有槽位可用时，将在主集群上运行查询。默认为 off。

JSON 属性：concurrency_scaling

并发

手动 WLM 队列中可以并发运行的查询的数量。此属性仅适用于手动 WLM。如果启用了并发扩展，则当队列达到并发级别（查询槽）时，符合条件的查询将转到扩展集群。如果未启用并发扩展，则查询将在队列中等待，直到有槽位可用。范围介于 1-50 之间。

JSON 属性：query_concurrency

用户组

逗号分隔的用户组名称列表。当用户组成员在数据库中运行查询时，其查询将路由至与相应用户组相关联的队列。

JSON 属性：user_group

用户组通配符

用来指示是否对用户组启用通配符的布尔值。如果该值为 0，则禁用通配符；如果该值为 1，则启用通配符。启用通配符后，您可以在运行查询时使用“*”或“?”指定多个用户组。有关更多信息，请参阅通配符。

JSON 属性：`user_group_wild_card`

查询组

逗号分隔的查询组列表。当查询组成员在数据库中运行查询时，其查询将路由至与相应查询组相关联的队列。

JSON 属性：`query_group`

Query Group Wildcard

用来指示是否对查询组启用通配符的布尔值。如果该值为 0，则禁用通配符；如果该值为 1，则启用通配符。启用通配符后，您可以在运行查询时使用“*”或“?”指定多个查询组。有关更多信息，请参阅通配符。

JSON 属性：`query_group_wild_card`

超时 (ms)

WLM 超时 (`max_execution_time`) 已弃用。使用自动 WLM 时不可用。相反，使用 `query_execution_time` 创建查询监控规则 (QMR) 来限制经过的查询执行时间。有关更多信息，请参阅 WLM 查询监控规则。

查询在取消之前可以运行的最长时间，以毫秒为单位。在一些情况下，只读查询（例如 SELECT 语句）可能会由于 WLM 超时而取消。在这些情况下，WLM 会尝试根据 WLM 队列分配规则将该查询路由到下一个匹配的队列。如果查询不匹配任何其他队列定义，则取消查询；系统不会将其分配给默认队列。有关更多信息，请参阅 WLM 查询队列跳过。WLM 超时不适用于已进入 `returning` 状态的查询。要查看查询的状态，请参阅 STV_WLM_QUERY_STATE 系统表。

JSON 属性：`max_execution_time`

内存(%)

分配给队列的内存百分比。如果您要为至少一个队列指定内存百分比，则必须为所有其他队列指定内存百分比，且所有队列的百分比合计不超过 100%。如果所有队列上的内存分配低于 100%，则未分配的内存将由服务管理。服务可以临时将此未分配内存提供给请求额外内存进行处理的队列。

JSON 属性：`memory_percent_to_use`

查询监控规则

您可以使用 WLM 查询监控规则，根据标准或谓词持续监控您的 WLM 队列中有无您指定的查询。例如，您可监控倾向于使用额外系统资源的查询，然后在查询超过您指定的性能界限时启动指定的操作。

Note

如果您选择以编程方式创建规则，强烈建议您使用控制台生成包含在参数组定义中的 JSON。

您将一个查询监控规则与特定的查询队列相关联。您可以让每个队列有最多 25 个规则，并且所有队列的总限制为 25 个规则。

JSON 属性：`rules`

JSON 属性层次结构：

```
rules
    rule_name
    predicate
        metric_name
        operator
        value
    action
        value
```

对于每个规则，您可以指定以下属性：

- rule_name – 规则名称必须在 WLM 配置中是唯一的。规则名称最多可包含 32 个字母数字字符或下划线，且不能包含空格或引号。您可以让每个队列有八个规则，并且所有队列的总限制为八个规则。
  - predicate – 您最多可以为每个规则设置 3 个谓词。对于每个谓词，指定以下属性。
    - metric_name – 有关指标的列表，请参阅 Amazon Redshift 数据库开发人员指南中的查询监控指标。
    - operator – 操作包括 =、< 和 >。
    - value – 指定指标的可触发操作的阈值。
- action – 每个规则都与一个操作相关联。有效的操作是：
  - log
  - hop（仅适用于手动 WLM）
  - abort
  - change_query_priority（仅适用于自动 WLM）

以下示例显示名为 rule_1 的 WLM 查询监控规则的 JSON，带有两个谓词以及操作 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"
          }
        ]
```

有关这些属性以及用于配置查询队列的策略的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的实施工作负载管理。

使用 Amazon CLI 配置 wlm_json_configuration 参数

要配置 WLM，您需要修改 wlm_json_configuration 参数。wlm_json_configuration 属性值的最大大小为 8000 个字符。相应值采用 JavaScript 对象表示法 (JSON) 格式。如果您想要使用 Amazon CLI、Amazon Redshift API 或其中一个 Amazon 开发工具包来配置 WLM，则可以使用此部分的其余内容来了解如何为 wlm_json_configuration 参数构建 JSON 结构。

> **Note**
>
> 如果您使用 Amazon Redshift 控制台来配置 WLM，则无需了解 JSON 格式，因为您可以通过控制台轻松添加队列并配置其属性。有关使用控制台配置 WLM 的更多信息，请参阅修改参数组 (p. 310)。

示例

下面的示例是默认的 WLM 配置，定义了使用自动 WLM 的队列。

```
{
   "auto_wlm": true
}
```

示例

下面的示例是一个自定义 WLM 配置，它定义了一个并发级别（查询槽）为五的手动 WLM 队列。

```
{
   "query_concurrency":5
}
```

语法

默认的 WLM 配置非常简单，只有一个队列和一个属性。您可以添加更多队列并为 JSON 结构中的每个队列配置多种属性。以下语法表示您用于配置具有多种属性的多个队列的 JSON 结构：

```
[
   {
      "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",
                ...
             }
             ...

         ]"
   }
]
```

在上述示例中，以 q1 开头的代表性属性是第一个队列的数组中的对象。其中每个对象都是名称/值对；name 和 value 共同设置第一个队列的 WLM 属性。以 q2 开头的代表性属性是第二个队列的数组中的对象。如果您需要更多队列，则可以为每个增加的队列添加另一个数组并为每个对象设置属性。

修改 WLM 配置时，您必须涵盖队列的整个结构，即使您只是想更改队列中的一个属性也是如此。这是因为整个 JSON 结构以字符串的形式传递为 wlm_json_configuration 参数的值。

设置 Amazon CLI 命令的格式

使用 Amazon CLI 时，您需要为 wlm_json_configuration 参数指定具体格式。您使用的格式取决于您的客户端操作系统。操作系统可以采用不同的方式将 JSON 结构括起来，因此它可以根据命令行正确地进行传输。要详细了解如何在 Linux、Mac OS X 和 Windows 操作系统中构建相应命令，请参阅以下部分。有关封闭 Amazon CLI 中的 JSON 数据结构的差异的更多信息，一般情况下，请参阅 Amazon Command Line Interface 用户指南中的引用字符串。

示例

以下示例命令为名为 example-parameter-group 的参数组配置手动 WLM。该配置可启用短查询加速，其中短查询的最大运行时间设置为 0，这指示 WLM 可动态设置该值。ApplyType 设置为 dynamic。此设置表示对参数中的动态属性做出的所有更改都将立即应用，除非同时对配置做出了其他静态更改。该配置定义下列三个队列：

- 通过第一个队列，用户可以将 report 指定为其查询中的标签（在 query_group 属性中所指定的），以帮助他们将查询路由至该队列。对于 report* 标签，通配符搜索处于启用状态，因此标签无需完全相同，查询也可路由至该队列。例如，reports 和 reporting 都与此查询组匹配。此队列将分配所有队列总内存的 25%，并且最多可同时运行四个查询。查询限制为最大时间 20000 毫秒 (ms)。模式设置为自动，因此当队列的查询槽位已满时，符合条件的查询将发送到扩展集群。

- 通过第二个队列，作为数据库中 admin 或 dba 组成员的用户可以将其查询路由至队列以进行处理。对于用户组，通配符搜索处于禁用状态，因此用户必须与数据库中的组完全匹配，其查询才能路由至该队列。此队列将跨所有队列分配总内存的 40%，并且最多可同时运行五个查询。模式设置为关闭，因此管理员或 dba 组的成员发送的所有查询都在主集群上运行。
- 配置中的最后一个队列是默认队列。此队列将分配所有队列总内存的 35%，并且最多可同时处理五个查询。模式设置为自动。

Note

为了便于演示，该示例分为多行显示出来。实际命令中不得使用换行符。

```
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,
    "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,
    "concurrency_scaling": "off",
    "queue_type": "manual"
  },
  {
    "query_concurrency": 5,
    "query_group": [],
    "query_group_wild_card": 0,
    "user_group": [],
    "user_group_wild_card": 0,
    "concurrency_scaling": "auto",
    "queue_type": "manual"
  },
  {"short_query_queue": true}
]'
```

以下是为自动 WLM 配置配置 WLM 查询监控规则的示例。该示例创建一个名为 example-monitoring-rules 的参数组。该配置定义了和上一示例相同的三个队列，但不再指定 query_concurrency 和 memory_percent_to_use。该配置还添加了以下规则和查询优先级：

- 第一个队列定义名为 rule_1 的规则。该规则有两个谓词：query_cpu_time > 10000000 和 query_blocks_read > 1000。规则操作是 log。此队列的优先级为 Normal。
- 第二个队列定义名为 rule_2 的规则。该规则有两个谓词：query_execution_time > 600000000 和 scan_row_count > 1000000000。规则操作是 abort。此队列的优先级为 Highest。
- 配置中的最后一个队列是默认队列。此队列的优先级为 Low。

Note

为了便于演示，该示例分为多行显示出来。实际命令中不得使用换行符。

```
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,
  "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,
  "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,
  "concurrency_scaling" : "auto",
  "priority": "low",
  "queue_type": "auto",
  "auto_wlm": true
}, {
  "short_query_queue" : true
} ]'
```

在命令行中使用 Amazon CLI 和 JSON 文件以配置 WLM

您可以使用 Amazon CLI 修改 `wlm_json_configuration` 参数，并将 `parameters` 参数值作为 JSON 文件传递。

```
aws redshift modify-cluster-parameter-group --parameter-group-name myclusterparaametergroup
 --parameters file://modify_pg.json
```

--parameters 的参数存储在 modify_pg.json 文件中。文件位置是使用操作系统格式指定的。有关更多信息，请参阅从文件中加载参数。下面显示了 modify_pg.json JSON 文件的内容示例。

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

在 Linux 和 macOS X 操作系统上的命令行中使用 Amazon CLI 配置 WLM 的规则

请按照以下规则在一行中使用参数运行 Amazon CLI 命令：

- 整个 JSON 结构必须使用单引号 (') 和方括号 ([ ]) 括起来。
- 所有参数名称和参数值必须使用双引号 (") 括起来。
- 在 ParameterValue 值中，必须使用双引号 (") 和方括号 ([ ]) 将整个嵌套结构括起来。
- 在嵌套结构中，必须使用大括号 ({ }) 将每个队列的每个属性和值括起来。
- 在嵌套结构中，必须在每个双引号 (") 前面使用反斜杠 (\) 转义符。
- 对于名称/值对，使用冒号 (:) 将每个属性与其值分隔开来。
- 可使用逗号 (,) 将各个名称/值对彼此分隔开来。
- 多个队列可通过在一个队列结束的右大括号 (}) 和下一个队列开始的左大括号 ({) 之间使用逗号 (,) 分隔开来。

在 Microsoft Windows 操作系统上的 Windows PowerShell 中使用 Amazon CLI 配置 WLM 的规则

请按照以下规则在一行中使用参数运行 Amazon CLI 命令：

- 整个 JSON 结构必须使用单引号 (') 和方括号 ([ ]) 括起来。
- 所有参数名称和参数值必须使用双引号 (") 括起来。
- 在 ParameterValue 值中，必须使用双引号 (") 和方括号 ([ ]) 将整个嵌套结构括起来。
- 在嵌套结构中，必须使用大括号 ({ }) 将每个队列的每个属性和值括起来。
- 在嵌套结构中，必须在每个双引号 (") 及其反斜杠 (\) 转义符前面使用反斜杠 (\) 转义符。该要求意味着，您将使用三个反斜杠和一个双引号以确保正确传递属性 (\\\")。
- 对于名称/值对，使用冒号 (:) 将每个属性与其值分隔开来。

- 可使用逗号 (,) 将各个名称/值对彼此分隔开来。
- 多个队列可通过在一个队列结束的右大括号 (}) 和下一个队列开始的左大括号 ({) 之间使用逗号 (,) 分隔开来。

在 Windows 操作系统上使用命令提示符配置 WLM 的规则

请按照以下规则在一行中使用参数运行 Amazon CLI 命令：

- 整个 JSON 结构必须使用双引号 (") 和方括号 ([ ]) 括起来。
- 所有参数名称和参数值必须使用双引号 (") 括起来。
- 在 `ParameterValue` 值中，必须使用双引号 (") 和方括号 ([ ]) 将整个嵌套结构括起来。
- 在嵌套结构中，必须使用大括号 ({ }) 将每个队列的每个属性和值括起来。
- 在嵌套结构中，必须在每个双引号 (") 及其反斜杠 (\) 转义符前面使用反斜杠 (\) 转义符。该要求意味着，您将使用三个反斜杠和一个双引号以确保正确传递属性 (\\\")。
- 对于名称/值对，使用冒号 (:) 将每个属性与其值分隔开来。
- 可使用逗号 (,) 将各个名称/值对彼此分隔开来。
- 多个队列可通过在一个队列结束的右大括号 (}) 和下一个队列开始的左大括号 ({) 之间使用逗号 (,) 分隔开来。

使用控制台管理参数组

您可以在 Amazon Redshift 控制台中查看、创建、修改和删除参数组。

您可以查看任意参数组，查看参数值的摘要以及工作负载管理 (WLM) 配置。组参数显示在 Parameters (参数) 选项卡中，Workload queues (工作负载队列) 显示在 Workload Management (工作负载管理) 选项卡中。

创建参数组

如果您要设置与默认参数组不同的参数值，您可以创建您自己的参数组。

创建参数组

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Configurations（配置），然后选择 Workload management（工作负载管理），以显示 Workload management（工作负载管理）页面。
3. 选择 Create (创建) 显示 Create parameter group (创建参数组) 窗口。
4. 为 Parameter group name (参数组名称) 和 Description (说明) 输入一个值。
5. 选择 Create (创建) 以创建参数组。

修改参数组

您可以修改参数来更改参数设置和 WLM 配置属性。

> **Note**
>
> 您无法修改默认参数组。

修改参数组

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。

2. 在导航菜单上，选择 Configurations（配置），然后选择 Workload management（工作负载管理），以显示 Workload management（工作负载管理）页面。
3. 选择要修改的参数组以便显示详细信息页面，该页面带有 Parameters (参数) 和 Workload management (工作负载管理) 选项卡。
4. 选择 Parameters (参数) 选项卡查看当前参数设置。
5. 选择 Edit parameters (编辑参数) 以便允许更改以下参数的设置：

   - `auto_analyze`
   - `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`

   有关这些参数的更多信息，请参阅 Amazon Redshift 参数组 (p. 299)。
6. 输入所做的更改，然后选择 Save (保存) 更新参数组。

修改参数组的 WLM 配置

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Configurations（配置），然后选择 Workload management（工作负载管理），以显示 Workload management（工作负载管理）页面。
3. 选择要修改的参数组以便显示详细信息页面，该页面带有 Parameters (参数) 和 Workload management (工作负载管理) 选项卡。
4. 选择 Workload management (工作负载管理) 选项卡查看当前 WLM 配置。
5. 选择 Edit workload queues (编辑工作负载队列) 以编辑 WLM 配置。
6. （可选）选择 Enable short query acceleration (启用短查询加速) 以便启用短查询加速 (SQA)。

   当您启用 SQA 时，原定设置情况下 Maximum run time for short queries (1 to 20 seconds) (短查询的最大运行时间 (1 到 20 秒)) 将设置为 Dynamic (动态)。要将最大运行时设置为固定值，请选择一个介于 1–20 之间的值。
7. 执行以下一项或多项操作来修改队列配置：

   - 选择 Switch WLM mode (切换 WLM 模式) 可在 Automatic WLM (自动 WLM) 和 Manual WLM (手动 WLM) 之间选择。

     使用 Automatic WLM (自动 WLM) 时，Memory (内存) 和 Concurrency on main (主集群上的并发) 值设置为 auto (自动)。
   - 要创建队列，请选择 Edit workload queues (编辑工作负载队列)，然后选择 Add Queue (添加队列)。
   - 要修改队列，更改表中的属性值。根据队列类型，属性可能包括：
     - 可以更改 Queue name (队列名称)。
     - 内存(%)
     - 主集群上的并发

- 并发扩展模式可以为关闭或自动
- 超时 (ms)
- 用户组
- 查询组

有关这些属性的更多信息，请参阅wlm_json_configuration 参数的属性 (p. 302)。

Important

如果您更改队列名称，则 WLM 队列指标（例如 WLMQueueLength、WLMQueueWaitTime、WLMQueriesCompletedPerSecond、WLMQueryDuration、WLM 等）的 `QueueName` 维度值也会发生更改。因此，如果您更改队列的名称，则可能需要更改已设置的 CloudWatch 警报。

- 要更改队列顺序，请选择 Up (向上) 和 Down (向下) 箭头按钮。
- 要删除队列，在表中选择改队列所在行中的 Delete (删除)。

8. （可选）选择 Defer dynamic changes until reboot (推迟动态更改，直到重新启动) 以便在下次重启集群后对其应用更改。

   Note

   对于某些设置，无论此项设置为何，都要求在集群重启之后才生效。有关更多信息，请参阅WLM 动态和静态属性 (p. 301)。

9. 选择保存。

使用控制台创建或修改查询监控规则

您可以使用 Amazon Redshift 控制台创建和修改 WLM 查询监控规则。查询监控规则是一个参数组的 WLM 配置参数的一部分。如果修改查询监控规则 (QMR)，无需修改集群即可自动进行更改。有关更多信息，请参阅 WLM 查询监控规则。

创建规则时，您要定义规则名称、一个或多个谓词以及一个操作。

保存包含规则的 WLM 配置时，您可以将规则定义的 JSON 代码视为 WLM 配置参数的 JSON 的一部分。

创建查询监控规则

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Configurations（配置），然后选择 Workload management（工作负载管理），以显示 Workload management（工作负载管理）页面。
3. 选择要修改的参数组以便显示详细信息页面，该页面带有 Parameters (参数) 和 Workload management (工作负载管理) 选项卡。
4. 选择 Workload management (工作负载管理) 选项卡，然后选择 Edit workload queues (编辑工作负载队列) 以编辑 WLM 配置。
5. 使用预定义模板或从头开始添加新规则。

   要使用预定义模板，请执行以下操作：

   1. 选择 Query monitoring rules（查询监控规则）组中的 Add rule from template（从模板中添加规则）。此时将显示规则模板的列表
   2. 选择一个或多个规则模板。选择 Save (保存) 后，WLM 将为您选择的每个模板创建一个规则。
   3. 输入或确认规则的值，其中包括 Rule names (规则名称)、Predicates (谓词) 和 Actions (操作)。
   4. 选择保存。

要从头开始添加新规则，请执行以下操作：

1. 要添加其他谓词，请选择 Add predicate (添加谓词)。您最多可以为每个规则设置 3 个谓词。如果满足所有谓词，WLM 会触发关联操作。
2. 选择 Action。每个规则具有一个操作。
3. 选择保存。

Amazon Redshift 将生成 JSON 格式的 WLM 配置参数，并在 JSON 部分中显示它。

删除参数组

如果您不再需要某个参数组而且它并没有与任何集群相关联，您可以删除该参数组。您只能删除自定义参数组。

删除参数组

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Configurations（配置），然后选择 Workload management（工作负载管理），以显示 Workload management（工作负载管理）页面。
3. 对于 Parameter groups,，选择您要修改的参数组。

   Note

   您无法删除默认参数组。
4. 选择 Delete (删除) 并确认要删除参数组。

将参数组与集群相关联

当您启动集群时，您必须将它与一个参数组相关联。如果您在以后要更改参数组，可以修改集群并选择其他参数组。

使用 Amazon SDK for Java 管理参数组

本示例演示以下与参数组相关的任务：

- 创建参数组
- 修改参数组
- 将参数组与集群相关联
- 获取关于参数组的信息

此示例创建一个新的参数组 `parametergroup1`，然后进行以下更新：

- 将参数 `extra_float_digits` 从默认值 0 更改为 2。
- 使用以下 JSON 替换现有的工作负载管理配置（`wlm_json_configuration` 参数），其作用是在默认队列之外再定义一个队列。

```
[
   {
      "user_group":[
```

```
         "example_user_group1"
      ],
      "query_group":[
         "example_query_group1"
      ],
      "query_concurrency":7
   },
   {
      "query_concurrency":5
   }
]
```

前面的 JSON 是两个对象的数组，每个对象对应一个队列。第一个对象定义的队列具有特定的用户组和查询组。它还将并发级别设置为 7。

```
{
   "user_group":[
      "example_user_group1"
   ],
   "query_group":[
      "example_query_group1"
   ],
   "query_concurrency":7
}
```

因为此示例替换 WLM 配置，所以此 JSON 配置还定义了未指定特定用户组或查询组的默认队列。它将并发设置为默认值 5。

```
{
   "query_concurrency":5
}
```

有关工作负载管理 (WML) 配置的更多信息，请转到实施工作负载管理。

有关运行以下示例的分步说明，请参阅 使用 Eclipse 运行 Amazon Redshift 的 Java 示例 (p. 464)。您需要更新该代码并提供集群标识符。

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
*/

// snippet-sourcedescription:[CreateAndModifyClusterParameterGroup demonstrates how to
 create and modify an Amazon Redshift parameter group.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[CreateClusterParameterGroup]
// snippet-keyword:[DescribeClusterParameterGroups]
```

```
// snippet-keyword:[ModifyClusterParameterGroup]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-02-01]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.CreateAndModifyClusterParameterGroup.complete]

package com.amazonaws.services.redshift;

import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

import com.amazonaws.services.redshift.model.*;


public class CreateAndModifyClusterParameterGroup {

    public static AmazonRedshift client;
    public static String clusterParameterGroupName = "parametergroup1";
    public static String clusterIdentifier = "***provide a cluster identifier***";
    public static String parameterGroupFamily = "redshift-1.0";

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
 com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
       client = AmazonRedshiftClientBuilder.defaultClient();

        try {
             createClusterParameterGroup();
             modifyClusterParameterGroup();
             associateParameterGroupWithCluster();
             describeClusterParameterGroups();
        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }

    private static void createClusterParameterGroup() {
       CreateClusterParameterGroupRequest request = new
 CreateClusterParameterGroupRequest()
           .withDescription("my cluster parameter group")
           .withParameterGroupName(clusterParameterGroupName)
           .withParameterGroupFamily(parameterGroupFamily);
       client.createClusterParameterGroup(request);
       System.out.println("Created cluster parameter group.");
    }

    private static void describeClusterParameterGroups() {
       DescribeClusterParameterGroupsResult result =
 client.describeClusterParameterGroups();
       printResultClusterParameterGroups(result);
    }

    private static void modifyClusterParameterGroup() {
       List<Parameter> parameters = new ArrayList<Parameter>();
       parameters.add(new Parameter()
           .withParameterName("extra_float_digits")
           .withParameterValue("2"));
       // Replace WLM configuration. The new configuration defines a queue (in addition to
 the default).
       parameters.add(new Parameter()
       .withParameterName("wlm_json_configuration")
       .withParameterValue("[{\"user_group\":[\"example_user_group1\"],\"query_group\":
[\"example_query_group1\"],\"query_concurrency\":7},{\"query_concurrency\":5}]"));
```

```
      ModifyClusterParameterGroupRequest request = new
ModifyClusterParameterGroupRequest()
          .withParameterGroupName(clusterParameterGroupName)
          .withParameters(parameters);
      client.modifyClusterParameterGroup(request);

   }

   private static void associateParameterGroupWithCluster() {

       ModifyClusterRequest request = new ModifyClusterRequest()
       .withClusterIdentifier(clusterIdentifier)
       .withClusterParameterGroupName(clusterParameterGroupName);

       Cluster result = client.modifyCluster(request);

       System.out.format("Parameter Group %s is used for Cluster %s\n",
               clusterParameterGroupName,
result.getClusterParameterGroups().get(0).getParameterGroupName());
   }
   private static void
printResultClusterParameterGroups(DescribeClusterParameterGroupsResult result)
   {
       if (result == null)
       {
           System.out.println("\nDescribe cluster parameter groups result is null.");
           return;
       }

       System.out.println("\nPrinting parameter group results:\n");
       for (ClusterParameterGroup group : result.getParameterGroups()) {
           System.out.format("\nDescription: %s\n", group.getDescription());
           System.out.format("Group Family Name: %s\n", group.getParameterGroupFamily());
           System.out.format("Group Name: %s\n", group.getParameterGroupName());
           describeClusterParameters(group.getParameterGroupName());
       }
   }

   private static void describeClusterParameters(String parameterGroupName) {
       DescribeClusterParametersRequest request = new DescribeClusterParametersRequest()
           .withParameterGroupName(parameterGroupName);

       DescribeClusterParametersResult result = client.describeClusterParameters(request);
       printResultClusterParameters(result, parameterGroupName);
   }

   private static void printResultClusterParameters(DescribeClusterParametersResult
result, String parameterGroupName)
   {
       if (result == null)
       {
           System.out.println("\nCluster parameters is null.");
           return;
       }

       System.out.format("\nPrinting cluster parameters for \"%s\"\n",
parameterGroupName);
       for (Parameter parameter : result.getParameters()) {
           System.out.println("  Name: " + parameter.getParameterName() + ", Value: " +
parameter.getParameterValue());
           System.out.println("  DataType: " + parameter.getDataType() + ",
MinEngineVersion: " + parameter.getMinimumEngineVersion());
           System.out.println("  AllowedValues: " + parameter.getAllowedValues() + ",
Source: " + parameter.getSource());
           System.out.println("  IsModifiable: " + parameter.getIsModifiable() + ",
Description: " + parameter.getDescription());
```

```
        }
    }
}

// snippet-end:[redshift.java.CreateAndModifyClusterParameterGroup.complete]
```

使用 Amazon CLI 和 Amazon Redshift API 管理参数组

您可以使用 Amazon CLI 中的以下 Amazon Redshift 操作来管理参数组。

- 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

您可以使用以下 Amazon Redshift API 操作来管理参数组。

- CreateClusterParameterGroup
- DeleteClusterParameterGroup
- DescribeClusterParameters
- DescribeClusterParameterGroups
- DescribeDefaultClusterParameters
- ModifyClusterParameterGroup
- ResetClusterParameterGroup

Amazon Redshift 快照

主题

- 概览 (p. 318)
- 自动快照 (p. 318)
- 自动快照计划 (p. 319)
- 快照计划格式 (p. 319)
- 手动快照 (p. 320)
- 管理快照存储 (p. 321)
- 从快照中排除表 (p. 321)
- 将快照复制到另一个 Amazon 区域 (p. 321)
- 从快照还原集群 (p. 322)
- 从快照中还原表 (p. 324)
- 共享快照 (p. 325)
- 使用控制台管理快照 (p. 326)
- 使用 Amazon SDK for Java 管理快照 (p. 331)
- 使用 Amazon CLI 和 Amazon Redshift API 管理快照 (p. 334)

概览

快照是集群的时间点备份。存在两种类型的快照：自动和手动。Amazon Redshift 通过使用加密的安全套接字层 (SSL) 连接，在 Amazon S3 内部存储这些快照。

Amazon Redshift 会自动拍摄递增快照，来跟踪自上次自动快照拍摄以来集群发生的变化。自动快照保留从快照还原集群所需的全部数据。您可以创建快照计划来控制何时拍摄自动快照，也可以随时拍摄手动快照。

当您从快照还原时，Amazon Redshift 将创建一个新集群并使该新集群在所有数据都已加载前可用，从而使您可以立即开始查询新集群。该集群将按需流式传输来自快照的数据以响应活动查询，然后在后台加载剩余的数据。

在启动集群时，可以设置自动快照和手动快照的保留期。您可以通过修改集群来更改自动快照和手动快照的默认保留期。您可以在创建快照时或通过修改快照来更改手动快照的保留期。

您可以通过下列方式监控快照进度：在 Amazon Web Services Management Console中查看快照详细信息、调用 CLI 中的 describe-cluster-snapshots 或调用 DescribeClusterSnapshots API 操作。对于正在进行的快照，通过上述方式可以看到增量快照的大小、传输速率、已用时间以及估计的剩余时间等信息。

为了确保您的备份始终对集群可用，Amazon Redshift 将快照存储在由 Amazon Redshift 管理的内部托管 Amazon S3 存储桶中。要管理存储费用，请估计需要将自动快照保留多少天并相应地配置其保留期。删除所有不再需要的手动快照。有关备份存储成本的更多信息，请参阅 Amazon Redshift 定价。

自动快照

当某个集群的自动快照处于启用状态时，Amazon Redshift 会定期拍摄该集群的快照。默认情况下，Amazon Redshift 大约每 8 小时或在每节点数据更改达到 5 GB 时拍摄一次快照，以先到者为准。或者，您也可以创建快照计划来控制何时拍摄自动快照。当您创建集群时，自动快照默认处于启用状态。

系统会在保留期结束时删除自动快照。默认保留期为一天；不过，您可以使用 Amazon Redshift 控制台对其进行修改，也可以使用 Amazon Redshift API 或 CLI 以编程方式对其进行修改。

要禁用自动快照，只需将保留期设置为零即可。如果您禁用自动快照，则 Amazon Redshift 会停止拍摄快照并删除相应集群的任何现有自动快照。您不能为 RA3 节点类型禁用自动快照。您可以将 RA3 节点类型的自动保留期设置为 1-35 天。

只有 Amazon Redshift 才能删除自动快照；您不能手动删除它们。Amazon Redshift 会在下列情况下删除自动快照：快照的保留期结束时、您禁用了集群的自动快照或您删除了集群。Amazon Redshift 会保留最新的自动快照，直到您禁用自动快照或删除集群为止。

如果您想要将自动快照保留更长时间，则可以创建一份副本作为手动快照。自动快照会保留至保留期结束；而相应的手动快照在您将其手动删除前或保留期结束前将会一直保留。

自动快照计划

要精确控制拍摄快照的时间，您可以创建快照计划并将其附加到一个或多个集群。修改快照计划时，将修改所有关联集群的计划。如果集群未附加快照计划，其将使用默认的自动快照计划。

快照计划 是一组计划规则。您可以基于指定的时间间隔（例如每 8 小时或每 12 小时）定义简单的计划规则。也可以添加规则来在一周中的某些天、特定时间或特定时段拍摄快照。此外，您还可以使用类 Unix 系统的 cron 表达式定义规则。

快照计划格式

您可以在 Amazon Redshift 控制台中创建快照计划。然后，您可以将计划附加到集群来触发创建系统快照。可以将计划附加到多个集群，也可以在计划中创建多个 cron 定义来触发快照。

您可以使用 cron 语法为快照定义计划。这些计划的定义使用经过修改的类 Unix 系统的 cron 语法。您可以使用协调世界时 (UTC) 格式指定时间。您可以创建最大频率为 1 小时、最小精度为 1 分钟的计划。

Amazon Redshift 修改后的 cron 表达式有 3 个必填字段，之间以空格分隔。

语法

```
cron(Minutes Hours Day-of-week)
```

字段	值	通配符
分钟	0-59	
小时	0–23	, - * /
星期几	1–7 或 SUN-SAT	, - * /

通配符

- , (逗号) 通配符包含其他值。在 `Day-of-week` 字段中，`MON,WED,FRI` 将包含星期一、星期三和星期五。总值限制为每字段 24 个。
- - (破折号) 通配符用于指定范围。在 `Hour` 字段中，1–15 将包含指定日期的 1 - 15 小时。

- * (星号) 通配符包含该字段中的所有值。在 Hours 字段中，* 将包含每个小时。
- / (正斜杠) 通配符用于指定增量。在 Hours 字段中，您可以输入 **1/10** 来指定从当天的第 1 个小时开始每隔 10 小时 (例如，01:00、11:00 和 21:00) 。

限制

- 不支持导致备份频率小于 1 小时或大于 24 小时的快照计划。如果您有重叠的计划导致在 1 小时时段内计划了多次快照，将产生验证错误。

在创建计划时，您可以使用以下示例 cron 字符串。

分钟	小时	星期几	意义			
0	14-20/1	TUE	星期二下午 2 点到晚上 8 点之间，每小时拍摄一次。			
0	21	MON-FRI	每天晚上 9 点，星期一至星期五。			
30	0/6	SAT-SUN	星期六和星期日从当天午夜 30 分 (00:30) 开始，每 6 小时拍摄一次。这导致在每天的 [00:30、06:30、12:30 和 18:30] 拍摄快照。			
30	12/4	*	每天从 12:30 开始，每 4 小时拍摄一次。这将解析为 [12:30、16:30、20:30]。			

例如，要运行每天从 15:15 开始、每 2 小时拍摄一次的计划 (解析为 [15:15、17:15、19:15、21:15、23:15]) ，请指定：

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

您可以在计划中创建多个 cron 计划定义。例如，以下 Amazon CLI 命令在一个计划中包含两个 cron 计划。

```
create-snapshot-schedule --schedule-identifier "my-test" --schedule-definition "cron(0 17
 SAT,SUN)" "cron(0 9,17 MON-FRI)"
```

手动快照

您可以随时制作手动快照。默认情况下，即使您删除相应集群，手动快照也会无限期保留。您可以在创建手动快照时指定保留期，也可以通过修改快照来更改保留期。有关更改保留期的更多信息，请参阅更改手动快照保留期 (p. 327)。

如果删除某个快照，则无法启动任何引用该快照的新操作。不过，如果某个还原操作正在进行中，则该还原操作会运行完成。

Amazon Redshift 设有配额，用以限制您能够创建的手动快照的总数；该配额因不同的 Amazon 账户及不同的 Amazon 区域而异。默认的配额列出在 Amazon Redshift 资源中的配额和限制 (p. 514) 中。

管理快照存储

由于快照会产生存储费用，因此，当您不再需要快照时，务必将其手动删除。在相应的快照保留期结束时，Amazon Redshift 将删除自动快照和手动快照。您也可以使用 Amazon Web Services Management Console 或 batch-delete-cluster-snapshots CLI 命令来删除手动快照。

您可以通过修改手动快照设置来更改手动快照的保留期。

您可以使用 Amazon Redshift 控制台或 describe-storage CLI 命令获取有关快照占用的存储量的信息。

从快照中排除表

默认情况下，所有用户定义的永久表都包含在快照中。如果表（如暂存表）不需要备份，您可以显著降低创建快照并从快照还原所需的时间。您还可以使用无备份表减小在 Amazon S3 上占用的存储空间。要创建无备份表，请在创建该表时包含 BACKUP NO 参数。有关语法的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 CREATE TABLE 和 CREATE TABLE AS。

将快照复制到另一个 Amazon 区域

您可以配置 Amazon Redshift，以将集群的快照（自动或手动）自动复制到另一个 Amazon 区域。在集群的主要 Amazon 区域创建快照时，它会复制到辅助 Amazon 区域。这两个 Amazon 区域分别称为源 Amazon 区域和目标 Amazon 区域。如果您在另一个 Amazon 区域中存储快照副本，则在有任何事情影响主要 Amazon 区域时，您可以使用最新数据还原集群。您可以配置集群，一次仅将快照复制到一个目标 Amazon 区域。有关 Amazon Redshift 区域的列表，请参阅 Amazon Web Services 一般参考中的区域和端点。

启用 Amazon Redshift 以自动将快照复制到另一个 Amazon 区域时，您需要指定要将快照复制到哪个目标 Amazon 区域。对于自动快照，您也可以指定此类快照在目标 Amazon 区域中的保留期。自动快照复制到目标 Amazon 区域且达到保留期之后，便会从目标 Amazon 区域删除。这样做可以降低快照的使用率。若要让自动快照在目标 Amazon 区域中保留更短时间或更长时间，请更改此保留期。

您为复制到目标 Amazon 区域的自动快照设置的保留期与源 Amazon 区域中的自动快照的保留期无关。复制的快照的默认保留期为七天。该七天保留期仅适用于自动快照。在源和目标 Amazon 区域中，将在快照保留期结束时或手动删除时删除手动快照。

您可以随时禁用集群的自动快照复制功能。当您禁用此功能时，快照将不再从源 Amazon 区域复制到目标 Amazon 区域。复制到目标 Amazon 区域的所有自动快照都将在达到保留期时删除，除非您为其创建手动快照副本。此类手动快照以及从目标 Amazon 区域复制的所有手动快照在您将其手动删除之前将会一直保留在目标 Amazon 区域中。

若要更改用于接收复制快照的目标 Amazon 区域，请先禁用自动复制功能。然后重新启用它，并指定新的目标 Amazon 区域。

某个快照复制到目标 Amazon 区域之后，便处于活动和可用状态，可用于还原相关内容。

要将 Amazon KMS 加密的集群的快照复制到另一个 Amazon 区域，则必须为 Amazon Redshift 创建授权，以在目标 Amazon 区域中使用客户主密钥。然后在启用源 Amazon 区域中的快照复制功能时选择该权限授予。有关配置快照复制授权的更多信息，请参阅将 Amazon KMS 加密的快照复制到另一个 Amazon 区域 (p. 348)。

从快照还原集群

快照包含来自您的集群上运行的任何数据库的数据。它还包含有关集群的信息，包括节点数、节点类型和管理员用户名称。如果您从快照恢复集群，Amazon Redshift 会使用集群信息来创建新集群。然后它会从快照数据中恢复所有数据库。

对于从源快照创建的新集群，您可以选择配置，例如节点类型和节点数。如果您没有在请求中指定其他可用区，则该集群存储在相同的 Amazon 区域和可用区。当您从快照还原集群时，可为新集群选择兼容的维护跟踪。

Note

当您将快照恢复到具有不同配置的集群时，该快照必须在集群版本为 1.0.10013 或更高版本的集群上获取。

恢复正在进行时，事件通常按以下顺序发出：

1. RESTORE_STARTED – 当恢复过程开始时发送 REDSHIFT-EVENT-2008。
2. RESTORE_SUCCEEDED – 新集群已创建时发送 REDSHIFT-EVENT-3003。

   集群可用于查询。
3. DATA_TRANSFER_COMPLETED – 数据传输完成时发送 REDSHIFT-EVENT-3537。

Note

RA3 集群仅发出 RESTORE_STARTED 和 RESTORE_SUCCEEDED 事件。由于 RA3 节点类型将数据存储在 Amazon Redshift 托管存储中，因此在 RESTORE 成功后不会进行显式的数据传输。使用 RA3 节点，作为正常查询处理的一部分，数据在 RA3 节点和 Amazon Redshift 托管存储之间持续传输。RA3 节点在本地缓存热数据，并自动将查询频率较低的数据块保存在 Amazon Redshift 托管存储中。

您可以通过下列方式监控还原进度：调用 DescribeClusters API 操作或在 Amazon Web Services Management Console 中查看集群详细信息。对于正在进行的还原，通过上述方式可以看到快照数据的大小、传输速率、已用时间以及估计的剩余时间等信息。有关这些指标的说明，请参阅 RestoreStatus。

您无法使用快照将活动的集群还原为之前的状态。

Note

当您将快照还原为新集群时，如果您没有指定其他值，则使用默认的安全组和参数组。

出于以下原因，您可能想要将快照恢复到具有不同配置的集群：

- 集群由较小的节点类型组成，且您想要将它合并到具有较少节点的较大节点类型。
- 您监控工作负载并确定需要迁移到具有更多 CPU 和存储的节点类型。
- 您想要衡量具有不同节点类型的测试工作负载的性能。

还原具有以下限制：

- 新的节点配置必须为现有数据提供足够的存储空间。甚至在添加节点时，由于数据的重新分配方式，新配置可能没有足够的存储空间。
- 还原操作将检查快照是否在与新集群的集群版本兼容的集群版本上创建。如果新集群的版本级别太早，则恢复操作将失败，并在错误消息中报告更多信息。

- 可还原到的可能配置（节点数和节点类型）取决于原始集群中的节点数量和新集群的目标节点类型。要确定可能的配置，您可以使用 Amazon Redshift 控制台或 `describe-node-configuration-options` Amazon CLI 命令结合 `action-type restore-cluster`。有关使用 Amazon Redshift 控制台进行还原的更多信息，请参阅从快照还原集群 (p. 328)。

以下步骤使用 Amazon CLI 获取具有许多节点的集群，并将它合并到具有较少节点数的更大节点类型。在此示例中，我们从一个具有 24 个 `ds2.xlarge` 节点的源集群开始。在本例中，假设我们已经为此集群创建了一个快照，并且我们想要将它恢复到更大的节点类型。

1. 运行以下命令，获取 24 节点 `ds2.xlarge` 集群的详细信息。

```
aws redshift describe-clusters --region eu-west-1 --cluster-identifier
 mycluster-123456789012
```

2. 运行以下命令，获取快照的详细信息。

```
aws redshift describe-cluster-snapshots --region eu-west-1 --snapshot-identifier
 mycluster-snapshot
```

3. 运行以下命令，描述此快照可用的选项。

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

此命令会返回一个选项列表，包括每个选项的建议节点类型、节点数和磁盘利用率。在此示例中，上述命令列出以下可能的节点配置。我们选择恢复到三节点 `ds2.8xlarge` 集群。

```
{
    "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. 运行以下命令，将快照恢复到我们选择的集群配置。恢复此集群之后，我们拥有与源集群相同的内容，但数据已合并到三个 `ds2.8xlarge` 节点。

```
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
```

如果您有预留节点，例如 DS2 或 DC2 预留节点，则可以升级到 RA3 预留节点。您可以在从快照还原或执行弹性调整大小时执行此操作。您可以使用控制台引导您完成此过程。有关升级到 RA3 节点的更多信息，请参阅升级到 RA3 节点类型。

从快照中还原表

您可以从快照还原单个表而不是还原整个集群。在从快照还原单个表时，需要指定源快照、数据库、schema 和表名以及目标集群、schema 和已还原表的新表名。

新表名不能是现有表的名称。要将现有表替换为从快照还原的表，请先重命名或删除现有表，然后再从快照还原表。

使用源表的列定义、表属性和列属性（外键除外）创建目标表。为了防止因依赖项而导致发生冲突，目标表不从源表继承外键。不向目标表应用任何依赖项（例如，源表上的视图或授予的权限）。

如果源表的所有者存在，那么该用户是已还原的表的所有者，前提是该用户拥有足够的权限成为在指定数据库和 schema 中指定的关系的所有者。否则，已还原的表由在启动集群时创建的管理员用户所有。

已还原的表将返回在执行备份时其所处的状态。这包括由 Amazon Redshift 对可序列化隔离的符合性定义的事务可见性规则，这意味着数据将立即对在备份后启动的进行中事务可见。

从快照还原表受以下限制：

- 您只能将表还原到当前正在运行的活动集群，并且只能从针对该集群制作的快照还原表。
- 一次只能还原一个表。
- 无法从在调整集群大小之前拍摄的集群快照还原表。一个例外是，如果节点类型没有更改，则可以在弹性大小调整后还原表。
- 不向目标表应用任何依赖项（例如，源表上的视图或授予的权限）。
- 如果为正在还原的表启用行级安全性，Amazon Redshift 将还原已启用行级安全性的表。

从快照还原表

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后选择还原表要使用的集群。
3. 对于 Actions (操作)，请选择 Restore table (还原表) 以便显示 Restore table (还原表) 页面。
4. 输入要使用的快照、源表和目标表的相关信息，然后选择 Restore table (还原表)。

Example 示例：使用 Amazon CLI 从快照中还原表

以下示例使用 `restore-table-from-cluster-snapshot` Amazon CLI 命令从 `my-source-table` 上的 `sample-database` 架构中还原 `my-snapshot-id` 表。此示例将快照还原到具有新表名 `mycluster-example` 的 `my-new-table` 集群。

```
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
```

共享快照

您可以授权其他 Amazon 客户账户访问现有手动快照，以与其共享该快照。对于每个快照，最多可以授权 20 个客户账户；对于每个 Amazon Key Management Service (Amazon KMS) 密钥，则最多可以授权 100 个。例如，如果您有 10 个快照，它们使用了一个 KMS 密钥加密，那么您可以授权 10 个 Amazon 账户来还原每个快照，或者是其他组合：总共 100 账户以及每个快照不超过 20 个账户。然后，以用户身份登录其中一个已授权账户的人可以对快照加以说明，也可以还原快照以在其账户下创建一个新的 Amazon Redshift 集群。例如，如果您针对生产和测试使用不同的 Amazon 客户账户，则用户可以使用生产账户登录并与使用测试账户的用户共享快照。然后，以测试账户用户身份登录的人可以还原快照以创建一个新的集群，该集群由测试账户所有，用于测试或诊断工作。

手动快照由在其下创建该快照的 Amazon 客户账户永久所有。只有拥有相应快照的账户中的用户可以授权其他账户访问该快照或撤消授权。已授权账户中的用户只能对与其共享的任何快照加以说明或还原相应快照；他们无法复制或删除与其共享的快照。授权在快照所有者将其撤消之前保持有效。如果所有者撤消授权，则之前已获授权的用户将无法再看到相应快照，也无法再启动任何引用该快照的新操作。如果在所有者撤消授权时相应账户正在还原快照，则该还原操作会运行完成。您无法删除具有活跃授权的快照；必须先撤消所有授权。

Amazon 客户账户始终能够访问相应账户所有的快照。如果尝试授予或撤消对所有者账户的访问权限，则会收到一条错误消息。您无法还原由非活动 Amazon 客户账户所有的快照，也无法对其加以说明。

您获得访问 Amazon 客户账户的授权之后，那么该账户中便没有任何 IAM 用户可以针对相应快照执行任何操作，除非他们具有相应的 IAM 策略，允许他们这样做。

- 快照拥有者账户中的 IAM 用户只能在以下情况下授予和撤消快照访问权限：此类用户具有相应的 IAM 策略，允许他们通过包含该快照的资源规范执行此类操作。例如，以下策略允许 Amazon 账户 (`012345678912`) 中的用户授权其他账户访问名为 `my-snapshot20130829` 的快照：

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
          "redshift:AuthorizeSnapshotAccess",
          "redshift:RevokeSnapshotAccess"
          ],
      "Resource":[
           "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-snapshot20130829"
          ]
    }
  ]
}
```

- 与其共享快照的 Amazon 账户中的 IAM 用户无法针对该快照执行操作，除非他们具有相应的 IAM 策略，允许他们执行这些操作：
  - 要列出快照或对其加以说明，相应用户必须具有相应的 IAM 策略，允许他们执行 `DescribeClusterSnapshots` 操作。下方代码显示了一个示例：

```
{
```

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

- 要还原快照，用户必须具有相应的 IAM 策略，允许他们执行 `RestoreFromClusterSnapshot` 操作，且该策略要有一个资源元素，同时涵盖他们尝试创建的集群以及相应快照。例如，如果账户 (012345678912) 中的用户与账户 (my-snapshot20130829) 共享了快照 (219876543210)，则要通过还原快照来创建集群，账户 (219876543210) 中的用户必须具有诸如以下的策略：

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

- 在撤销 Amazon 账户对快照的访问权限后，该账户中的所有用户均无法访问该快照。即使这些用户具有允许对以前共享的快照资源执行操作的 IAM 策略，也是如此。

使用控制台管理快照

Amazon Redshift 会定期自动对您的数据拍摄递增快照，并将其保存到 Simple Storage Service（Amazon S3）中。此外，您可以随时对数据制作手动快照。在本节中，您可以了解如何从 Amazon Redshift 控制台管理快照。有关 快照的更多信息，请参阅 Amazon Redshift 快照 (p. 318)。

Amazon Redshift 控制台中的所有快照任务都从快照列表开始。您可以使用时间范围、快照类型以及与快照关联的集群来筛选该列表。此外，您可以按日期、大小和快照类型对列表进行排序。根据您选择的快照类型，您处理快照的选项可能有所不同。

主题

- 创建快照计划 (p. 327)
- 创建手动快照 (p. 327)
- 更改手动快照保留期 (p. 327)
- 删除手动快照 (p. 327)
- 复制自动快照 (p. 328)
- 从快照还原集群 (p. 328)
- 从快照还原无服务器命名空间 (p. 328)
- 共享集群快照 (p. 329)

- 为未加密的集群配置跨区域快照复制 (p. 330)
- 为 Amazon KMS 加密的集群配置跨区域快照复制 (p. 330)
- 修改跨区域快照复制的保留期 (p. 331)

创建快照计划

要精确控制拍摄快照的时间，您可以创建快照计划并将其附加到一个或多个集群。您可以在创建集群时或通过修改集群来附加计划。有关更多信息，请参阅自动快照计划 (p. 319)。

要创建快照计划

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）、Snapshots（快照），然后选择 Snapshot schedules（快照计划）选项卡。此时将显示快照计划。
3. 选择 Add schedule（添加计划）以显示添加计划的页面。
4. 输入计划定义的属性，然后选择 Add schedule（添加计划）。
5. 在显示的页面上，您可以将集群附加到新的快照计划，然后选择 OK（确定）。

创建手动快照

您可以从如下所示的快照列表中创建集群的手动快照。您也可以在集群配置窗格中制作集群快照。有关更多信息，请参阅创建集群快照 (p. 88)。

创建手动快照

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）、Snapshots（快照），然后选择 Create snapshot（创建快照）。此时将显示用于创建手动快照的快照页面。
3. 输入快照定义的属性，然后选择 Create snapshot（创建快照）。快照可能需要一段时间才可用。

更改手动快照保留期

您可以通过修改快照设置来更改手动快照的保留期。

更改手动快照保留期

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）、Snapshots（快照），然后选择要更改的手动快照。
3. 对于 Actions（操作），选择 Manual snapshot settings（手动快照设置）以显示手动快照的属性。
4. 输入快照定义的修订属性，然后选择 Save（保存）。

删除手动快照

您可以通过在快照列表中选择一个或多个快照来删除手动快照。

删除手动快照

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）、Snapshots（快照），然后选择要删除的快照。
3. 对于 Actions（操作），选择 Delete snapshot（删除快照）以删除快照。
4. 确认删除列出的快照，然后选择 Delete（删除）。

复制自动快照

自动快照会在其保留期到期、您禁用自动快照或者您删除集群时自动删除。如果要保留自动快照，可将其复制到手动快照。

复制自动快照

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）、Snapshots（快照），然后选择要复制的快照。
3. 对于 Actions（操作），选择 Copy automated snapshot（复制自动快照）以复制快照。
4. 更新新快照的属性，然后选择 Copy（复制）。

从快照还原集群

当您从快照还原集群时，Amazon Redshift 会创建一个包含所有快照数据的新集群。

从快照还原集群

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）、Snapshots（快照），然后选择要还原的快照。
3. 选择 Restore from snapshot（从快照还原）以查看使用快照信息创建的新集群的 Cluster configuration（集群配置）和 Cluster details（集群详细信息）值。
4. 更新新集群的属性，然后选择 Restore cluster from snapshot（从快照中还原集群）。

如果您有预留节点，例如 DS2 或 DC2 预留节点，则可以升级到 RA3 预留节点。您可以在从快照还原或执行弹性调整大小时执行此操作。您可以使用控制台引导您完成此过程。有关升级到 RA3 节点的更多信息，请参阅升级到 RA3 节点类型。

从快照还原无服务器命名空间

从快照还原无服务器命名空间会将命名空间的所有数据库替换为快照中的数据库。有关无服务器快照的更多信息，请参阅使用快照和恢复点。

将快照从您的预置集群还原到 Amazon Redshift Serverless 实例。

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）、Snapshots（快照），然后选择要使用的快照。
3. 选择 Restore from snapshot（从快照还原）、Restore to serverless namespace（还原到无服务器命名空间）。
4. 选择您要还原到的命名空间。

5. 确认想要从快照还原。选择 Restore（还原）。此操作会将您的 Amazon Redshift Serverless 实例中的所有数据库替换为来自您的预置集群的数据。

共享集群快照

您可以授权其他用户访问自己的手动快照，随后在不再需要时撤消该访问权限。

要与另一个账户共享快照

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择Clusters（集群）、Snapshots（快照），然后选择要共享的手动快照。
3. 对于 Actions（操作），选择 Manual snapshot settings（手动快照设置）以显示手动快照的属性。
4. 在 Manage access（管理访问权限）部分中输入要与之共享的一个或多个账户，然后选择 Save（保存）。

共享加密快照的安全注意事项

当您提供对加密快照的访问权限时，Redshift 要求用于创建快照的 Amazon KMS 客户托管式密钥与执行恢复的一个或多个账户共享。如果密钥未共享，尝试恢复快照将导致拒绝访问错误。当您授予快照访问权限并共享密钥时，授予访问权限的身份必须对用于加密快照的密钥具有 `kms:DescribeKey` 权限。有关此权限的更多详细信息，请参阅 Amazon KMS 权限。有关更多信息，请参阅 Amazon Redshift API 参考文档中的 DescribeKey。

客户托管式密钥策略可以通过编程方式或在控制台上使用 Amazon Key Management Service 更新。

允许访问加密快照的 Amazon KMS 密钥

共享加密快照的 Amazon KMS 客户托管式密钥，请执行以下步骤更新密钥策略：

1. 使用 KMS 密钥策略中作为 `Principal` 共享的 Amazon 账户的 Amazon Resource Name（ARN）更新 KMS 密钥策略。
2. 允许 `kms:Decrypt` 操作。

在下面的密钥策略示例中，用户 `111122223333` 是 KMS 密钥的所有者，而用户 `444455556666` 是与之共享密钥的账户。通过包含用户 `444455556666` 的根 Amazon 账户身份的 ARN 作为策略的 `Principal`，以及通过允许 `kms:Decrypt` 操作，此密钥策略为 Amazon 账户提供了访问 KMS 密钥的权限。

```
{
    "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": "*"
```

```
        }
    ]
}
```

授予客户托管式 KMS 密钥访问权限后，恢复加密快照的账户必须创建 Amazon Identity and Access Management（IAM）角色或用户（如果用户尚未拥有该角色）。此外，该 Amazon 账户还必须将 IAM policy 附加到该 IAM 角色或用户，以允许他们使用您的 KMS 密钥恢复加密的数据库集群快照。

要详细了解如何提供对 Amazon KMS 密钥的访问权限，请参阅《Amazon Key Management Service 开发人员指南》中的允许其他账户中的用户使用 KMS 密钥。

有关密钥策略的概览，请参阅 Amazon Redshift 如何使用 Amazon KMS。

为未加密的集群配置跨区域快照复制

您可以配置 Amazon Redshift，以将集群的快照复制到其他 Amazon 区域。要配置跨区域快照复制，您需要为每个集群启用该复制功能，并配置复制快照的位置以及在目标 Amazon 区域中保留复制的自动或手动快照的时间。如果为集群启用了跨区域复制，所有新的手动和自动快照将复制到指定的 Amazon 区域。复制的快照名称带有前缀：**`copy:`**。

配置跨区域快照

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后选择要移动其快照的集群。
3. 对于 Actions（操作），选择 Configure cross-region snapshot（配置跨区域快照）。

   此时将显示 Configure cross-Region（配置跨区域）对话框。
4. 对于 Copy snapshots（复制快照），选择 Yes（是）。
5. 在 Destination Amazon Region（目标 Amazon 区域）中，选择要将快照复制到的 Amazon 区域。
6. 在 Automated snapshot retention period (days)（自动快照保留期 (天数)）中，选择您希望自动快照被删除之前在目标 Amazon 区域中保留的天数。
7. 在 Manual snapshot retention period（手动快照保留期）中，选择您希望手动快照被删除之前在目标 Amazon 区域中保留的天数。如果选择 Custom value（自定义值），则保留期必须在 1 到 3653 天之间。
8. 选择保存。

为 Amazon KMS 加密的集群配置跨区域快照复制

启动 Amazon Redshift 集群时，您可以选择使用 Amazon Key Management Service（Amazon KMS）中的根密钥对其进行加密。Amazon KMS 密钥特定于 Amazon 区域。如果您想为 Amazon KMS 加密的集群启用跨区域快照复制，则必须在目标 Amazon 区域中为根密钥配置快照复制授权。通过执行此操作，您可以使 Amazon Redshift 在目标 Amazon 区域执行加密操作。

以下过程说明了为 Amazon KMS 加密的集群启用跨区域快照复制的过程。要详细了解 Amazon Redshift 中的加密功能以及快照复制授予，请参阅将 Amazon KMS 加密的快照复制到另一个 Amazon 区域 (p. 348)。

要为 Amazon KMS 加密的集群配置跨区域快照

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后选择要移动其快照的集群。
3. 对于 Actions（操作），选择 Configure cross-region snapshot（配置跨区域快照）。

此时将显示 Configure cross-Region（配置跨区域）对话框。

4. 对于 Copy snapshots（复制快照），选择 Yes（是）。
5. 在 Destination Amazon Region（目标 Amazon 区域）中，选择要将快照复制到的 Amazon 区域。
6. 在 Automated snapshot retention period (days)（自动快照保留期 (天数)）中，选择您希望自动快照被删除之前在目标 Amazon 区域中保留的天数。
7. 在 Manual snapshot retention period（手动快照保留期）中，选择您希望手动快照被删除之前在目标 Amazon 区域中保留的天数。如果选择 Custom value（自定义值），则保留期必须在 1 到 3653 天之间。
8. 选择保存。

修改跨区域快照复制的保留期

在配置跨区域快照复制后，您可能希望更改这些设置。您可以选择新的天数并保存更改，从而轻松更改保留期。

Warning

在配置跨区域快照复制后，您无法修改目标 Amazon 区域。
如果要将快照复制到其他 Amazon 区域，请先禁用跨区域快照复制。然后使用新的目标 Amazon 区域和保留期重新启用它。在禁用跨区域快照复制后，将删除任何复制的自动快照。因此，在禁用跨区域快照复制之前，您应该确定是否具有任何要保留的快照，并将其复制到手动快照。

修改跨区域快照

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后选择要修改其快照的集群。
3. 对于 Actions (操作)，请选择 Configure cross-region snapshot (配置跨区域快照) 以显示快照的属性。
4. 输入快照定义的修订属性，然后选择 Save（保存）。

使用 Amazon SDK for Java 管理快照

下面的示例显示了涉及快照的常见操作：

- 创建集群的手动快照。
- 显示与集群的所有快照有关的信息。
- 删除集群的手动快照。

在此示例中，系统启动了集群的快照。成功创建快照后，系统将删除在此新快照之前为该集群创建的所有手动快照。在启动创建手动快照的过程时，该快照不会立即可供使用。因此，此示例通过调用 `describeClusterSnapshot` 方法，使用循环来轮询快照的状态。通常，快照在启动片刻之后才可供使用。有关 快照的更多信息，请参阅 Amazon Redshift 快照 (p. 318)。

有关运行以下示例的分步说明，请参阅 使用 Eclipse 运行 Amazon Redshift 的 Java 示例 (p. 464)。您需要更新该代码并提供集群标识符。

Example

```
/**
```

```
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
*/

// snippet-sourcedescription:[CreateAndDescribeSnapshot demonstrates how to create an
 Amazon Redshift cluster snapshot and describe existing snapshots.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[CreateClusterSnapshot]
// snippet-keyword:[DeleteClusterSnapshot]
// snippet-keyword:[DescribeClusterSnapshots]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-01-30]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.CreateAndDescribeSnapshot.complete]

package com.amazonaws.services.redshift;

import java.io.IOException;
import java.text.SimpleDateFormat;
import java.util.Date;

import com.amazonaws.services.redshift.model.*;

public class CreateAndDescribeSnapshot {

    public static AmazonRedshift client;
    public static String clusterIdentifier = "***provide a cluster identifier***";
    public static long sleepTime = 20;

    public static void main(String[] args) throws IOException {

         // Default client using the {@link
 com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
        client = AmazonRedshiftClientBuilder.defaultClient();

        try {
             // Unique snapshot identifier
             String snapshotId = "my-snapshot-" + (new SimpleDateFormat("yyyy-MM-dd-HH-mm-
ss")).format(new Date());

             Date createDate = createManualSnapshot(snapshotId);
             waitForSnapshotAvailable(snapshotId);
             describeSnapshots();
             deleteManualSnapshotsBefore(createDate);
             describeSnapshots();

        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }

    private static Date createManualSnapshot(String snapshotId) {

        CreateClusterSnapshotRequest request = new CreateClusterSnapshotRequest()
```

```
        .withClusterIdentifier(clusterIdentifier)
        .withSnapshotIdentifier(snapshotId);
        Snapshot snapshot = client.createClusterSnapshot(request);
        System.out.format("Created cluster snapshot: %s\n", snapshotId);
        return snapshot.getSnapshotCreateTime();
    }

    private static void describeSnapshots() {

        DescribeClusterSnapshotsRequest request = new DescribeClusterSnapshotsRequest()
            .withClusterIdentifier(clusterIdentifier);
        DescribeClusterSnapshotsResult result = client.describeClusterSnapshots(request);

        printResultSnapshots(result);
    }

    private static void deleteManualSnapshotsBefore(Date creationDate) {

        DescribeClusterSnapshotsRequest request = new DescribeClusterSnapshotsRequest()
            .withEndTime(creationDate)
            .withClusterIdentifier(clusterIdentifier)
            .withSnapshotType("manual");

        DescribeClusterSnapshotsResult result = client.describeClusterSnapshots(request);

        for (Snapshot s : result.getSnapshots()) {
            DeleteClusterSnapshotRequest deleteRequest = new DeleteClusterSnapshotRequest()
            .withSnapshotIdentifier(s.getSnapshotIdentifier());
            Snapshot deleteResult = client.deleteClusterSnapshot(deleteRequest);
            System.out.format("Deleted snapshot %s\n",
deleteResult.getSnapshotIdentifier());
        }
    }

    private static void printResultSnapshots(DescribeClusterSnapshotsResult result) {
        System.out.println("\nSnapshot listing:");
        for (Snapshot snapshot : result.getSnapshots()) {
            System.out.format("Identifier: %s\n", snapshot.getSnapshotIdentifier());
            System.out.format("Snapshot type: %s\n", snapshot.getSnapshotType());
            System.out.format("Snapshot create time: %s\n",
snapshot.getSnapshotCreateTime());
            System.out.format("Snapshot status: %s\n\n", snapshot.getStatus());
        }
    }

    private static Boolean waitForSnapshotAvailable(String snapshotId) throws
InterruptedException {
        Boolean snapshotAvailable = false;
        System.out.println("Wating for snapshot to become available.");
        while (!snapshotAvailable) {
            DescribeClusterSnapshotsResult result = client.describeClusterSnapshots(new
DescribeClusterSnapshotsRequest()
                .withSnapshotIdentifier(snapshotId));
            String status = (result.getSnapshots()).get(0).getStatus();
            if (status.equalsIgnoreCase("available")) {
                snapshotAvailable = true;
            }
            else {
                System.out.print(".");
                Thread.sleep(sleepTime*1000);
            }
        }
        return snapshotAvailable;
    }

}
```

```
// snippet-end:[redshift.java.CreateAndDescribeSnapshot.complete]
```

使用 Amazon CLI 和 Amazon Redshift API 管理快照

您可以通过以下 Amazon Redshift CLI 操作来管理快照。

- 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

您可以通过以下 Amazon Redshift API 操作来管理快照。

- AuthorizeSnapshotAccess
- CopyClusterSnapshot
- CreateClusterSnapshot
- DeleteClusterSnapshot
- DescribeClusterSnapshots
- DisableSnapshotCopy
- EnableSnapshotCopy
- ModifySnapshotCopyRetentionPeriod
- RestoreFromClusterSnapshot
- RevokeSnapshotAccess

有关 Amazon Redshift 快照的更多信息，请参阅Amazon Redshift 快照 (p. 318)。

将 Amazon Redshift 与 Amazon 合作伙伴集成

通过使用 Amazon Redshift，您可以从 Amazon Redshift 控制台上的 Cluster details（集群详细信息）页面与 Amazon 合作伙伴集成。从 Cluster details（集群详细信息）页面上，您可以使用 Amazon 合作伙伴应用程序加速数据到 Amazon Redshift 数据仓库的载入。您还可以联接和分析来自不同来源的数据以及集群中的现有数据。以下 Amazon 合作伙伴可以与 Amazon Redshift 集成：

- Datacoral
- Etleap
- Fivetran
- Informatica
- SnapLogic
- Stitch
- Upsolver
- Matillion（预览版）
- Sisense（预览版）

Amazon 合作伙伴可以使用 Amazon CLI 或 Amazon Redshift API 操作与 Amazon Redshift 集成。有关更多信息，请参阅 Amazon Redshift API 参考上的 Amazon CLI 命令参考。

使用 Amazon Redshift 控制台与 Amazon 合作伙伴集成

使用以下过程将集群与 Amazon 合作伙伴集成。

要将 Amazon Redshift 集群与 Amazon 合作伙伴集成

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。
3. 选择要集成的集群。
4. 选择 Add partner integration（添加合作伙伴集成）。Choose partner（选择合作伙伴）页面将打开，其中包含有关可用 Amazon 合作伙伴的详细信息。
5. 选择一位 Amazon 合作伙伴，然后选择 Next（下一步）。

   有关选择的 Amazon 合作伙伴的更多详细信息出现，还包括您正在集成的集群的详细信息。Cluster details（集群详细信息）部分包含您在 Amazon 合作伙伴网站上提供的信息，例如集群标识符、端点、数据库名称, 和用户名（这是一个数据库用户名）。此信息将发送到您选择的合作伙伴。
6. 选择 Add partner（添加合作伙伴）以打开 Amazon 合作伙伴的网站。
7. 在合作伙伴的网站上配置与您的 Amazon Redshift 集群的集成。在合作伙伴的网站上，您可以选择并配置加载到 Amazon Redshift 集群的数据源。您还可以定义其他数据提取、加载和转换 (ELT) 转换，以处理业务数据、将其与其他数据集联接并构建用于分析和报告的合并视图。

您可以查看和管理集群详细信息 Properties（属性）选项卡中的 Amazon 合作伙伴集成。Integrations（集成）部分列出合作伙伴名称（您可以使用该名称链接到 Amazon 合作伙伴网站）、集成的状态、接收数据的数据库，以及可能已更新集群的上一次成功连接。

可能的状态值如下所示：

- Active（活动）– Amazon 合作伙伴可以连接到集群并完成配置的任务。
- Inactive（非活动）– Amazon 合作伙伴集成不存在。
- Runtime failure（运行时失败）– Amazon 合作伙伴可以连接到集群并无法完成配置的任务。
- Connection failure（连接失败）– Amazon 合作伙伴无法连接到集群。

删除来自 Amazon Redshift 的 Amazon 合作伙伴集成，数据会继续流入您的集群。在合作伙伴网站上完成删除操作。

购买 Amazon Redshift 预留节点

概览

在 Amazon 中，您使用 Amazon Redshift 产生的费用取决于计算节点。每个计算节点均按每小时费率计费。每小时费率因诸多因素而言，如区域、节点类型以及相应节点使用的是按需节点定价还是预留节点定价。

按需节点定价费用最高，但在 Amazon Redshift 中灵活性最高。使用按需费率，您只需为正在运行的集群中的计算节点付费。如果您关闭或删除某个集群，则无需再为该集群中的计算节点付费。您只需为所使用的计算节点付费，无需支付任何其他费用。您为每个计算节点支付的每小时费率因区域和节点类型等因素而异。

预留节点定价比按需定价的费用低一些，因为计算节点以打折后的每小时费率计费。不过，要享受此类打折费率，您必须购买预留节点产品。购买产品即进行预留。这种预留为您针对预留持续时间预留的每个节点设置一个打折费率。产品的打折费率因区域、节点类型、持续时间以及付款选项等因素而异。

您可以通过调用 `PurchaseReservedNodeOffering` API 操作或在 Amazon Redshift 控制台上选择 Purchase reserved nodes (购买预留节点)，将节点指定为预留节点。购买预留节点时，您必须为适用的预留节点类型指定 Amazon 区域、节点类型、期限、节点数量和产品类型。预留节点只能用于指定的 Amazon 区域。

本主题讨论了有哪些预留节点产品，以及如何购买此类产品才能减少运行 Amazon Redshift 集群的费用。本主题粗略介绍了按需费率和打折费率，以便您可以了解一些定价概念以及定价如何影响计费。有关具体费率的更多信息，请转到 Amazon Redshift 定价。

关于预留节点产品

如果您打算让 Amazon Redshift 集群持续运行很长一段时间，则不妨考虑购买预留节点产品。与按需定价相比，购买这些产品可以节省大量费用，但您必须预留计算节点并承诺在一年或三年的期限里为所使用的节点支付相应费用。

预留节点是一个计费概念，完全用于确定您为节点付费所使用的费率。实际上，预留节点并不会为您创建任何节点。无论如何使用，您都需要为预留节点付费，也就是说，您必须为预留持续时间预留的每个节点付费，无论正在运行的集群中是否有任何节点可以使用打折费率。

在项目评估阶段或运行概念验证时，您可以通过按需定价灵活地按需付费，仅为使用的服务付费，并随时关闭或删除集群以停止付费。满足了生产环境的需求并进入实施阶段后，不妨考虑购买一个或多个产品来预留计算节点。

一个产品适用于一个或多个计算节点。当您购买产品时，需指定要预留的计算节点的数量。您可以选择为多个计算节点购买一个产品，也可以选择购买多个产品并在每个产品中指定一定数量的计算节点。

例如，您可以采用以下有效方法为三个计算节点购买产品：

- 购买一个产品并指定三个计算节点。
- 购买两个产品，为第一个产品指定一个计算节点，为第二个产品指定两个计算节点。
- 购买三个产品并为这三个产品各指定一个计算节点。

比较不同预留节点产品的定价

Amazon Redshift 提供多种产品付款选项。您选择的付款选项会影响您针对相应预留付费的付款计划和打折费率。您为预留预先支付的费用越多，总体节省的费用就越多。

针对产品付费可使用下列付款选项。这些产品以与按需费率相比，节省的费用从低到高列出。

Note

无论您是否使用预留节点，都需要为指定预留持续时间里的每个小时支付相应的每小时费率。付款选项仅确定付款频率以及应用的折扣。有关更多信息，请参阅 关于预留节点产品 (p. 337)。

比较预留节点产品

付款选项	付款计划	相对节省的费用	Duration	预付费用	定期支付的月度费用
无费用预付	在预留持续时间里按月分期付款。不预付任何费用。	与按需费率相比，节省 20%。	一年期。	无	是
预付部分费用	预付部分费用，然后在预留持续时间里按月分期付款。	根据持续时间，节省 41% 到 73%。	一年期或三年期	是	是
预付全部费用	针对预留预付全费。无月度费用。	根据持续时间，节省 42% 到 76%。	一年期或三年期	是	无

Note

如果您之前购买的是 Amazon Redshift 的高利用率产品，则可比较的产品是预付部分费用产品。

预留节点的工作方式

使用预留节点产品，您需要根据上一部分所述的付款方式付费。无论您已有正在运行的集群，还是在进行预留后启动集群，都需要按这种方式付费。

当您购买产品时，您的预留将处于 payment-pending 状态，直到预留得到处理。如果预留未得到处理，则该状态将显示为 payment-failed，直到您再次尝试进行此流程。预留成功得到处理后，该状态将变为 active。在该状态变为 active 之前，您的预留适用的打折费率将不会应用于您的账单。预留持续时间过后，该状态将变为 retired，但您可以继续出于历史目的访问预留的相关信息。当预留处于 retired 状态时，您的集群将继续运行，但您可能要以按需费率付费，除非您进行另一次预留，针对节点应用打折定价。

预留节点专用于您在其中购买产品的区域。如果您使用 Amazon Redshift 控制台来购买产品，请选择您要在其中购买产品的 Amazon 区域，然后完成预留流程。如果您以编程方式购买产品，则区域由您连接到的 Amazon Redshift 端点确定。有关 Amazon Redshift 区域的更多信息，请参阅 Amazon Web Services 一般参考中的区域和端点。

为确保相应的打折费率在您启动集群时应用于所有节点，请确保区域、节点类型以及您选择的节点数量与一个或多个有效预留匹配。否则，对于与有效预留不匹配的节点，将以按需费率对您进行收费。

在正在运行的集群中，如果您超出预留的节点数量，则您将以按需费率为超出预留数量的节点付费。这种费用意味着，您可能以不同的费率为同一个集群中的节点付费，具体取决于您预留的节点数量。您可以再购买一个产品来涵盖超出预留数量的这部分节点，然后在预留状态变为 active 之后，相应的打折费率将在剩余持续时间里应用于这部分节点。

如果您调整集群的大小以采用其他节点类型，并且您没有预留此类型的节点，则您将以按需费率付费。如果您希望大小经过调整后的集群享受到打折费率，则可以采用新的节点类型再购买一个产品。不过，您还将继续为原始预留付费，直到其持续时间过去。如果您需要在期限到期前更改预留，请使用 Amazon 控制台创建支持案例。

预留节点和整合账单

当购买账户属于在一个整合账单付款人账户之下开具账单的一套账户的一部分时，预留节点的定价优惠可以共享。将所有子账户的小时使用量每月聚合到付款人账户。这通常对具有不同职能团队或团体的公司很有

用；然后，将应用正常的预留节点逻辑来计算账单。有关更多信息，请参阅 Amazon Billing 用户指南中的整合账单。

预留节点示例

本部分中的情景演示了节点如何根据按需费率和打折费率（后者的预留详细信息如下所示）产生费用：

- 区域：美国西部（俄勒冈）
- 节点类型：ds2.xlarge
- 付款选项：No Upfront
- 持续时间：一年
- 预留节点的数量：16

示例 1

您在美国西部（俄勒冈）区域有一个 ds2.xlarge 集群，其中有 20 个节点。

在此情景中，其中 16 个节点享受预留打折费率，但集群中的另外 4 个节点以按需费率计费。

示例 2

您在美国西部（俄勒冈）区域有一个 ds2.xlarge 集群，其中有 12 个节点。

在此情景中，集群中的全部 12 个节点都享受预留打折费率。不过，您还需要为预留中的剩余预留节点付费，即使您当前并没有正在运行的集群可供这些预留节点应用于其中。

示例 3

您在美国西部（俄勒冈）区域有一个 ds2.xlarge 集群，其中有 12 个节点。您采用此配置运行该集群几个月时间，然后您需要向其中添加节点。您调整了集群的大小，选择相同的节点类型并指定共计 16 个节点。

在此情景中，您将以打折费率为这 16 个节点付费。在整年的持续时间里您的费用保持不变，因为集群中的节点数量与您预留的节点数量相同。

示例 4

您在美国西部（俄勒冈）区域有一个 ds2.xlarge 集群，其中有 16 个节点。您采用此配置运行该集群几个月时间，然后您需要添加节点。您调整了集群的大小，选择相同的节点类型并指定共计 20 个节点。

在此情景中，您将以打折费率为调整大小之前的所有节点付费。调整大小之后，您将在一年中剩下的时间以打折费率为 16 个节点付费，并以按需费率为添加到集群中的另外 4 个节点付费。

示例 5

您在美国西部（俄勒冈）区域有两个 ds2.xlarge 集群。一个集群中有 6 个节点，另一个集群中有 10 个节点。

在此情景中，您将以打折费率为所有节点付费，因为两个集群中的节点总数与您预留的节点数量相同。

示例 6

您在美国西部（俄勒冈）区域有两个 ds2.xlarge 集群。一个集群中有 4 个节点，另一个集群中有 6 个节点。

在此情景中，您将以打折费率为正在运行的集群中的 10 个节点付费；此外，您还需以打折费率为预留的额外 6 个节点，即使您当前并没有任何正在运行的集群可供这些预留节点应用于其中。

使用 Amazon Redshift 控制台购买预留节点产品

您可以使用 Amazon Redshift 控制台中的 Reserved Nodes（预留节点）页面，以购买预留节点产品，并查看当前和过去的预留。

在您购买产品之后，Reserved Node 列表将显示您的预留和每个预留的详细信息，例如节点类型、节点数量和预留的状态。有关预留的更多信息，如需了解更多信息，请参阅预留节点的工作方式 (p. 338)。

要购买预留节点

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后选择 Reserved nodes（预留节点）以显示预留节点列表。
3. 选择 Purchase reserved nodes（购买预留节点）显示页面，以选择要购买的节点的属性。
4. 输入节点的属性，然后选择 Purchase reserved nodes（购买预留节点）。

要升级预留节点，请使用 Amazon CLI。

使用 Amazon CLI 升级预留节点

要利用 Amazon CLI 升级预留节点预留

1. 获取 ReservedNodeOfferingID 的列表以找到可满足您对支付类型、期限和费用的要求的产品。以下示例说明了该步骤。

```
aws redshift get-reserved-node-exchange-offerings --reserved-node-id xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxx
{
    "ReservedNodeOfferings": [
        {
            "Duration": 31536000,
            "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
            "UsagePrice": 0.0,
            "NodeType": "dc2.large",
            "RecurringCharges": [
                {
                    "RecurringChargeFrequency": "Hourly",
                    "RecurringChargeAmount": 0.2
                }
            ],
            "CurrencyCode": "USD",
            "OfferingType": "No Upfront",
            "ReservedNodeOfferingType": "Regular",
            "FixedPrice": 0.0
        }
    ]
}
```

2. 调用 `accept-reserved-node-exchange` 并为要与在上一步中获取的 ReservedNodeOfferingID 一起交换的 DC1 预留节点提供 ID。

   以下示例说明了该步骤。

```
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
    }
}
```

您可以通过调用 describe-reserved-nodes 并检查 `Node type` 的值来确认该交换是否完成。

使用 Amazon SDK for Java 购买预留节点产品

以下示例演示如何使用 Amazon SDK for Java 执行以下操作：

- 列出现有的预留节点。
- 根据指定的节点标准搜索新的预留节点产品。
- 购买预留节点。

此示例首先选择与特定的节点类型和固定价格值相匹配的所有预留节点产品。然后，此示例遍历找到的每个产品，并允许您购买产品。

> **Important**
>
> 如果您运行此示例并接受购买预留节点产品的提议，您将被收取与该产品相关的费用。

有关运行此示例的分步说明，请参阅使用 Eclipse 运行 Amazon Redshift 的 Java 示例 (p. 464)。要获得这里未列出的其他节点类型和固定价格的信息，请更新代码并提供相应的节点类型和固定价格。

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
*/
```

```
// snippet-sourcedescription:[ListAndPurchaseReservedNodeOffering demonstrates how to list
 and purchase Amazon Redshift reserved node offerings.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[DescribeReservedNodeOfferings]
// snippet-keyword:[PurchaseReservedNodeOffering]
// snippet-keyword:[ReservedNode]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-01-31]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.ListAndPurchaseReservedNodeOffering.complete]

package com.amazonaws.services.redshift;

import java.io.DataInput;
import java.io.DataInputStream;
import java.io.IOException;
import java.util.ArrayList;

import com.amazonaws.services.redshift.model.*;

public class ListAndPurchaseReservedNodeOffering {

    public static AmazonRedshift client;
    public static String nodeTypeToPurchase = "dc2.large";
    public static Double fixedPriceLimit = 10000.00;
    public static ArrayList<ReservedNodeOffering> matchingNodes = new
 ArrayList<ReservedNodeOffering>();

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
 com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
       client = AmazonRedshiftClientBuilder.defaultClient();

        try {
             listReservedNodes();
             findReservedNodeOffer();
             purchaseReservedNodeOffer();

        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }

    private static void listReservedNodes() {
        DescribeReservedNodesResult result = client.describeReservedNodes();
        System.out.println("Listing nodes already purchased.");
        for (ReservedNode node : result.getReservedNodes()) {
            printReservedNodeDetails(node);
        }
    }

    private static void findReservedNodeOffer()
    {
        DescribeReservedNodeOfferingsRequest request = new
 DescribeReservedNodeOfferingsRequest();
        DescribeReservedNodeOfferingsResult result =
 client.describeReservedNodeOfferings(request);
        Integer count = 0;

        System.out.println("\nFinding nodes to purchase.");
        for (ReservedNodeOffering offering : result.getReservedNodeOfferings())
```

```
        {
            if (offering.getNodeType().equals(nodeTypeToPurchase)){

                if (offering.getFixedPrice() < fixedPriceLimit) {
                    matchingNodes.add(offering);
                    printOfferingDetails(offering);
                    count +=1;
                }
            }
        }
        if (count == 0) {
            System.out.println("\nNo reserved node offering matches found.");
        } else {
            System.out.println("\nFound " + count + " matches.");
        }
    }

    private static void purchaseReservedNodeOffer() throws IOException {
        if (matchingNodes.size() == 0) {
            return;
        } else {
            System.out.println("\nPurchasing nodes.");

            for (ReservedNodeOffering offering : matchingNodes) {
                printOfferingDetails(offering);
                System.out.println("WARNING: purchasing this offering will incur costs.");
                System.out.println("Purchase this offering [Y or N]?");
                DataInput in = new DataInputStream(System.in);
                String purchaseOpt = in.readLine();
                if (purchaseOpt.equalsIgnoreCase("y")){

                    try {
                        PurchaseReservedNodeOfferingRequest request = new
PurchaseReservedNodeOfferingRequest()

.withReservedNodeOfferingId(offering.getReservedNodeOfferingId());
                        ReservedNode reservedNode =
client.purchaseReservedNodeOffering(request);
                        printReservedNodeDetails(reservedNode);
                    }
                    catch (ReservedNodeAlreadyExistsException ex1){
                    }
                    catch (ReservedNodeOfferingNotFoundException ex2){
                    }
                    catch (ReservedNodeQuotaExceededException ex3){
                    }
                    catch (Exception ex4){
                    }
                }
            }
            System.out.println("Finished.");

        }
    }

    private static void printOfferingDetails(
            ReservedNodeOffering offering) {
        System.out.println("\nOffering Match:");
        System.out.format("Id: %s\n", offering.getReservedNodeOfferingId());
        System.out.format("Node Type: %s\n", offering.getNodeType());
        System.out.format("Fixed Price: %s\n", offering.getFixedPrice());
        System.out.format("Offering Type: %s\n", offering.getOfferingType());
        System.out.format("Duration: %s\n", offering.getDuration());
    }

    private static void printReservedNodeDetails(ReservedNode node) {
```

```
        System.out.println("\nPurchased Node Details:");
        System.out.format("Id: %s\n", node.getReservedNodeOfferingId());
        System.out.format("State: %s\n", node.getState());
        System.out.format("Node Type: %s\n", node.getNodeType());
        System.out.format("Start Time: %s\n", node.getStartTime());
        System.out.format("Fixed Price: %s\n", node.getFixedPrice());
        System.out.format("Offering Type: %s\n", node.getOfferingType());
        System.out.format("Duration: %s\n", node.getDuration());
    }
}
// snippet-end:[redshift.java.ListAndPurchaseReservedNodeOffering.complete]
```

使用 Amazon CLI 和 Amazon Redshift API 购买预留节点产品

您可以通过以下 Amazon CLI 操作来购买预留节点产品。

- purchase-reserved-node-offering
- describe-reserved-node-offerings
- describe-orderable-cluster-options

您可以使用以下 Amazon Redshift API 操作购买预留节点产品。

- PurchaseReservedNodeOffering
- DescribeReservedNodeOfferings
- DescribeOrderableClusterOptions

Amazon Redshift 中的安全性

Amazon的云安全性的优先级最高。作为 Amazon 客户，您将从专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。

安全性是 Amazon 和您的共同责任。责任共担模型将其描述为云的 安全性和云中 的安全性：

- 云的安全性 – Amazon负责保护在Amazon云中运行Amazon服务的基础设施。Amazon还向您提供可安全使用的服务。作为 Amazon 合规计划的一部分，我们的安全有效性会定期由第三方审核员进行测试和验证。要了解适用于 Amazon Redshift 的合规性计划，请参阅合规性计划范围内的 Amazon 服务。
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

您可以在以下四个级别控制对 Amazon Redshift 资源的访问：

- 集群管理 – 创建、配置和删除集群的能力由授予给与您的 Amazon 安全凭证相关的 IAM 用户或账户的权限进行控制。具有适当权限的 IAM 用户可以使用 Amazon Web Services Management Console、Amazon Command Line Interface (CLI) 或 Amazon Redshift 应用程序编程接口 (API) 来管理其集群。可以借助 IAM 策略对这种访问加以管理。有关详细信息，请参阅Amazon Redshift 中的 Identity and Access Management (p. 356)。
- 集群连接 – Amazon Redshift 安全组用于指定有权连接到无类别域间路由 (CIDR) 格式的 Amazon Redshift 集群的 Amazon 实例。有关创建 Amazon Redshift、Amazon EC2 和 Amazon VPC 安全组以及将其与集群关联的信息，请参阅Amazon Redshift 集群安全组 (p. 458)。
- 数据库访问 – 访问数据库对象（如表和视图）的功能由 Amazon Redshift 数据库中的用户账户所控制。用户只能访问其用户账户有权访问的数据库中的资源。您可以创建这些 Amazon Redshift 用户账户并使用 CREATE USER、CREATE GROUP、GRANT 和 REVOKE SQL 语句管理权限。有关更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的管理数据库安全。
- 临时数据库凭证和单点登录 –除了使用 SQL 命令（如 CREATE USER 和 ALTER USER）创建和管理数据库用户之外，您还可以使用自定义 Amazon Redshift JDBC 或 ODBC 驱动程序配置 SQL 客户端。这些驱动程序将创建数据库用户和临时密码的过程作为数据库登录过程的一部分进行管理。

  这些驱动程序将基于 Amazon Identity and Access Management (IAM) 身份验证来验证数据库用户的身份。如果您已在 Amazon 外部管理用户身份，则可以使用符合 SAML 2.0 标准的身份提供商 (IdP) 来管理对 Amazon Redshift 资源的访问。您使用 IAM 角色将 IdP 和 Amazon 配置为允许联合身份用户生成临时数据库凭证并登录 Amazon Redshift 数据库。有关更多信息，请参阅使用 IAM 身份验证生成数据库用户凭证 (p. 393)。

此文档将帮助您了解如何在使用 Amazon Redshift 时应用责任共担模式。以下主题说明如何配置 Amazon Redshift 以实现您的安全性和合规性目标。您还会了解如何使用其他 Amazon 服务以帮助您监控和保护 Amazon Redshift 资源。

主题

- Amazon Redshift 中的数据保护 (p. 346)
- Amazon Redshift 中的 Identity and Access Management (p. 356)
- Amazon Redshift 中的日志记录和监控 (p. 443)
- Amazon Redshift 的合规性验证 (p. 456)
- Amazon Redshift 中的恢复能力 (p. 457)
- Amazon Redshift 中的基础设施安全性 (p. 457)

- Amazon Redshift 中的配置和漏洞分析 (p. 461)

Amazon Redshift 中的数据保护

Amazon 责任共担模式适用于 Amazon Redshift 中的数据保护。如该模式中所述，Amazon 负责保护运行所有 Amazon Web Services 云 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 Amazon Web Services 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

出于数据保护目的，我们建议您保护 Amazon Web Services 账户 凭证并使用 Amazon Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 Amazon 资源进行通信。建议使用 TLS 1.2 或更高版本。
- 使用 Amazon CloudTrail 设置 API 和用户活动日志记录。
- 使用 Amazon 加密解决方案以及 Amazon 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Simple Storage Service（Amazon S3）中的个人数据。
- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（例如您客户的电子邮件地址）放入标签或自由格式字段（例如名称字段）。这包括当您通过控制台、API、Amazon CLI 或 Amazon 开发工具包使用 Amazon Redshift 或其他 Amazon 服务时。您在用于名称的标签或自由格式字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，我们强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

AQUA（高级查询加速器）是在独立于 Amazon Redshift 集群的服务器上运行的多租户服务。AQUA 支持身份验证、加密、隔离和合规性，以确保静态数据和传输中的数据安全。访问 Amazon Redshift 的权限同样适用于 AQUA。在 AQUA 服务器上处理的查询以独立的进程运行，以确保数据保护。

数据加密

数据保护指在数据传输（发往和离开 Amazon Redshift 时）和处于静态（存储在 Amazon Redshift 数据中心的磁盘上时）期间保护数据。可以使用 SSL 或使用客户端加密保护传输中的数据。您可以通过以下选项在 Amazon Redshift 中保护静态数据。

- 使用服务器端加密 – 您请求 Amazon Redshift 在将数据保存到数据中心的磁盘上之前加密对象，并在下载对象时进行解密。
- 使用客户端加密 – 您可以在客户端加密数据并将加密的数据上载到 Amazon Redshift。在这种情况下，您需要管理加密过程、加密密钥和相关的工具。

静态加密

服务器端加密是静态数据加密，即，Amazon Redshift 在将数据写入其数据中心时选择性地对其进行加密，并在您访问时进行解密。只要您验证了您的请求并且拥有访问权限，您访问加密和未加密数据的方式就没有区别。

Amazon Redshift 通过加密为静态数据提供保护。（可选）您可以通过高级加密标准 AES-256，为存储在集群中磁盘上的所有数据以及 Simple Storage Service（Amazon S3）中的所有备份提供保护。

要管理用于加密和解密 Amazon Redshift 资源的密钥，您可以使用 Amazon Key Management Service (Amazon KMS)。Amazon KMS 将安全、高度可用的硬件和软件结合起来，提供可扩展到云的密钥管理系统。利用 Amazon KMS，您可创建加密密钥并定义控制这些密钥的使用方式的策略。Amazon KMS 支持 Amazon CloudTrail，因此，您可审核密钥使用情况以验证密钥是否使用得当。您可将 Amazon KMS 密钥与 Amazon Redshift 和支持的 Amazon 服务结合使用。有关支持 Amazon KMS 的服务的列表，请参阅 Amazon Key Management Service 开发人员指南中的 Amazon 服务如何使用 Amazon KMS。

AQUA（高级查询加速器）接收并使用 Amazon Redshift 用于在 Simple Storage Service（Amazon S3）中存储数据快照的数据库加密密钥 (DEK)。Amazon Redshift 使用信封加密，这意味着您可以轮换密钥，而无需重新加密数据块。如果 Amazon Redshift 集群未加密，则 AQUA 会使用自己的托管密钥对数据进行加密。有关更多信息，请参阅Amazon Redshift 数据库加密 (p. 347)。

在某些情况下，您可以撤消 Amazon KMS 对与集群关联的 IAM 角色的访问权限。如果是这样，则在进行中的查询完成后，无法进一步访问 AQUA 中缓存的数据。这是因为 AQUA 不会在单个下推扫描或聚合操作之外保留密钥。这种缺乏持久性也意味着您无法访问有关这些数据块的任何元数据。

Amazon Redshift 查询编辑器 v2 安全存储输入到查询编辑器中的信息，如下所示：

- 用于加密查询编辑器 v2 数据的 KMS 密钥的 Amazon Resource Name（ARN）。
- 数据库连接信息。
- 文件和文件夹的名称和内容。

Amazon Redshift 查询编辑器 v2 使用 KMS 密钥或服务账户 KMS 密钥的数据块级加密来加密信息。Amazon Redshift 数据的加密由 Amazon Redshift 集群属性控制。

主题

- Amazon Redshift 数据库加密 (p. 347)

Amazon Redshift 数据库加密

在 Amazon Redshift 中，您可以为集群启用数据库加密，以保护静态数据。为集群启用加密时，会对集群及其快照的数据块和系统元数据进行加密。

您可以在启动集群时启用加密，也可以修改未加密的集群以使用 Amazon Key Management Service (Amazon KMS) 加密。为此，您可以使用 Amazon 托管式密钥或客户托管式密钥。当您修改集群以启用 Amazon KMS 加密时，Amazon Redshift 会自动将您的数据迁移到新加密的集群。从加密集群创建的快照也会被加密。您还可以通过修改集群和更改 Encrypt database（加密数据库）选项将加密的集群迁移到未加密的集群。有关更多信息，请参阅更改集群加密 (p. 350)。

虽然加密是 Amazon Redshift 中的一项可选设置，但我们建议您为包含敏感数据的集群启用该设置。此外，根据管理数据的准则或法规，您可能需要使用加密。例如，支付卡行业数据安全标准 (PCI DSS)、萨班斯-奥克斯利法 (SOX)、健康保险流通与责任法案 (HIPAA) 以及其他此类法规为处理特定类型数据提供了准则。

Amazon Redshift 使用加密密钥层次结构来加密数据库。您可以使用 Amazon Key Management Service (Amazon KMS) 或硬件安全模块 (HSM) 来管理该层次结构中的顶级加密密钥。Amazon Redshift 用于加密的流程因您管理密钥的方式而异。Amazon Redshift 自动集成了 Amazon KMS 但没有集成 HSM。当您使用 HSM 时，必须使用客户端和服务器证书在 Amazon Redshift 和 HSM 之间配置受信任的连接。

主题

- 使用 Amazon KMS 为 Amazon Redshift 进行数据库加密 (p. 348)
- 使用硬件安全模块的 Amazon Redshift 加密 (p. 349)
- Amazon Redshift 中的加密密钥轮换 (p. 350)
- 更改集群加密 (p. 350)
- 使用控制台配置数据库加密 (p. 352)
- 使用 Amazon Redshift API 和 Amazon CLI 配置数据库加密 (p. 353)

使用 Amazon KMS 为 Amazon Redshift 进行数据库加密

当您选择 Amazon KMS 对 Amazon Redshift 进行密钥管理时，加密密钥层次结构有四层。按层次顺序，这些密钥是根密钥、集群加密密钥（CEK）、数据库加密密钥（DEK）和数据加密密钥。

当您启动集群时，Amazon Redshift 会返回 Amazon KMS keys 列表，此列表为您的 Amazon 账户所创建或有权在 Amazon KMS 中使用。在加密层次结构中选择要用作根密钥的 KMS 密钥。

默认情况下，Amazon Redshift 选择您的默认密钥作为根密钥。您的默认密钥是由 Amazon 管理的密钥，系统为您的 Amazon 账户创建该密钥，以便在 Amazon Redshift 中使用。当您首次启动 Amazon 区域中某个已加密的集群并选择默认密钥时，Amazon KMS 便会创建此密钥。

如果不希望使用默认密钥，在 Amazon Redshift 中启动集群之前，您必须在 Amazon KMS 中单独拥有（或创建）一个客户托管式 KMS 密钥。客户托管式密钥可为您提供更大灵活度，包括创建、转动、禁用、定义访问控制，以及审计用于保护数据的加密密钥的能力。有关创建 KMS 密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

如果您希望使用其他 Amazon 账户中的 Amazon KMS 密钥，则您必须有权使用该密钥并在 Amazon Redshift 中指定其 Amazon Resource Name (ARN)。有关在 Amazon KMS 中访问密钥的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的控制对您的密钥的访问。

当您选择根密钥之后，Amazon Redshift 会请求 Amazon KMS 生成数据密钥，并使用所选的根密钥对其进行加密。此数据密钥在 Amazon Redshift 中用作 CEK。Amazon KMS 将已加密的 CEK 导出到 Amazon Redshift 中，该 CEK 以及对 KMS 密钥的授权和 CEK 的加密上下文在独立于该集群的网络中的磁盘内部存储。只有加密的 CEK 才会导出到 Amazon Redshift；KMS 密钥仍保留在 Amazon KMS 中。Amazon Redshift 还会通过安全通道将已加密的 CEK 传递到集群中，并将其加载到内存中。然后，Amazon Redshift 会调用 Amazon KMS 以解密 CEK，并将已解密的 CEK 加载到内存中。有关授予、加密上下文和其他 Amazon KMS 相关概念，请参阅 Amazon Key Management Service 开发人员指南中的概念。

接着，Amazon Redshift 会随机生成一个密钥以用作 DEK，并将其加载到集群的内存中。已解密的 CEK 用于加密 DEK，然后，Amazon Redshift 便会通过安全通道从该集群传递 DEK，以使其在独立于该集群的网络中的磁盘内部存储。与 CEK 一样，DEK 的加密版本和解密版本都会加载到集群中的内存中。然后，DEK 的解密版本将用于加密为数据库中的每个数据块随机生成的各个加密密钥。

当该集群重启时，Amazon Redshift 先使用内部存储的加密版 CEK 和 DEK，将其重新加载到内存中，然后调用 Amazon KMS 以再次使用 KMS 密钥解密 CEK，以便其加载到内存中。然后使用解密的 CEK 再次解密 DEK，并将解密的 DEK 加载到内存中，并根据需要用于加密和解密数据块密钥。

有关创建使用 Amazon KMS 密钥加密的 Amazon Redshift 集群的更多信息，请参阅创建集群 (p. 84)和使用 Amazon CLI 和 Amazon Redshift API 管理集群 (p. 89)。

将 Amazon KMS 加密的快照复制到另一个 Amazon 区域

Amazon KMS 密钥特定于 Amazon 区域。如果您启用将 Amazon Redshift 快照复制到另一个 Amazon 区域的功能，并且源集群及其快照使用 Amazon KMS 中的根密钥进行加密，则您需要为 Amazon Redshift 配置授权，以便在目标 Amazon 区域中使用根密钥。此授权使 Amazon Redshift 可以在目标 Amazon 区域中加密快照。有关跨区域快照复制的更多信息，请参阅将快照复制到另一个 Amazon 区域 (p. 321)。

> **Note**
>
> 如果您启用已加密集群中的快照复制功能，并针对根密钥使用 Amazon KMS，则无法重命名集群，因为集群名称是加密上下文的一部分。如果您必须重命名集群，则可以禁用在源 Amazon 区域中复制快照，重命名集群，然后再次配置并启用快照复制。

配置复制快照的授权的过程如下所示。

1. 在目标 Amazon 区域中，通过执行以下操作创建快照复制授权：
   - 如果您没有 Amazon KMS 密钥可用，请创建一个。有关创建 Amazon KMS 密钥的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的创建密钥。

- 指定快照复制授权的名称。此名称必须在您的 Amazon 账户的 Amazon 区域中唯一。
- 为您创建的授权指定 Amazon KMS 密钥 ID。如果您未指定密钥 ID，则该授予会应用于您的默认密钥。

2. 在源 Amazon 区域中，启用快照复制并指定您在目标 Amazon 区域中创建的快照复制授权的名称。

前述流程仅适用于您使用 Amazon CLI、Amazon Redshift API 或开发工具包启用快照复制功能的情况。如果您使用控制台，在您启用跨区域快照复制时，Amazon Redshift 将提供相应的工作流程以配置授权。有关使用控制台为 Amazon KMS 加密的集群配置跨区域快照复制的更多信息，请参阅为 Amazon KMS 加密的集群配置跨区域快照复制 (p. 330)。

快照复制到目标 Amazon 区域之前，Amazon Redshift 使用源 Amazon 区域中的根密钥解密快照并使用 Amazon Redshift 内部管理的随机生成的 RSA 密钥临时对其进行重新加密。然后，Amazon Redshift 将快照通过安全通道复制到目标 Amazon 区域，使用内部托管式 RSA 密钥解密快照，然后使用目标 Amazon 区域中的根密钥重新加密快照。

有关为 Amazon KMS 加密的集群配置快照复制授权的更多信息，请参阅将 Amazon Redshift 配置为通过 Amazon Redshift API 和 Amazon CLI 使用 Amazon KMS 加密密钥 (p. 353)。

使用硬件安全模块的 Amazon Redshift 加密

如果您不使用 Amazon KMS 管理密钥，则可以使用硬件安全模块 (HSM) 在 Amazon Redshift 中管理密钥。

> Important
>
> DC2 和 RA3 节点类型不支持 HSM 加密。

HSM 是直接控制密钥生成和管理的设备。HSM 使密钥管理独立于应用程序和数据库层，以提供更强的安全性。Amazon Redshift 支持 Amazon CloudHSM Classic 进行密钥管理。使用 HSM 管理加密密钥的加密流程与 Amazon KMS 不同。

> Important
>
> Amazon Redshift 仅支持 Amazon CloudHSM Classic。我们不支持较新的 Amazon CloudHSM 服务。
> Amazon CloudHSM Classic 不对新客户开放。有关更多信息，请参阅 CloudHSM Classic 定价。Amazon CloudHSMClassic 并非在所有 Amazon 区域可用。有关可用 Amazon 区域的更多信息，请参阅 Amazon 区域列表。

当您配置集群以使用 HSM 时，Amazon Redshift 会向 HSM 发出请求，以生成并存储要用作 CEK 的密钥。不过，与 Amazon KMS 不同，HSM 不会将 CEK 导出到 Amazon Redshift 中。Amazon Redshift 会在集群中随机生成 DEK，并将其传递到 HSM 中，由 CEK 进行加密。HSM 会将已加密的 DEK 返回到 Amazon Redshift 中，由随机生成的内部根密钥进行加密并在独立于该集群的网络中的磁盘内部存储。Amazon Redshift 还会将解密版 DEK 加载到集群的内存中，以便 DEK 可用于加密和解密数据块的各个密钥。

如果该集群重启，则 Amazon Redshift 会使用内部根密钥解密内部存储的双重加密 DEK，以将内部存储的 DEK 还原为 CEK 加密状态。然后，CEK 加密的 DEK 会传递到 HSM 进行加密并传递回 Amazon Redshift，以便再次加载到内存中用于各个数据块密钥。

在 Amazon Redshift 和 HSM 之间配置受信任的连接

如果您选择使用 HSM 管理集群密钥，则需要在 Amazon Redshift 和 HSM 之间配置受信任的网络连接。执行此操作需要配置客户端和服务器证书。在加密和解密操作过程中，受信任的连接用于在 HSM 和 Amazon Redshift 之间传递加密密钥。

Amazon Redshift 会通过随机生成的私有和公有键前缀创建公有客户端证书。这些都进行了加密，并在内部存储。您可以在 HSM 中下载并注册公有客户端证书，并将其分配给适用的 HSM 分区。

您需要为 Amazon Redshift 提供 HSM IP 地址、HSM 分区名称、HSM 分区密码以及公有 HSM 服务器证书，该证书使用内部根密钥进行了加密。Amazon Redshift 会完成配置流程并验证其能否连接到 HSM。如果

无法使用，则集群将进入 INCOMPATIBLE_HSM 状态，并且不会创建集群。在这种情况下，您必须删除不完整的集群，然后重试。

Important

当您将集群修改为使用其他 HSM 分区时，Amazon Redshift 将验证它是否能连接到新分区，但不会验证是否存在有效的加密密钥。在使用新分区之前，您必须将密钥复制到新分区。如果集群已重新启动，而 Amazon Redshift 无法找到有效密钥，重新启动将失败。有关更多信息，请参阅在 HSM 中复制密钥。

初始配置之后，如果 Amazon Redshift 无法连接到 HSM，则系统会记录一个事件。有关这些事件的更多信息，请参阅 Amazon Redshift 事件通知。

Amazon Redshift 中的加密密钥轮换

在 Amazon Redshift 中，您可以轮换已加密集群的加密密钥。当您启动密钥轮换流程时，Amazon Redshift 会轮换指定集群以及该集群的任何自动或手动快照的 CEK。Amazon Redshift 还会轮换指定集群的 DEK，但不会轮换快照的 DEK，而这些快照在 Amazon Simple Storage Service（Amazon S3）内部存储并使用现有 DEK 进行了加密。

在轮换进行过程中，该集群将处于 ROTATING_KEYS 状态一直到轮换完成为止，届时，该集群将还原为 AVAILABLE 状态。Amazon Redshift 会在密钥轮换过程中处理解密和重新加密。

Note

如果没有源集群，则无法轮换快照的密钥。在删除集群之前，请考虑其快照是否依赖密钥轮换。

由于集群在密钥轮换过程中暂时不可用，因此您应该只在数据需求需要时或在怀疑密钥可能已被破坏时轮换密钥。作为最佳实践，您应该查看存储的数据的类型，并计划对该数据进行加密的密钥的轮换频率。轮换密钥的频率取决于贵公司的数据安全策略以及关于敏感数据和监管合规的任何行业标准。确保您的计划平衡安全需求和集群的可用性考虑因素。

有关轮换密钥的更多信息，请参阅使用 Amazon Redshift 控制台轮换加密密钥 (p. 353)和使用 Amazon Redshift API 和 Amazon CLI 轮换加密密钥 (p. 354)。

更改集群加密

您可以使用 Amazon 托管式密钥或客户托管式密钥修改未加密的集群以使用 Amazon Key Management Service（Amazon KMS）加密。当您修改集群以启用 Amazon KMS 加密时，Amazon Redshift 会自动将您的数据迁移到新加密的集群。您还可以通过修改集群将未加密的集群迁移到加密的集群。

在迁移操作过程中，您的集群在只读模式下可用，并且集群状态显示为调整大小。

如果您的集群配置为启用跨 Amazon 区域快照副本，您必须在更改加密之前将其禁用。有关更多信息，请参阅将快照复制到另一个 Amazon 区域 (p. 321)和为 Amazon KMS 加密的集群配置跨区域快照复制 (p. 330)。您无法通过修改集群启用硬件安全模块 (HSM) 加密。而是创建一个新的 HSM 加密集群，并将您的数据迁移到新集群。有关更多信息，请参阅迁移到 HSM 加密的集群 (p. 351)。

要修改集群上的数据库加密

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后选择要修改加密的集群。
3. 选择 Properties (属性)。
4. 在 Database configurations（数据库配置）部分，选择 Edit（编辑），然后选择 Edit encryption（编辑加密）。
5. 选择其中一个加密选项，然后选择 Save changes（保存更改）。

要使用 CLI 更改集群加密

若要修改未加密的集群以使用 Amazon KMS，请运行 `modify-cluster` CLI 命令并指定 `--encrypted`，如下所示。预设情况下，使用默认 KMS 密钥。要指定客户托管式密钥，请包含 `--kms-key-id` 选项。

```
aws redshift modify-cluster --cluster-identifier <value> --encrypted --kms-key-id <value>
```

要从集群中删除加密，请运行以下 CLI 命令。

```
aws redshift modify-cluster --cluster-identifier <value> --no-encrypted
```

迁移到 HSM 加密的集群

要将未加密的集群迁移到使用硬件安全模块 (HSM) 加密的集群，请创建新的加密集群并将数据移动到新集群。您不能通过修改集群迁移到 HSM 加密的集群。

要从未加密的集群迁移到 HSM 加密的集群，首先从现有的源集群中卸载数据。然后使用所选的加密设置将数据重新加载到新的目标集群中。有关启动加密集群的更多信息，请参阅Amazon Redshift 数据库加密 (p. 347)。

在迁移过程中，源集群可用于只读查询，直到最后一步。最后一步是重命名目标集群和源集群，用于切换端点，以便将所有流量路由到新的目标集群。在重命名后重新启动之前，目标集群不可用。在传输数据时，暂停源集群上的所有数据加载和其他写入操作。

准备迁移

1. 确定与 Amazon Redshift 交互的所有关联系统，例如业务情报 (BI) 工具以及提取、转换和加载 (ETL) 系统。
2. 确定用于测试迁移的验证查询。

   例如，您可以使用以下查询来查找用户定义表的数目。

   ```
   select count(*)
   from pg_table_def
   where schemaname != 'pg_catalog';
   ```

   以下查询返回所有用户定义表的列表以及每个表中的行数。

   ```
   select "table", tbl_rows
   from svv_table_info;
   ```

3. 选择迁移的好时机。要查找集群使用率最低的时间，请监控 CPU 利用率和数据库连接数量等集群指标。有关更多信息，请参阅查看集群性能数据 (p. 480)。
4. 删除未使用的表。

   要创建表列表和查询每个表的次数，请运行以下查询。

   ```
   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. 启动新的加密集群。

   对目标集群使用与源集群相同的端口号。有关启动加密集群的更多信息，请参阅Amazon Redshift 数据库加密 (p. 347)。
6. 设置卸载和加载过程。

   您可以使用 Amazon Redshift 卸载/复制实用工具来帮助您在集群之间迁移数据。该实用工具会将源集群的数据导出到 Simple Storage Service（Amazon S3）上的某个位置。使用 Amazon KMS 加密数据。然后，该实用工具会自动将数据导入到目标中。或者，您可以使用该实用程序在迁移完成后清除 Simple Storage Service（Amazon S3）。
7. 运行测试以验证您的过程并估计必须暂停写入操作的时间。

   在卸载和加载操作期间，通过暂停数据加载和其他写入操作来维护数据一致性。使用最大的表之一，运行卸载和加载过程，以帮助您估计时间。
8. 创建数据库对象，如 schema、视图和表。要帮助您生成必要的数据定义语言 (DDL) 语句，您可以使用 Amazon GitHub 存储库中的 AdminViews 中的脚本。

要迁移集群

1. 停止源集群上的所有 ETL 流程。

   要确认进程中未执行任何写入操作，请使用 Amazon Redshift 管理控制台来监控写入 IOPS。有关更多信息，请参阅查看集群性能数据 (p. 480)。
2. 运行您之前确定的验证查询，以便在迁移前收集有关未加密源集群的信息。
3. （可选）创建一个工作负载管理 (WLM) 队列，以使用源集群和目标集群中的最大可用资源。例如，创建名为 `data_migrate` 的队列并将队列配置为内存 95%，并发性为 4。有关更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的基于用户组和查询组将查询路由至队列中。
4. 使用 `data_migrate` 队列，运行 UnloadCopyUtility。

   使用 Amazon Redshift 控制台监控 UNLOAD 和 COPY 进程。
5. 再次运行验证查询，并验证结果是否与源集群的结果匹配。
6. 重命名源集群和目标集群以交换端点。为避免中断，请在工作时间以外执行此操作。
7. 验证您是否可以使用所有 SQL 客户端（如 ETL 和报告工具）连接到目标集群。
8. 关闭未加密的源集群。

使用控制台配置数据库加密

您可以使用 Amazon Redshift 控制台配置 Amazon Redshift 以使用 HSM 和轮换加密密钥。有关如何使用 Amazon KMS 加密密钥创建集群的信息，请参阅创建集群 (p. 84)和使用 Amazon CLI 和 Amazon Redshift API 管理集群 (p. 89)。

要修改集群上的数据库加密

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后选择要移动其快照的集群。
3. 对于 Actions（操作），选择 Modify（修改）以显示配置页面。
4. 在 Database configuration（数据库配置）部分中，选择 Encryption（加密）的设置，然后选择 Modify cluster（修改集群）。

使用 Amazon Redshift 控制台轮换加密密钥

您可以借助 Amazon Redshift 控制台以使用以下过程来轮换加密密钥。

要为集群轮换加密密钥

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后选择要更新加密密钥的集群。
3. 对于 Actions（操作），选择 Rotate encryption（轮换加密）以显示 Rotate encryption keys（轮换加密密钥）页面。
4. 正在 Rotate encryption keys（轮换加密密钥）页面上，选择 Rotate encryption keys（轮换加密密钥）。

使用 Amazon Redshift API 和 Amazon CLI 配置数据库加密

使用 Amazon Redshift API 和 Amazon Command Line Interface (Amazon CLI) 为 Amazon Redshift 数据库配置加密密钥选项。有关数据库加密的更多信息，请参阅Amazon Redshift 数据库加密 (p. 347)。

将 Amazon Redshift 配置为通过 Amazon Redshift API 和 Amazon CLI 使用 Amazon KMS 加密密钥

您可以使用以下 Amazon Redshift API 操作将 Amazon Redshift 配置为使用 Amazon KMS 加密密钥。

- CreateCluster
- CreateSnapshotCopyGrant
- DescribeSnapshotCopyGrants
- DeleteSnapshotCopyGrant
- DisableSnapshotCopy
- EnableSnapshotCopy

您可以使用以下 Amazon Redshift CLI 操作将 Amazon Redshift 配置为使用 Amazon KMS 加密密钥。

- create-cluster
- create-snapshot-copy-grant
- describe-snapshot-copy-grants
- delete-snapshot-copy-grant
- disable-snapshot-copy
- enable-snapshot-copy

将 Amazon Redshift 配置为通过 Amazon Redshift API 和 Amazon CLI 使用 HSM

您可以使用下列 Amazon Redshift API 操作来管理硬件安全模块。

- CreateHsmClientCertificate
- CreateHsmConfiguration
- DeleteHsmClientCertificate
- DeleteHsmConfiguration
- DescribeHsmClientCertificates
- DescribeHsmConfigurations

您可以使用下列 Amazon CLI 操作来管理硬件安全模块。

- create-hsm-client-certificate
- create-hsm-configuration
- delete-hsm-client-certificate
- delete-hsm-configuration
- describe-hsm-client-certificates
- describe-hsm-configurations

使用 Amazon Redshift API 和 Amazon CLI 轮换加密密钥

您可以使用下列 Amazon Redshift API 操作来轮换加密密钥。

- RotateEncryptionKey

您可以使用下列 Amazon CLI 操作来轮换加密密钥。

- rotate-encryption-key

传输中加密

您可以配置环境来保护传输中数据的机密性和完整性。

在 Amazon Redshift 集群和 SQL 客户端之间加密通过 JDBC/ODBC 传输的数据：

- 您可以通过 Java 数据库连接 (JDBC) 和开放式数据库连接 (ODBC) 这两种连接将 SQL 客户端工具连接到 Amazon Redshift 集群。
- Amazon Redshift 支持安全套接字层 (SSL) 连接来加密数据和服务器证书，以验证客户端连接到的服务器证书。客户端连接到 Amazon Redshift 集群的领导节点。有关更多信息，请参阅配置连接的安全选项 (p. 217)。
- 为了支持 SSL 连接，Amazon Redshift 会在每个集群中创建并安装 Amazon Certificate Manager (ACM) 颁发的证书。有关更多信息，请参阅将 SSL 连接过渡到 ACM 证书 (p. 220)。
- 为保护Amazon云中的传输中数据，Amazon Redshift 使用硬件加速的 SSL 与 Simple Storage Service（Amazon S3）或 Amazon DynamoDB 通信以执行 COPY、UNLOAD、备份和还原操作。

Amazon Redshift 集群与 Simple Storage Service（Amazon S3）或 DynamoDB 之间传输的数据的加密：

- Amazon Redshift 使用硬件加速的 SSL 与 Simple Storage Service（Amazon S3）或 DynamoDB 通信以执行 COPY、UNLOAD、备份和还原操作。
- Redshift Spectrum 支持使用受 Amazon Key Management Service (KMS) 管理的账户默认密钥的 Simple Storage Service（Amazon S3）服务器端加密 (SSE)。
- 使用 Simple Storage Service（Amazon S3）和 Amazon KMS 加密 Amazon Redshift 加载。有关更多信息，请参阅使用 Simple Storage Service（Amazon S3）和 Amazon KMS 加密您的 Amazon Redshift 加载。

对在 Amazon CLI、开发工具包或 API 客户端与 Amazon Redshift 端点之间传输的数据进行加密和签名：

- Amazon Redshift 为加密传输中的数据提供了 HTTPS 端点。
- 为了保护向 Amazon Redshift 出的 API 请求的完整性，API 调用必须由调用者签名。调用由 X.509 证书或客户的 Amazon 秘密访问密钥根据前面版本 4 签名流程 (Sigv4) 签名。有关更多信息，请参阅 https://docs.amazonaws.cn/general/latest/gr/signature-version-4.html 一般参考中的Amazon签名版本 4 签名流程。
- 使用 Amazon CLI 或 Amazon 开发工具包之一向 Amazon 发出请求。这些工具会自动使用您在配置工具时指定的访问密钥为您签署请求。

Amazon Redshift 集群与 AQUA 之间传输的数据的加密：

- 数据通过 TLS 加密通道在 AQUA 与 Amazon Redshift 集群之间传输。该通道根据签名版本 4 签名流程 (Sigv4) 进行签名。有关更多信息，请参阅 https://docs.amazonaws.cn/general/latest/gr/signature-version-4.html 一般参考中的Amazon签名版本 4 签名流程。

Amazon Redshift 集群与 Amazon Redshift 查询编辑器 v2 之间传输的数据加密

- 数据通过 TLS-加密通道在查询编辑器 V2 与 Amazon Redshift 集群之间传输。

密钥管理

您可以配置环境以使用密钥保护数据：

- Amazon Redshift 自动与 Amazon Key Management Service (Amazon KMS) 集成以进行密钥管理。Amazon KMS 使用信封加密。有关更多信息，请参阅信封加密。
- 在 Amazon KMS 中管理加密密钥时，Amazon Redshift 使用基于密钥的四层架构进行加密。此架构包括随机生成的 AES-256 数据加密密钥、数据库密钥、集群密钥和根密钥。有关更多信息，请参阅 Amazon Redshift 如何使用 Amazon KMS。
- 您可以在 Amazon KMS 中创建自己的客户托管式密钥。有关更多信息，请参阅创建密钥。
- 您也可为新 Amazon KMS keys 导入自己的密钥材料。有关更多信息，请参阅将密钥材料导入 Amazon Key Management Service (Amazon KMS) 中。
- Amazon Redshift 支持在外部硬件安全模块 (HSM) 中管理加密密钥。HSM 可以为本地，也可以为 Amazon CloudHSM。当您使用 HSM 时，必须使用客户端和服务器证书在 Amazon Redshift 和 HSM 之间配置受信任的连接。Amazon Redshift 仅支持 Amazon CloudHSM Classic 进行密钥管理。有关更多信息，请参阅使用硬件安全模块的 Amazon Redshift 加密 (p. 349)。有关 Amazon CloudHSM 的信息，请参阅什么是 Amazon CloudHSM？
- 您可以轮换已加密集群的加密密钥。有关更多信息，请参阅Amazon Redshift 中的加密密钥轮换 (p. 350)。

数据令牌化

令牌化是为了数据安全目的将实际值替换为不透明值的过程。安全敏感型应用程序使用令牌化来替换敏感数据，如个人身份信息（PII）或受保护健康信息（PHI），以降低安全风险。取消令牌化使用适当的安全策略为授权用户使用实际值来反转令牌。

为了与第三方令牌化服务集成，您可以使用 Amazon Redshift 用户定义的函数 (UDF)，这些函数使用 Amazon Lambda 创建。有关更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 Lambda 用户定义的函数。例如，请参阅 Protegrity。

Amazon Redshift 将令牌化请求发送到通过 REST API 或预定义端点访问的令牌化服务器。两个或多个互补的 Lambda 函数处理令牌化和取消令牌化请求。对于此处理，您可以使用第三方令牌化提供程序提供的 Lambda 函数。您还可以使用在 Amazon Redshift 中注册为 Lambda UDF 的 Lambda 函数。

例如，假设提交的查询在列上调用令牌化或取消令牌化 UDF。Amazon Redshift 集群可以后台处理适用的参数行，并将这些行分批并行发送到 Lambda 函数。Amazon Redshift 计算节点和 Lambda 之间的数据传输是在客户端无法访问的独立隔离网络连接中进行的。Lambda 函数将数据传递到令牌化服务器端点。令牌化服务器根据需要对数据进行令牌化或取消令牌化，并返回数据。然后，Lambda 函数将结果传输到 Amazon Redshift 集群进行进一步处理（如有必要），然后返回查询结果。

互联网络流量隐私

要在 Amazon Redshift 与公司网络上的客户端和应用程序之间路由流量，请执行以下操作：

- 在 Virtual Private Cloud (VPC) 和公司网络之间建立私有连接。通过互联网设置 IPsec VPN 连接或使用 Amazon Direct Connect 连接设置专用物理连接。Amazon Direct Connect 使您可以在本地网络与 Amazon VPC 之间直接建立一个专用虚拟接口，从而在您的网络和 VPC 之间提供一个专用的高带宽网络连接。借助多个虚拟接口，您甚至可以在保持网络隔离性的同时，与多个 VPC 建立专用连接。有关更多信息，请参阅什么是 Amazon Site-to-Site VPN？和什么是 Amazon Direct Connect？

要在 VPC 中的 Amazon Redshift 集群与相同 Amazon 区域中的 Simple Storage Service（Amazon S3）桶之间路由流量，请执行以下操作：

- 设置 Simple Storage Service（Amazon S3）私有 VPC 端点以从 ETL 负载或分载私密访问 Simple Storage Service（Amazon S3）数据。有关更多信息，请参阅用于 Simple Storage Service（Amazon S3）的端点。
- 为 Amazon Redshift 集群启用“增强型 VPC 路由”，指定目标 Simple Storage Service（Amazon S3）VPC 端点。Amazon Redshift COPY、UNLOAD 或 CREATE LIBRARY 命令生成的流量随后路由通过私有端点。有关更多信息，请参阅启用增强型 VPC 路由 (p. 294)。

Amazon Redshift 中的 Identity and Access Management

访问 Amazon Redshift 时需要可供 Amazon 用来验证您的请求的凭证。这些凭证必须有权访问 Amazon 资源，如 Amazon Redshift 集群。下面几节提供详细信息来说明如何使用 Amazon Identity and Access Management (IAM) 和 Amazon Redshift 控制谁能访问您的资源，从而对这些资源进行保护：

- 使用身份进行身份验证 (p. 356)
- 访问控制 (p. 358)

使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。有关使用Amazon Web Services Management Console登录的更多信息，请参阅 IAM 用户指南中的以 IAM 用户或根用户身份登录Amazon Web Services Management Console。

您必须作为Amazon Web Services 账户根用户、IAM 用户或代入 IAM 角色以进行身份验证（登录到 Amazon）。您还可以使用公司的单一登录身份验证方法，甚至使用 Google 或 Facebook 登录。在这些情况下，您的管理员以前使用 IAM 角色设置了联合身份验证。在您使用来自其它公司的凭证访问 Amazon 时，您间接地代入了角色。

要直接登录到Amazon Web Services Management Console，请将密码与根用户电子邮件地址或 IAM 用户名一起使用。您可以使用根用户或 IAM 用户访问密钥以编程方式访问 Amazon。Amazon 提供了 SDK 和命令行工具，可使用您的凭证对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。使用 Signature Version 4（用于对入站 API 请求进行验证的协议）完成此操作。有关验证请求的更多信息，请参阅《Amazon 一般参考》中的 Signature Version 4 签名流程。

无论使用何种身份验证方法，您可能还需要提供其它安全信息。例如，Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的在 Amazon 中使用多重身份验证 (MFA)。

Amazon Web Services 账户根用户

当您创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services和资源拥有完全访问权限的登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，

并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《Amazon 一般参考》中的需要根用户凭证的任务。

IAM 用户和组

IAM 用户是Amazon Web Services 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，我们建议依赖于临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

IAM 角色是Amazon Web Services 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 Amazon Web Services Management Console 中暂时代入 IAM 角色。您可以调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 以代入角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南 中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（联合用户访问）– 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。

  如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《Amazon IAM Identity Center (successor to Amazon Single Sign-On) 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 Amazon Web Services，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 – 某些 Amazon Web Services使用其它 Amazon Web Services中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 主体权限 – 当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为主体。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作，请参阅《服务授权参考》https://docs.amazonaws.cn/service-authorization/latest/reference/list_amazonredshift.html中的 Amazon Redshift 的操作、资源和条件键。
  - 服务角色 – 服务角色是服务代表您在您的账户中执行操作而担任的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 IAM 用户指南中的创建向 Amazon Web Service 委派权限的角色。
  - 服务相关角色 – 服务相关角色是与 Amazon Web Service关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配

给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

访问控制

您可以使用有效的凭证来对自己的请求进行身份验证，但您还必须拥有权限才能创建或访问 Amazon Redshift 资源。例如，您必须拥有权限才能创建 Amazon Redshift 集群、创建快照、添加事件订阅等。

下面几节介绍如何管理 Amazon Redshift 的权限。我们建议您先阅读概述。

- 管理 Amazon Redshift 资源的访问权限的概览 (p. 358)
- 将基于身份的策略（IAM policy）用于 Amazon Redshift (p. 363)

管理 Amazon Redshift 资源的访问权限的概览

每个 Amazon 资源都归某个 Amazon 账户所有，创建或访问这些资源的权限由权限策略控制。账户管理员可以向 IAM 身份（即：用户、组和角色）附加权限策略，某些服务（如 Amazon Lambda）也支持向资源附加权限策略。

> **Note**
>
> 账户管理员（或管理员用户）是具有管理员权限的用户。有关更多信息，请参阅 IAM 用户指南中的 IAM 最佳实践。

在授予权限时，您要决定谁获得权限，获得对哪些资源的权限，以及您允许对这些资源执行的具体操作。

Amazon Redshift 资源和操作

在 Amazon Redshift 中，主要资源是集群。Amazon Redshift 支持可与主要资源配合使用的其他资源，如快照、参数组和事件订阅。这些资源称作子资源。

这些资源和子资源具有与其关联的唯一 Amazon Resource Name (ARN)，如下表所示。

资源类型	ARN 格式
Cluster	`arn:aws:redshift:`*region*`:`*account-id*`:cluster:`*cluster-name*
集群数据库	`arn:aws:redshift:`*region*`:`*account-id*`:dbname:`*cluster-name*`/`*database-name*
集群数据库用户	`arn:aws:redshift:`*region*`:`*account-id*`:dbuser:`*cluster-name*`/`*database-user-name*
集群数据库用户组	`arn:aws:redshift:`*region*`:`*account-id*`:dbgroup:`*cluster-name*`/`*database-group-name*
集群参数组	`arn:aws:redshift:`*region*`:`*account-id*`:parametergroup:`*parameter-group-name*
集群安全组	`arn:aws:redshift:`*region*`:`*account-id*`:securitygroup:`*security-group-name*

资源类型	ARN 格式
CIDR/IP 地址	arn:aws:redshift:*region*:*account-id*:securitygroupingress:*security-group-name*/cidrip/*IP-range*
EC2 安全组	arn:aws:redshift:*region*:*account-id*:securitygroupingress:*security-group-name*/ec2securitygroup/*owner*/*EC2-security-group-id*
事件订阅	arn:aws:redshift:*region*:*account-id*:eventsubscription:*event-subscription-name*
硬件安全模块 (HSM) 客户端证书	arn:aws:redshift:*region*:*account-id*:hsmclientcertificate:*HSM-client-certificate-id*
HSM 配置	arn:aws:redshift:*region*:*account-id*:hsmconfiguration:*HSM-configuration-id*
参数组	arn:aws:redshift:*region*:*account-id*:parametergroup:*parameter-group-name*
Redshift 托管的 VPC 端点	arn:aws:redshift:*region*:*account-id*:managedvpcendpoint:*endpoint-name*
快照	arn:aws:redshift:*region*:*account-id*:snapshot:*cluster-name*/*snapshot-name*
快照复制授权	arn:aws:redshift:*region*:*account-id*:snapshotcopygrant:*snapshot-copy-grant-name*
子网组	arn:aws:redshift:*region*:*account-id*:subnetgroup:*subnet-group-name*

Amazon Redshift 提供一组操作用来处理 Amazon Redshift 资源。有关可用操作的列表，请参阅 Amazon Redshift API 权限参考 (p. 389)。

Amazon Redshift 查询编辑器 v2 资源

这些 Amazon Redshift 查询编辑器 v2 资源具有关联的唯一 Amazon Resource Name（ARN），如下表所示。

资源类型	ARN 格式
连接	arn:aws:sqlworkbench:*region*:*account-id*:connection/
Query	arn:aws:sqlworkbench:*region*:*account-id*:query/
图表	arn:aws:sqlworkbench:*region*:*account-id*:chart/

了解资源所有权

资源所有者是创建资源的 Amazon 账户。也就是说，资源拥有者是 主体实体（根账户、IAM 用户或 IAM 角色）的 Amazon 账户，该账户会对创建资源的请求进行身份验证。以下示例说明了它的工作原理：

- 如果您使用 Amazon 账户的根账户凭证创建数据库集群，则您的 Amazon 账户即为该 Amazon Redshift 资源的拥有者。

- 如果您在 Amazon 账户中创建 IAM 用户并对该用户授予创建 Amazon Redshift 资源的权限，则该用户也可以创建 Amazon Redshift 资源。但是，该用户所属的 Amazon 账户拥有这些 Amazon Redshift 资源。
- 如果您在您的 Amazon 账户中创建具有创建 Amazon Redshift 资源的权限的 IAM 角色，则能够担任该角色的任何人都可以创建 Amazon Redshift 资源。该角色所属的您的 Amazon 账户拥有这些 Amazon Redshift 资源。

管理对资源的访问

权限策略描述了谁可以访问哪些内容。下一节介绍创建权限策略时的可用选项。

> Note
>
> 本节讨论如何在 Amazon Redshift 范围内使用 IAM。这里不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅 IAM 用户指南中的什么是 IAM？。有关 IAM policy 语法和说明的信息，请参阅 IAM 用户指南中的 Amazon IAM policy 参考。

附加到 IAM 身份的策略称作基于身份 的策略（IAM policy），附加到资源的策略称作基于资源 的策略。Amazon Redshift 只支持基于身份的策略（IAM policy）。

基于身份的策略（IAM policy）

您可以向 IAM 身份附加策略。例如，可以：

- 向您账户中的用户或组附加权限策略 – 账户管理员可以使用与特定用户关联的权限策略。此类策略授予该用户创建 Amazon Redshift 资源（例如集群）的权限。
- 向角色附加权限策略（授予跨账户权限）– 您可以向 IAM 角色附加基于身份的权限策略，以授予跨账户的权限。例如，账户 A 中的管理员可以创建一个角色，以向其他Amazon账户（如账户 B）或某项Amazon服务授予跨账户权限，如下所述：
  1. 账户 A 管理员可以创建一个 IAM 角色，然后向该角色附加授予其访问账户 A 中资源的权限策略。
  2. 账户 A 管理员可以把信任策略附加至用来标识账户 B 的角色，账户 B 由此可以作为主体代入该角色。
  3. 之后，账户 B 管理员可以委派权限，指派账户 B 中的任何用户担任该角色。这样，账户 B 中的用户就可以创建或访问账户 A 中的资源了。如果您需要授予 Amazon 服务权限以便用户担任该角色，信任策略中的主体也可以是 Amazon 服务主体。

  有关使用 IAM 委派权限的更多信息，请参阅 IAM 用户指南中的访问权限管理。

下面的示例策略允许某位用户创建、删除、修改和重启您的 Amazon 账户的 Amazon Redshift 集群。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowManageClusters",
      "Effect":"Allow",
      "Action": [
        "redshift:CreateCluster",
        "redshift:DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource":"*"
    }
  ]
}
```

有关将基于身份的策略与 Amazon Redshift 结合使用的更多信息，请参阅将基于身份的策略（IAM policy）用于 Amazon Redshift (p. 363)。有关用户、组、角色和权限的更多信息，请参阅 IAM 用户指南中的身份（用户、组和角色）。

基于资源的策略

其他服务 [如Simple Storage Service（Amazon S3）] 还支持基于资源的权限策略。例如，您可以将策略附加到 S3 桶以管理对该桶的访问权限。Amazon Redshift 不支持基于资源的策略。

指定策略元素：操作、效果、资源和主体

对于每个 Amazon Redshift 资源（请参阅 Amazon Redshift 资源和操作 (p. 358)），该服务都定义了一组 API 操作（请参阅操作）。为授予这些 API 操作的权限，Amazon Redshift 定义了一组您可以在策略中指定的操作。执行一个 API 操作可能需要多个操作的权限。

以下是基本的策略元素：

- Resource（资源）- 在策略中，您可以使用 Amazon Resource Name (ARN) 标识策略应用到的资源。有关更多信息，请参阅Amazon Redshift 资源和操作 (p. 358)。
- 操作 – 您可以使用操作关键字标识要允许或拒绝的资源操作。例如，`redshift:DescribeClusters` 权限允许执行 Amazon Redshift `DescribeClusters` 操作的用户权限。
- Effect（效果）— 您可以指定当用户请求特定操作（可以是允许或拒绝）时的效果。如果没有显式授予（允许）对资源的访问权限，则隐式拒绝访问。您也可显式拒绝对资源的访问，这样可确保用户无法访问该资源，即使有其他策略授予了访问权限的情况下也是如此。
- 主体 – 在基于身份的策略（IAM policy）中，附加了策略的用户是隐式主体。对于基于资源的策略，您可以指定要接收权限的用户、账户、服务或其他实体 (仅适用于基于资源的策略)。Amazon Redshift 不支持基于资源的策略。

有关 IAM policy 语法和描述的更多信息，请参阅 IAM 用户指南中的 Amazon IAM policy 参考。

有关显示所有 Amazon Redshift API 操作及其适用的资源的表，请参阅Amazon Redshift API 权限参考 (p. 389)。

在策略中指定条件

当您授予权限时，可使用访问策略语言来指定规定策略何时生效的条件。例如，您可能希望策略仅在特定日期后应用。有关使用访问策略语言指定条件的更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素：条件。

要确定权限策略适用的条件，请在 IAM 权限策略中包含元素 `Condition`。例如，您可以创建一个策略，允许用户使用 `redshift:CreateCluster` 操作来创建集群，也可以添加 `Condition` 元素来限制用户只能在特定的区域中创建集群。有关详细信息，请参阅使用 IAM policy 条件进行精细访问控制 (p. 361)。有关所有条件键值及其适用的 Amazon Redshift 操作和资源的列表，请参阅Amazon Redshift API 权限参考 (p. 389)。

使用 IAM policy 条件进行精细访问控制

在 Amazon Redshift 中，您可以根据资源的标签使用条件键来限制对资源的访问。以下是常见的 Amazon Redshift 条件密钥。

条件键	描述
`aws:RequestTag`	要求用户在创建资源时添加标签密钥（名称）和值。有关更多信息，请参阅 IAM 用户指南中的 aws:RequestTag。
`aws:ResourceTag`	根据特定标签密钥和值限制用户对资源的访问。有关更多信息，请参阅 IAM 用户指南中的 aws:ResourceTag。

条件键	描述
aws:TagKeys	使用此键可将请求中的标签键与您在策略中指定的键进行比较。有关更多信息，请参阅 IAM 用户指南中的 aws:TagKeys。

有关标签的信息，请参阅标记概述 (p. 520)。

有关支持 redshift:RequestTag 和 redshift:ResourceTag 条件密钥的 API 操作的列表，请参阅Amazon Redshift API 权限参考 (p. 389)。

以下条件密钥可用于 Amazon Redshift GetClusterCredentials 操作。

条件键	描述
redshift:DurationSeconds	限制可为持续时间指定的秒数。
redshift:DbName	限制可指定的数据库名称。
redshift:DbUser	限制可指定的数据库用户名。

示例 1：使用 aws:ResourceTag 条件键限制访问

使用以下 IAM policy，仅允许用户针对位于 us-west-2 区域的特定 Amazon 账户修改标签名为 environment、值为 test 的 Amazon Redshift 集群。

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

示例 2：使用 aws:RequestTag 条件键限制访问

使用以下 IAM policy，仅允许用户在创建集群的命令包含名为 usage、值为 production 的标签时创建 Amazon Redshift 集群。带有 aws:TagKeys 和 ForAllValues 修饰符的条件指定只能在请求中指定 costcenter 和 usage 键。

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

将基于身份的策略（IAM policy）用于 Amazon Redshift

本主题提供了基于身份的策略的示例，在这些策略中，账户管理员可以向 IAM 身份（即：用户、组和角色）附加权限策略。

> **Important**
>
> 我们建议您首先阅读以下介绍性主题，这些主题讲解了管理 Amazon Redshift 资源访问的基本概念和选项。有关更多信息，请参阅管理 Amazon Redshift 资源的访问权限的概览 (p. 358)。

下面介绍权限策略示例。该权限允许用户创建、删除、修改和重启所有集群，但拒绝删除或修改集群标识符以 `production` 开头的任何集群的权限。

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

该策略包含两条语句：

- 第一条语句授予用户创建、删除、修改和重启集群的权限。该语句指定通配符 (*) 作为 `Resource` 的值，因此，该策略适用于归根 Amazon 账户所有的一切 Amazon Redshift 资源。

- 第二条语句拒绝删除或修改集群的权限。该语句指定包含通配符 (*) 的集群 Amazon Resource Name (ARN) 作为 `Resource` 的值。因此，该语句适用于归根 Amazon 账户所有的一切 Amazon Redshift 集群（集群标识符以 `production` 开头）。

Amazon适用于 Amazon Redshift 的 托管（预定义）策略

Amazon通过提供由创建和管理的独立 IAM policy来满足许多常用案例的要求。Amazon托管式策略可授予常用案例的必要权限，因此，您可以免去调查都需要哪些权限的工作。有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。

此外，您还可以创建自定义 IAM policy，以授予账户 Amazon Redshift API 操作和资源访问的权限。您可以将这些自定义策略附加到需要这些权限的 IAM 用户或组。

以下部分描述 Amazon Redshift 特有的 Amazon 托管式策略（可附加至您账户中的用户）：

AmazonRedshiftReadOnlyAccess

授予 Amazon 账户对所有 Amazon Redshift 资源的只读访问权限。

您可以在 IAM 控制台上找到 AmazonRedshiftReadOnlyAccess 策略。

AmazonRedshiftFullAccess

授予 Amazon 账户对所有 Amazon Redshift 资源的完全访问权限。此外，此策略还授予对所有 Amazon Redshift Serverless 资源的完全访问权限。

您可以在 IAM 控制台上找到 AmazonRedshiftFullAccess 策略。

AmazonRedshiftQueryEditor

授予账户对 Amazon Redshift 控制台查询编辑器的完全访问权限。

您可以在 IAM 控制台上找到 AmazonRedshiftQueryEditor 策略。

AmazonRedshiftDataFullAccess

授予 Amazon 账户对所有 Amazon Redshift 数据 API 操作和资源的完全访问权限。

您可以在 IAM 控制台上找到 AmazonRedshiftDataFullAccess 策略。

AmazonRedshiftQueryEditorV2FullAccess

授予账户对 Amazon Redshift 查询编辑器 v2 的完全访问权限。此策略还授予访问其它所需服务的权限。

您可以在 IAM 控制台上找到 AmazonRedshiftQueryEditorV2FullAccess 策略。

AmazonRedshiftQueryEditorV2NoSharing

授予账户使用 Amazon Redshift 查询编辑器 v2 的能力（资源不共享）。此策略还授予访问其它所需服务的权限。使用此策略的主体无法标记其资源（例如查询），因此无法与同一 Amazon Web Services 账户 中的其它主体共享这些资源。

您可以在 IAM 控制台上找到 AmazonRedshiftQueryEditorV2NoSharing 策略。

AmazonRedshiftQueryEditorV2ReadSharing

授予账户使用 Amazon Redshift 查询编辑器 v2 的能力（资源共享受限）。此策略还授予访问其它所需服务的权限。使用此策略的主体可以标记其资源（例如查询），以便与同一 Amazon Web Services 账户 中的其它主体共享这些资源。获得授权的主体可读取其与团队共享的资源，但无法更新。

您可以在 IAM 控制台上找到 AmazonRedshiftQueryEditorV2ReadSharing 策略。

AmazonRedshiftQueryEditorV2ReadWriteSharing

授予账户使用 Amazon Redshift 查询编辑器 v2 共享资源的能力。此策略还授予访问其它所需服务的权限。使用此策略的主体可以标记其资源（例如查询），以便与同一 Amazon Web Services 账户 中的其它主体共享这些资源。获得授权的主体可以读取和更新其与团队共享的资源。

您可以在 IAM 控制台上找到 AmazonRedshiftQueryEditorV2ReadWriteSharing 策略。

AmazonRedshiftServiceLinkedRolePolicy

您无法将 AmazonRedshiftServiceLinkedRolePolicy 策略附加至您的 IAM 实体。把此策略附加至服务相关的角色，该角色允许 Amazon Redshift 访问账户资源。有关更多信息，请参阅使用面向 Amazon Redshift 的服务相关角色。

AmazonRedshiftAllCommandsFullAccess

授予账户使用从 Amazon Redshift 控制台创建的 IAM 角色的能力，并将其设置为默认角色，以便集群从 Simple Storage Service（Amazon S3）运行 COPY、UNLOAD、CREATE EXTERNAL SCHEMA、CREATE EXTERNAL FUNCTION 和 CREATE MODEL 命令。该策略还授予账户为相关服务运行 SELECT 语句的权限，例如 Simple Storage Service（Amazon S3）、CloudWatch Logs、Amazon SageMaker 或 Amazon Glue。

您可以在 IAM 控制台上找到 AmazonRedshiftAllCommandsFullAccess 策略。

此外，您还可以创建自定义 IAM policy，以授予账户 Amazon Redshift API 操作和资源访问的权限。您可以将这些自定义策略附加到需要这些权限的 IAM 用户或组。

Amazon 托管式策略的 Amazon Redshift 更新

查看有关 Amazon Redshift（自从其开始跟踪更新更改以来）的 Amazon 托管式策略更新的详细信息。有关此页面更改的自动提示，请订阅 Amazon Redshift 文档历史记录页面上的 RSS 源。

更改	说明	日期
AmazonRedshiftQueryEditorV2NoSharing (p. 364) – 对现有策略的更新	Amazon Redshift 添加了用于执行 `sqlworkbench:ListQueryExecutionHistory` 和 `sqlworkbench:GetQueryExecutionHistory` 操作的权限。这授予了查看查询历史记录的权限。	2022 年 8 月 30 日
AmazonRedshiftQueryEditorV2ReadSharing (p. 364) – 对现有策略的更新	Amazon Redshift 添加了用于执行 `sqlworkbench:ListQueryExecutionHistory` 和 `sqlworkbench:GetQueryExecutionHistory` 操作的权限。这授予了查看查询历史记录的权限。	2022 年 8 月 30 日
AmazonRedshiftQueryEditorV2ReadWriteSharing (p. 365) – 对现有策略的更新	Amazon Redshift 添加了用于执行 `sqlworkbench:ListQueryExecutionHistory` 和 `sqlworkbench:GetQueryExecutionHistory`	2022 年 8 月 30 日

更改	说明	日期
	操作的权限。这授予了查看查询历史记录的权限。	
AmazonRedshiftFullAccess (p. 364) – 对现有策略的更新	Amazon Redshift Serverless 的权限已添加到现有的 AmazonRedshiftFullAccess 托管策略中。	2022 年 7 月 22 日
AmazonRedshiftDataFullAccess (p. 364) – 对现有策略的更新	Amazon Redshift 已将标签 `aws:ResourceTag/RedshiftDataFullAccess` 权限的 `redshift-serverless:GetCredentials` 默认作用域条件从 `StringEquals` 更新为 `StringLike`，以授予对使用标签键 `RedshiftDataFullAccess` 和任何标签值标记的资源的访问权限。	2022 年 7 月 11 日
AmazonRedshiftDataFullAccess (p. 364) – 对现有策略的更新	Amazon Redshift 添加了新权限，以允许 `redshift-serverless:GetCredentials` 获得对 Amazon Redshift Serverless 的临时凭证。	2022 年 7 月 8 日
AmazonRedshiftQueryEditorV2NoSharing (p. 364) – 对现有策略的更新	Amazon Redshift 添加了用于执行 `sqlworkbench:GetAccountSettings` 操作的权限。这将授予获取账户设置的权限。	2022 年 6 月 15 日
AmazonRedshiftQueryEditorV2ReadSharing (p. 364) – 对现有策略的更新	Amazon Redshift 添加了用于执行 `sqlworkbench:GetAccountSettings` 操作的权限。这将授予获取账户设置的权限。	2022 年 6 月 15 日
AmazonRedshiftQueryEditorV2ReadWriteSharing (p. 364) – 对现有策略的更新	Amazon Redshift 添加了用于执行 `sqlworkbench:GetAccountSettings` 操作的权限。这将授予获取账户设置的权限。	2022 年 6 月 15 日
AmazonRedshiftServiceLinkedRolePolicy (p. 364) – 对现有策略的更新	为了允许对新的 Amazon Redshift Serverless 端点进行公有访问，Amazon Redshift 在客户账户中分配弹性 IP 地址并将其关联到 VPC 端点的弹性网络接口。它通过由服务相关角色提供的权限来完成此操作。要启用此使用案例，分配和释放弹性 IP 地址的操作将添加到 Amazon Redshift Serverless 服务相关角色中。	2022 年 5 月 26 日

更改	说明	日期
AmazonRedshiftQueryEditorV2FullAccess (p. 364) – 对现有策略的更新	操作 `sqlworkbench:ListTaggedResources` 的权限。它专门适用于 Amazon Redshift 查询编辑器 v2 资源。此策略更新授予仅可通过查询编辑器 v2 调用 `tag:GetResources` 的权限。	2022 年 2 月 22 日
AmazonRedshiftQueryEditorV2NoSharing (p. 364) – 对现有策略的更新	操作 `sqlworkbench:ListTaggedResources` 的权限。它专门适用于 Amazon Redshift 查询编辑器 v2 资源。此策略更新授予仅可通过查询编辑器 v2 调用 `tag:GetResources` 的权限。	2022 年 2 月 22 日
AmazonRedshiftQueryEditorV2ReadSharing (p. 364) – 对现有策略的更新	操作 `sqlworkbench:ListTaggedResources` 的权限。它专门适用于 Amazon Redshift 查询编辑器 v2 资源。此策略更新授予仅可通过查询编辑器 v2 调用 `tag:GetResources` 的权限。	2022 年 2 月 22 日
AmazonRedshiftQueryEditorV2ReadWriteSharing (p. 365) – 对现有策略的更新	操作 `sqlworkbench:ListTaggedResources` 的权限。它专门适用于 Amazon Redshift 查询编辑器 v2 资源。此策略更新授予仅可通过查询编辑器 v2 调用 `tag:GetResources` 的权限。	2022 年 2 月 22 日
AmazonRedshiftQueryEditorV2ReadSharing (p. 364) – 对现有策略的更新	托管式策略增加了 `sqlworkbench:AssociateQueryWithTab` 操作的权限。增加此权限将允许客户创建编辑器选项卡，以链接到与其共享的查询。	2022 年 2 月 22 日
AmazonRedshiftServiceLinkedRolePolicy (p. 364) – 对现有策略的更新	Amazon Redshift 添加了新操作的权限，允许对 Amazon Redshift 网络和 VPC 资源进行管理。	2021 年 11 月 22 日
AmazonRedshiftAllCommandsFullAccess (p. 363) – 新策略	Amazon Redshift 添加了一项新策略，允许使用从 Amazon Redshift 控制台创建的 IAM 角色，并将其设置为默认角色，以便集群从 Simple Storage Service（Amazon S3）运行 COPY、UNLOAD、CREATE EXTERNAL SCHEMA、CREATE EXTERNAL FUNCTION 和 CREATE MODEL 和 CREATE LIBRARY 命令。	2021 年 11 月 18 日

更改	说明	日期
AmazonRedshiftServiceLinkedRolePolicy (p. 361) – 对现有策略的更新	Amazon Redshift 添加了新操作的权限，允许管理 Amazon Redshift CloudWatch 日志组和日志流，包括审计日志导出。	2021 年 11 月 15 日
AmazonRedshiftFullAccess (p. 364) – 对现有策略的更新	Amazon Redshift 添加了新权限。以允许模型可解释性、DynamoDB、Redshift Spectrum 和 Amazon RDS 联合身份验证等功能。	2021 年 10 月 7 日
AmazonRedshiftQueryEditorV2FullAccess (p. 364) – 新策略	Amazon Redshift 添加了一项新策略，允许对 Amazon Redshift 查询编辑器 v2 的wan q完全访问。	2021 年 9 月 24 日
AmazonRedshiftQueryEditorV2NoSharing (p. 364) – 新策略	Amazon Redshift 添加了一项新策略，允许在不共享资源的情况下使用 Amazon Redshift 查询编辑器 v2。	2021 年 9 月 24 日
AmazonRedshiftQueryEditorV2ReadSharing (p. 364) – 新策略	Amazon Redshift 添加了一项新策略，允许在 Amazon Redshift 查询编辑器 v2 中进行读取共享。	2021 年 9 月 24 日
AmazonRedshiftQueryEditorV2ReadWriteSharing (p. 364) – 新策略	Amazon Redshift 添加了一项新策略，允许在 Amazon Redshift 查询编辑器 v2 中进行读取和更新共享。	2021 年 9 月 24 日
AmazonRedshiftFullAccess (p. 364) – 对现有策略的更新	Amazon Redshift 添加了新的权限，以允许 `sagemaker:*Job*`。	2021 年 8 月 18 日
AmazonRedshiftDataFullAccess (p. 364) – 对现有策略的更新	Amazon Redshift 添加了新的权限，以允许 `AuthorizeDataShare`。	2021 年 8 月 12 日
AmazonRedshiftDataFullAccess (p. 364) – 对现有策略的更新	Amazon Redshift 添加了新的权限，以允许 `BatchExecuteStatement`。	2021 年 7 月 27 日
Amazon Redshift 开始跟踪更改	Amazon Redshift 开始跟踪其 Amazon 托管式策略的更改。	2021 年 7 月 27 日

使用 Redshift Spectrum 所需的权限

Amazon Redshift Spectrum 需要其他 Amazon 服务访问资源的权限。有关 Redshift Spectrum 的 IAM policy 中的权限的详细信息，请参阅 Amazon Redshift 数据库开发人员指南中的 Amazon Redshift Spectrum 的 IAM policy。

使用 Amazon Redshift 控制台所需的权限

用户若要能够使用 Amazon Redshift 控制台，则必须拥有一组最低的权限来允许用户为自己的 Amazon 账户描述 Amazon Redshift 资源。这些权限还必须允许用户描述其他相关信息（包括 Amazon EC2 安全、Amazon CloudWatch、Amazon SNS 和网络信息）。

如果创建比必需的最低权限更为严格的 IAM policy，对于附加了该 IAM policy的用户，控制台无法按预期正常运行。要确保这些用户仍可使用 Amazon Redshift 控制台，也可向用户附加 `AmazonRedshiftReadOnlyAccess` 托管式策略。其操作方法，请见Amazon适用于 Amazon Redshift 的托管（预定义）策略 (p. 364)所述。

有关授予用户访问 Amazon Redshift 控制台上的查询编辑器的权限，请参阅使用 Amazon Redshift 控制台查询编辑器所需的权限 (p. 369)。

对于只需要调用 Amazon CLI 或 Amazon Redshift API 的用户，无需为其提供最低限度的控制台权限。

使用 Amazon Redshift 控制台查询编辑器所需的权限

一个用户若要使用 Amazon Redshift 查询编辑器，该用户必须具有一组 Amazon Redshift 和 Amazon Redshift 数据 API 操作的最低权限。要使用密钥连接到数据库，您还必须具有 Secrets Manager 权限。

要授予用户对 Amazon Redshift 控制台上的查询编辑器的访问权限，请附加 `AmazonRedshiftQueryEditor` 和 `AmazonRedshiftReadOnlyAccess` Amazon 托管式策略。`AmazonRedshiftQueryEditor` 策略允许用户只检索其自己的 SQL 语句的结果。也就是说，相同 `aws:userid` 提交的语句，如 `AmazonRedshiftQueryEditor` Amazon 托管式策略的此部分所示。

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

要允许用户检索同一 IAM 角色中其他用户的 SQL 语句的结果，请创建您自己的策略，而不需要限制对当前用户的访问权限的条件。同时限制管理员更改策略的访问权限。

使用查询编辑器 v2 所需的权限

需要使用 Amazon Redshift 查询编辑器 v2 的用户必须拥有一组 Amazon Redshift、查询编辑器 v2 操作和其它操作的最低权限，以及其它 Amazon 服务的权限，诸如 Amazon Key Management Service、Amazon Secrets Manager和标记服务。

要授予用户对查询编辑器 v2 的完全访问权，请附上 `AmazonRedshiftQueryEditorV2FullAccess` Amazon 托管式策略。这些 `AmazonRedshiftQueryEditorV2FullAccess` 策略授权用户与同一团队中的其它人共享查询编辑器 v2 资源（例如查询）。有关如何控制查询编辑器 v2 资源访问的详细信息，请参阅 IAM 控制台上查询编辑器 v2 的特定托管式策略的定义。

一些 Amazon Redshift 查询编辑器 v2 Amazon 托管式策略使用 Amazon 标签在条件范围内限制对资源的访问。在查询编辑器 v2 中，共享查询的基础是附加至主体（IAM 用户或 IAM 角色）的 IAM policy 中的标记密钥和值 `"aws:ResourceTag/sqlworkbench-team": "${aws:PrincipalTag/sqlworkbench-team}"`。同样 Amazon Web Services 账户 的主体具有相同标记值（例如 `accounting-team`），在查询编辑器 v2 中处于同一个团队。您同时只能与一个团队关联。具有管理权限的用户可以在 IAM 控制台上设置团队，方法是为所有团队成员提供相同的 `sqlworkbench-team` 标记值。如果标记值 `sqlworkbench-team` 已为 IAM 用户或 IAM 角色更改，可能要经过延迟后，更改才会反映在共享资源中。如果资源（例如查

询）的标记值发生了更改，在更改生效之前可能再次出现延迟。团队成员还必须拥有 `tag:GetResources` 权限才能分享。

示例：添加 IAM 角色的 **`accounting-team`** 标签

1. 登录Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在控制台的导航窗格中，选择 Roles（角色），然后选择要编辑的角色的名称。
3. 选择 Tags（标签）选项卡，然后选择 Add（添加）标签。
4. 添加标记密钥 sqlworkbench-team 和值 `accounting-team`。
5. 选择保存更改。

   现在，当 IAM 主体（附加了此 IAM 角色）与团队共享查询时，其它具有同样 `accounting-team` 标记值的主体可以查看查询。

有关如何将标签附加至主体（包括 IAM 角色和 IAM 用户）的更多信息，请参阅《IAM 用户指南》中的标记 IAM 资源部分。

您还可以使用身份提供者（IdP）在会话级别设置团队。这允许使用同一 IAM 角色的多个用户拥有不同的团队。IAM 角色信任策略必须允许 `sts:TagSession` 操作。有关更多信息，请参阅《IAM 用户指南》中的添加会话标签所需的权限。将主标签属性添加到 IdP 提供的 SAML 断言中。

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:sqlworkbench-team">
    <AttributeValue>accounting-team</AttributeValue>
</Attribute>
```

按照身份提供者（IdP）提供的说明使用来自目录的内容填充 SAML 属性。有关身份提供者（IdP）和 Amazon Redshift 的更多信息，请参阅《IAM 用户指南》 中的使用 IAM 身份验证生成数据库用户凭证 (p. 393)和身份提供者和联合身份验证。

使用 Amazon Redshift 调度程序所需的权限

使用 Amazon Redshift 计划程序时，您应设置与 Amazon Redshift 计划程序 (**`scheduler.redshift.amazonaws.com`**) 具有信任关系的 IAM 角色，以便允许该计划程序代表您承担权限。您还可以为要计划的 Amazon Redshift API 操作将策略（权限）附加到角色。

以下示例演示 JSON 格式的策略文档，该策略用于在 Amazon Redshift 调度程序和 Amazon Redshift 之间设置信任关系。

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

有关信任实体更多信息，请参阅 IAM 用户指南中的创建向 Amazon 服务委派权限的角色。

您还必须为要计划的 Amazon Redshift 操作添加权限。

为使计划程序使用 `ResizeCluster` 操作，请为 IAM policy 添加如下权限。根据您的环境，您可能希望使策略限制更严格。

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

有关为 Amazon Redshift 调度程序创建角色的步骤，请参阅 IAM 用户指南中的为 Amazon 服务（控制台）创建角色。在 IAM 控制台中创建角色时，请选择以下选项：

- 对于 Choose the service that will use this role (选择将使用此角色的服务)：选择 Redshift。
- 对于 Select your use case (选择您的使用案例)，选择 Redshift - Scheduler (Redshift - 计划程序)。
- 为允许计划的 Amazon Redshift 操作的角色创建或附加策略。选择 Create policy (创建策略) 或修改角色以便附加策略。输入计划操作的 JSON 策略。
- 在创建角色后，编辑 IAM 角色的 Trust Relationship (信任关系) 以便包含服务 `redshift.amazonaws.com`。

您创建的 IAM 角色具有信任实体 `scheduler.redshift.amazonaws.com` 和 `redshift.amazonaws.com`。它还具有附加策略，该策略允许支持的 Amazon Redshift API 操作，例如 `"redshift:ResizeCluster"`。

使用 Amazon EventBridge 调度程序所需的权限

使用 Amazon EventBridge 调度程序时，您应设置与 EventBridge 计划程序 (**`events.amazonaws.com`**) 具有信任关系的 IAM 角色，以便允许该计划程序代表您承担权限。您还可以为要计划的 Amazon Redshift 数据 API 操作将策略（权限）附加到角色，并附加 Amazon EventBridge 操作的策略。

当您使用控制台上的 Amazon Redshift 查询编辑器创建计划查询时，您可以使用 EventBridge 调度程序。

您可以创建 IAM 角色以在 IAM 控制台上运行计划查询。在此 IAM 角色中，附加 `AmazonEventBridgeFullAccess` 和 `AmazonRedshiftDataFullAccess`。

以下示例演示 JSON 格式的策略文档，该策略用于设置与EventBridge 调度程序的信任关系。

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

有关信任实体更多信息，请参阅 IAM 用户指南中的创建向 Amazon 服务委派权限的角色。

有关为 EventBridge 调度程序创建角色的步骤，请参阅 IAM 用户指南中的为 Amazon 服务（控制台）创建角色。在 IAM 控制台中创建角色时，请选择以下选项：

- 在 Choose the service that will use this role（选择将使用此角色的服务）下，选择 CloudWatch Events。
- 对于 Select your use case（选择您的使用案例）：选择 CloudWatch Events。
- 附加以下权限策略：`AmazonEventBridgeFullAccess` 和 `AmazonRedshiftDataFullAccess`。

您创建的 IAM 角色具有信任实体 `events.amazonaws.com`。它还具有附加策略，该策略允许支持的 Amazon Redshift 数据 API 操作，例如 `"redshift-data:*"`。

在 Amazon SageMaker 中使用 Amazon Redshift 机器学习（ML）所需的权限。

接下来，您可以找到在 Amazon SageMaker 中使用 Amazon Redshift 机器学习（ML）所需权限的描述（不同使用案例）。

为了让用户在 Amazon SageMaker 中使用 Amazon Redshift ML，请创建一个拥有比默认策略更具限制性策略的 IAM 角色。您可以使用以下策略。您还可以修改此策略以满足您的需求。

以下策略显示了从 Amazon Redshift 运行 SageMaker Autopilot（具备模型可解释性）所需的权限。

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

以下策略显示了允许访问 Amazon DynamoDB、Redshift Spectrum 和 Amazon RDS 联合身份验证的完全最低权限。

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

或者，要使用 Amazon KMS 密钥用于加密，将以下权限添加到策略中。

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

要允许 Amazon Redshift 和 SageMaker 代入先前的 IAM 角色以便与其它服务交互，请将以下信任策略添加到 IAM 角色中。

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

先前的 Simple Storage Service（Amazon S3）桶 `redshift-downloads/redshift-ml/`，是存储用于其他步骤和示例的示例数据的位置。如果您不需要从 Simple Storage Service（Amazon S3）加载数据，您可以将桶删除。或者，将其替换为用于将数据加载到 Amazon Redshift 的其它 Simple Storage Service（Amazon S3）桶。

`your-account-id`、**`your-role`** 和 **`your-s3-bucket`** 值是您在 CREATE MODEL（创建模型）命令中指定的账户 ID、角色和桶。

（可选）如果您为使用 Amazon Redshift ML 指定了一个 Amazon KMS 密钥，请使用示例策略的 Amazon KMS 密钥部分。**`your-kms-key`** 值是作为 CREATE MODEL 命令一部分使用的键。

如果您为超参数优化任务指定了一个私有的虚拟私有云（VPC），请添加以下权限：

```
{
            "Effect": "Allow",
            "Action": [
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeVpcs",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups"
            ]
}
```

要使用模型解释，请确保您具备调用 SageMaker API 操作的权限。建议使用 `AmazonSageMakerFullAccess` 托管式策略。如果您要使用更具限制性的策略创建 IAM 角色，您可以使用以下策略。

```
{
          "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": "*"
          }
          ]
}
```

有关 `AmazonSageMakerFullAccess` 托管式策略的更多信息，请参阅《Amazon SageMaker 开发人员指南》中的 AmazonSageMakerFullAccess。

有关 Amazon Redshift ML 的更多信息，请参阅在 Amazon Redshift 中使用机器学习或 CREATE MODEL。

使用数据共享 API 操作所需的权限

要控制对数据共享 API 操作的访问，请使用基于 IAM 操作的策略。有关如何管理IAM policy 的信息，请参阅 IAM 用户指南中的管理 IAM policy。

当创建者集群管理员需要使用 AuthorizeDataShare 调用来授权 Amazon Web Services 账户 账户外数据共享出口的时候，更是如此。在这种情况下，您可以设置基于 IAM 操作的策略来授予此权限。使用 DeauthorizeDataShare 调用以撤消出口。

使用基于 IAM 操作的策略时，您还可以在策略中指定 IAM 资源，例如 DataShareARN。下面显示了 DataShareARN 的格式和示例。

```
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
```

您可以通过在 IAM policy 中指定数据更新名称来限制对特定数据共享的 AuthorizeDataShare 访问权限。

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/SalesShare"
      ],
      "Effect": "Deny"
    }
  ]
}
```

您还可以将 IAM policy 限制为特定创建器集群拥有的所有数据共享。若要执行此操作，请将策略中的 **datashare-name** 值替换为通配符或星号。保留集群的 namespace-guid 值。

```
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/*
```

以下 IAM policy 防止实体面向特定创建者集群拥有的数据共享调用 AuthorizeDataShare。

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

DataShareARN 会根据数据共享名称和所拥有的全局唯一的集群命名空间 ID（GUID）来限制访问。它通过将名称指定为星号来完成此操作。

GetClusterCredentials 的资源策略

要使用 JDBC 或 ODBC 利用 IAM 数据库凭证连接集群数据库，或者以编程方式调用 GetClusterCredentials 操作，您需要拥有一组最低的权限。至少，您需要具有访问 redshift:GetClusterCredentials 资源的 dbuser 操作的权限。

如果使用 JDBC 或 ODBC 连接，您可以指定 `server` 和 `port` 来代替 `cluster_id` 和 `region`，为此，您的策略必须允许能够访问 `redshift:DescribeClusters` 资源的 `cluster` 操作。

如果您使用可选参数 `Autocreate`、`DbGroups` 和 `DbName` 调用 `GetClusterCredentials` 操作，您还必须允许这些操作，并允许访问下表中列出的资源。

GetClusterCredentials 参数	操作	资源
`Autocreate`	`redshift:CreateClusterUser`	`dbuser`
`DbGroups`	`redshift:JoinGroup`	`dbgroup`
`DbName`	NA	`dbname`

有关资源的更多信息，请参阅 Amazon Redshift 资源和操作 (p. 358)。

您还可以在策略中包括以下条件：

- `redshift:DurationSeconds`
- `redshift:DbName`
- `redshift:DbUser`

有关条件的更多信息，请参阅“在策略中指定条件 (p. 361)”。

客户托管式策略示例

本节的用户策略示例介绍如何授予各 Amazon Redshift 操作的权限。当您使用 Amazon Redshift API、Amazon 开发工具包或 Amazon CLI 时，可以使用这些策略。

> Note
>
> 所有示例都使用美国西部 (俄勒冈) 区域 (`us-west-2`) 并且包含虚构的账户 ID。

示例 1：为用户授予所有 Amazon Redshift 操作和资源的完全访问权限

以下策略允许访问所有资源上的所有 Amazon Redshift 操作。

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

`Action` 元素中的 `redshift:*` 值指示 Amazon Redshift 中的所有操作。

示例 2：拒绝用户访问一组 Amazon Redshift 操作

默认情况下，所有权限都将被拒绝。不过，有时您需要明确拒绝对某个或某组操作的访问。以下策略允许访问所有 Amazon Redshift 操作，但明确拒绝对名称以 `Delete` 开头的任何 Amazon Redshift 操作的访问。该策略适用于 `us-west-2` 中的所有 Amazon Redshift 资源。

```
{
  "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:*"
   }
  ]
}
```

示例 3：允许用户管理集群

以下策略允许用户创建、删除、修改和重启所有集群，但拒绝删除名称以 `protected` 开头的任何集群的权限。

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

示例 4：允许用户授予和撤销快照访问权限

以下策略允许用户（如用户 A）执行以下操作：

- 授予对从名为 `shared` 的集群中创建的任何快照的访问权限。
- 撤消对从快照名称以 `shared` 开头的 `revokable` 集群中创建的任何快照的访问权限。

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

如果用户 A 允许用户 B 访问快照，则用户 B 必须拥有以下某项策略才能从该快照还原集群。以下策略允许用户 B 描述集群、从快照还原集群以及创建集群。这些集群的名称必须以 `from-other-account` 开头。

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

示例 5：允许用户复制集群快照以及从快照中还原集群

以下策略允许用户复制从名为 `big-cluster-1` 的集群中创建的任何快照，以及还原名称以 `snapshot-for-restore` 开头的任何快照。

```
{
```

```
  "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"
    }
  ]
}
```

示例 6：允许用户访问 Amazon Redshift 以及相关 Amazon 服务的常见操作和资源

以下示例策略允许访问 Amazon Redshift、Amazon Simple Notification Service (Amazon SNS) 和 Amazon CloudWatch 的所有操作和资源。它还允许对账户下的所有相关 Amazon EC2 资源执行指定的操作。

> **Note**
>
> 此示例策略中指定的 Amazon EC2 操作不支持资源级权限。

```
{
  "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": [
        "*"
      ]
    }
  ]
}
```

示例 7：允许用户使用 Amazon Redshift 控制台标记资源

以下示例策略允许用户使用 Amazon Resource Groups 通过 Amazon Redshift 控制台对资源进行标记。此策略可附加到调用新的或原始 Amazon Redshift 控制台的用户角色。有关标记的更多信息，请参阅在 Amazon Redshift 中为资源添加标签 (p. 520)。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Tagging permissions",
            "Effect": "Allow",
            "Action": [
                "redshift:DeleteTags",
                "redshift:CreateTags",
                "redshift:DescribeTags",
                "tag:UntagResources",
                "tag:TagResources"
            ],
            "Resource": "*"
        }
    ]
}
```

使用 GetClusterCredentials 的示例策略

以下策略使用这些示例参数值：

- 区域：`us-west-2`
- Amazon*, 账户`123456789012`
- 集群名称: `examplecluster`

以下策略启用 `GetCredentials`、`CreateClusterUser` 和 `JoinGroup` 操作。仅在 Amazon 用户 ID 与 `"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"` 匹配时，该策略才使用条件密

钥以允许 GetClusterCredentials 和 CreateClusterUser 操作。IAM 访问权限仅对 "testdb" 数据库是必需的。该策略还允许用户参与名为 "common_group" 的组。

```
{
"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"
      ]
    }
  ]
}


  }
}
```

Amazon Redshift 的原生身份提供者 (IdP) 联合身份验证

借助原生身份提供者联合身份验证，管理 Amazon Redshift 的身份和权限变得更加容易，因为它利用现有身份提供者来简化身份验证和管理权限。它可以通过使身份提供者向 Redshift 共享身份元数据来实现这一目标。对于此功能的第一次迭代，受支持的身份提供者是 Microsoft Azure Active Directory (Azure AD)。

要将 Amazon Redshift 配置为对来自第三方身份提供者的身份进行身份验证，您可以向 Amazon Redshift 注册身份提供者。这样做可以让 Redshift 对身份提供者定义的用户和角色进行身份验证。这样，您可以避免必须同时在第三方身份提供者和 Amazon Redshift 中执行精细的身份管理，因为身份信息是共享的。

在 Amazon Redshift 上设置身份提供者

本节介绍配置身份提供者和 Amazon Redshift 以便为原生身份提供者联合身份验证建立通信的步骤。您需要身份提供者的有效账户。在配置 Amazon Redshift 之前，您可以向身份提供者注册 Redshift 作为应用程序，并授予管理员同意。

在 Amazon Redshift 中，完成以下步骤：

1. 运行 SQL 语句来注册身份提供者，包括 Azure 应用程序元数据的说明。要在 Amazon Redshift 中创建身份提供者，请在替换参数值 issuer、client_id、client_secret 和 audience 后运行以下命令。这些参数特定于 Microsoft Azure AD。将身份提供者名称替换为您选择的名称，然后用唯一名称替换命名空间，以包含来自身份提供者目录中的用户和角色。

```
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"]
}'
```

   类型 `azure` 表示该提供商特意加强了与 Microsoft Azure AD 的通信。这是目前唯一受支持的第三方身份提供者。

   - issuer - 收到令牌时要信任的发布者 ID。tenant_id 的唯一标识符附加到发布者之后。
   - client_id - 向身份提供者注册的应用程序的唯一公有标识符。这可以称为应用程序 ID。
   - client_secret - 只有身份提供者和注册的应用程序才知道的秘密标识符或密码。
   - audience - 在 Azure 中分配给应用程序的应用程序 ID。

   您可以在创建身份提供者时设置参数来指定证书、私有密钥和私有密钥密码，而不使用共享客户端密钥。

```
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"}';
```

   私有密钥密码 client_pk_password 为可选项。

2. 可选：在 Amazon Redshift 中运行 SQL 命令以预先创建用户和角色。这有助于提前授予权限。Amazon Redshift 中的角色名称如下所示：<Namespace>:<GroupName on Azure AD>。例如，当您在 Microsoft Azure AD 中创建一个名为 `rsgroup` 的组和一个名为 `aad` 的命名空间时，角色名称为 `aad:rsgroup`。用户名和组成员资格映射到 Amazon Redshift 中的用户和角色（位于身份提供者命名空间中）。

   角色和用户的映射包括验证他们的 `external_id` 值，以确保它是最新的。外部 ID 将映射到身份提供程序中组或用户的标识符。例如，角色的外部 ID 将映射到相应的 Azure AD 组 ID。同样，每个用户的外部 ID 都将映射到他们在身份提供程序中的 ID。

```
create role "aad:rsgroup";
```

3. 根据您的要求向角色授予相关权限。例如：

```
GRANT SELECT on all tables in schema public to role "aad:rsgroup";
```

4. 您还可向特定用户授予权限。

```
GRANT SELECT on table foo to aad:alice@example.com
```

命名空间的解释

命名空间将用户或角色映射到特定身份提供者。例如，IAM 用户的前缀为 `iam:`。这样做是为了避免用户名冲突并支持多个身份存储。如果用户 alice@example.com 来自向 aad 命名空间注册的身份源，则当此用户登录时，会在 Redshift 中创建用户 `aad:alice@example.com`（如果此用户尚未存在）。请注意，用户和角色命名空间与 Amazon Redshift 集群命名空间具有不同的功能，后者是与集群关联的唯一标识符。

如何使用原生身份提供者 (IdP) 联合身份验证进行登录

要完成身份提供者和 Amazon Redshift 之间的初步设置，您需要执行以下几个步骤：首先，向身份提供者注册 Amazon Redshift 作为第三方应用程序，同时请求必要的 API 权限。然后在身份提供者中创建用户和组。最后，您可以使用 SQL 语句向 Amazon Redshift 注册身份提供者，这些语句设置身份提供者特有的身份验证参数。在向 Redshift 注册身份提供者的过程中，您分配一个命名空间以确保正确地对用户和角色进行分组。

在向 Amazon Redshift 注册身份提供者后，Redshift 和身份提供者之间就建立了通信。然后，客户端可以作为身份提供者实体传递令牌并向 Redshift 进行身份验证。Amazon Redshift 使用 IdP 组成员资格信息来映射到 Redshift 角色。如果用户之前不存在于 Redshift 中，则会创建该用户。创建映射到身份提供者组的角色（如果它们不存在）。Amazon Redshift 管理员授予对角色的权限，而用户可以运行查询和执行其他数据库任务。

以下步骤概述当用户登录时原生身份提供者联合身份验证的工作方式：

1. 当用户从客户端使用原生 IdP 选项登录时，身份提供者令牌将从客户端发送到驱动程序。
2. 对用户进行身份验证。如果 Amazon Redshift 中不存在此用户，则将创建一个新用户。Redshift 将用户的身份提供者组映射到 Redshift 角色。
3. 权限是根据用户的 Redshift 角色分配的。管理员将这些权限授予用户和角色。
4. 用户可以查询 Redshift。

使用桌面客户端工具连接到 Amazon Redshift

有关如何使用原生身份提供者联合身份验证通过 Power BI 连接到 Amazon Redshift 的说明，请参阅博客文章将 Amazon Redshift 原生 IdP 联合身份验证与 Microsoft Azure Active Directory (AD) 和 Power BI 集成。它介绍了使用 Azure AD 实施 Amazon Redshift 原生 IdP 设置的按步骤过程。它详细介绍了为 Power BI 桌面或 Power BI 服务设置客户端连接的步骤。这些步骤包括应用程序注册、配置权限和配置凭证。

要了解如何使用 Power BI 桌面和 JDBC 客户端 SQL WorkBench/J 将 Amazon Redshift 原生 IdP 联合身份验证与 Azure AD 集成，请观看以下视频：

有关如何使用原生身份提供者联合身份验证通过 SQL 客户端（特别是 DBEaver 或 SQL WorkBench/J）连接到 Amazon Redshift 的说明，请参阅博客文章使用 SQL 客户端将 Amazon Redshift 原生 IdP 联合身份验证与 Microsoft Azure AD 集成。

Amazon Redshift API 权限参考

在设置 访问控制 (p. 358) 时，您编写可附加到 IAM 身份的权限策略（基于身份的策略）。有关详细参考信息，请参阅《服务授权参考》中的以下主题：

- Amazon Redshift 的操作、资源和条件键。
- Amazon Redshift Serverless 的操作、资源和条件键。
- Amazon Redshift Data API 的操作、资源和条件键。
- Amazon SQL 工作台的操作、资源和条件键，它们列出了 Amazon Redshift 查询编辑器 v2 的操作。

此参考包含有关可在 IAM policy 中使用哪些 API 操作的信息。它还包括您可以授予权限的 Amazon 资源以及您可以针对细粒度访问控制包含的条件键。有关条件的更多信息，请参阅“使用 IAM policy 条件进行精细访问控制 (p. 361)”。

您需要在策略的 `Action` 字段中指定操作、在策略的 `Resource` 字段中指定资源值、在策略的 `Condition` 字段中指定条件。要为 Amazon Redshift 指定操作，请在 API 操作名称之前使用 `redshift:` 前缀（例如 `redshift:CreateCluster`）。

对 Amazon Redshift 使用服务相关角色

Amazon Redshift 使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特类型的 IAM 角色，它与 Amazon Redshift 直接相关。服务相关角色由 Amazon Redshift 预定义，具有服务代表您的 Amazon Redshift 集群调用 Amazon 服务所需的所有权限。

服务相关角色可让您更轻松地设置 Amazon Redshift，因为您不必手动添加必要权限。该角色与 Amazon Redshift 使用案例相关联并且具有预定义的权限。只有 Amazon Redshift 可以代入该角色，并且只有服务相关角色可以使用预定义的权限策略。Amazon Redshift 会在您首次创建集群时在您的账户中创建服务相关角色。只有删除您账户中的所有 Amazon Redshift 集群之后，您才可以删除服务相关角色。这将保护您的 Amazon Redshift 资源，因为您不会无意中删除访问资源所需的权限。

Amazon Redshift 支持在该服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 Amazon 区域和终端节点。

有关支持服务相关角色的其它服务的信息，请参阅与 IAM 配合使用的 Amazon 服务，并查找 Service-Linked Role（服务相关角色）列中为 Yes（是）的服务。选择是和链接，查看该服务的服务相关角色文档。

Amazon Redshift 的服务相关角色权限

Amazon Redshift 使用名为 AWSServiceRoleForRedshift 的服务相关角色 – 允许 Amazon Redshift 代表您调用 Amazon 服务。此服务相关角色附加至以下托管式策略上：`AmazonRedshiftServiceLinkedRolePolicy`。有关此策略的更新，请参阅适用于 Amazon Redshift 的 Amazon 托管式策略（预定义）。

AWSServiceRoleForRedshift 服务相关角色仅信任 **`redshift.amazonaws.com`** 来代入该角色。

AWSServiceRoleForRedshift 服务相关角色权限策略允许 Amazon Redshift 对所有相关资源完成以下操作：

- `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

对网络和 VPC 资源的权限

以下权限允许在 Amazon EC2 上执行操作，以创建和管理网络及虚拟私有云资源。它们特别与 RedshiftMigrateToVpc 资源标签有关联。这将权限范围限制为从特定 Amazon EC2 Classic 到 Amazon EC2 VPC 迁移任务。有关更多信息，请参阅控制对使用标签的 Amazon 资源进行访问。

- ec2:AuthorizeSecurityGroupEgress
- ec2:AuthorizeSecurityGroupIngress
- ec2:UpdateSecurityGroupRuleDescriptionsEgress
- ec2:ReplaceRouteTableAssociation
- ec2:CreateRouteTable
- ec2:AttachInternetGateway
- ec2:UpdateSecurityGroupRuleDescriptionsIngress
- ec2:AssociateRouteTable
- ec2:RevokeSecurityGroupIngress
- ec2:CreateRoute
- ec2:CreateSecurityGroup
- ec2:RevokeSecurityGroupEgress
- ec2:ModifyVpcAttribute
- ec2:CreateSubnet
- ec2:CreateInternetGateway
- ec2:CreateVpc

有关 Amazon EC2 操作和资源的更多信息，请参阅 Amazon EC2 的操作、资源和条件键。

审计日志记录的操作

列出的带 logs 前缀的操作与审计日志记录和相关功能有关。具体来说是创建和管理日志组和日志流的操作。

- logs:CreateLogGroup
- logs:PutRetentionPolicy
- logs:CreateLogStream
- logs:PutLogEvents
- logs:DescribeLogStreams

- `logs:GetLogEvents`

以下 JSON 向 Amazon Redshift 显示了用于审计日志记录的操作和资源范围。

```
[
    {
        "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:*"
        ]
    }
]
```

有关服务相关角色及它们在 Amazon 中的作用的更多信息，请参阅使用服务相关角色。有关 Amazon Redshift 的特定操作和其它 IAM 资源的更多信息，请参阅 Amazon Redshift 的操作、资源和条件键。

要允许 IAM 实体创建 AWSServiceRoleForRedshift 服务相关角色

在中国（北京）区域中，将以下策略语句添加到该 IAM 实体的权限中：

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

在中国（北京）区域中，将以下策略语句添加到该 IAM 实体的权限中：

```
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws-cn:iam::<AWS-account-ID>:role/aws-service-role/
redshift.amazonaws.com/AWSServiceRoleForRedshift",
    "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}
```

要允许 IAM 实体删除 AWSServiceRoleForRedshift 服务相关角色

向该 IAM 实体的权限中添加以下策略声明：

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

在中国（北京）区域中，将以下策略语句添加到该 IAM 实体的权限中：

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws-cn:iam::<AWS-account-ID>:role/aws-service-role/
redshift.amazonaws.com/AWSServiceRoleForRedshift",
    "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}
```

或者，您可以使用 Amazon 托管式策略提供对 Amazon Redshift 的完全访问权限。

为 Amazon Redshift 创建服务相关角色

您无需手动创建 AWSServiceRoleForRedshift 服务相关角色。Amazon Redshift 将为您创建服务相关角色。如果已从您的账户中删除 AWSServiceRoleForRedshift 服务相关角色，Amazon Redshift 将在您启动新 Amazon Redshift 集群时创建该角色。

> Important
>
> 如果您在 2017 年 9 月 18 日（从此时开始支持服务相关角色）之前已使用 Amazon Redshift 服务，则 Amazon Redshift 已在您的账户中创建 AWSServiceRoleForRedshift 角色。要了解更多信息，请参阅我的 IAM 账户中出现新角色。在中国（北京）区域，如果您在 2017 年 11 月 17 日之前就已使用 Amazon Redshift 服务，则 Amazon Redshift 已在您的账户中创建 AWSServiceRoleForRedshift 角色。

为 Amazon Redshift 编辑服务相关角色

Amazon Redshift 不允许您编辑 AWSServiceRoleForRedshift 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 控制台、Amazon Command Line Interface (Amazon CLI) 或 IAM API 编辑角色描述。有关更多信息，请参阅 IAM 用户指南中的修改角色。

删除 Amazon Redshift 的服务相关角色

如果您不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。

在删除账户的服务相关角色之前，您需要关闭并删除该账户中的所有集群。有关更多信息，请参阅 关闭和删除集群 (p. 74)。

您可以使用 IAM 控制台、Amazon CLI 或 IAM API 删除服务相关角色。有关更多信息，请参阅 IAM 用户指南中的删除服务相关角色。

使用 IAM 身份验证生成数据库用户凭证

您可以根据通过 Amazon Identity and Access Management (IAM) 权限策略授予的权限生成临时数据库凭证，以管理用户的 Amazon Redshift 数据库访问权限。

通常，Amazon Redshift 数据库用户提供数据库用户名和密码以登录到数据库。不过，您不必在 Amazon Redshift 数据库中维护用户名和密码。作为替代方法，您可以将系统配置为允许用户创建用户凭证，并根据其 IAM 凭证登录到数据库。

有关更多信息，请参阅 IAM 用户指南中的身份提供者和联合。

主题

- 概览 (p. 393)
- 创建临时 IAM 用户凭证 (p. 393)
- 用于提供 IAM 凭证的选项 (p. 401)

概览

Amazon Redshift 提供 GetClusterCredentials API 操作以生成临时数据库用户凭证。您可使用 Amazon Redshift JDBC 或 ODBC 驱动程序来配置您的 SQL 客户端，这些驱动程序可管理调用 `GetClusterCredentials` 操作的过程。它们通过检索数据库用户凭证并在您的 SQL 客户端和您的 Amazon Redshift 数据库之间建立连接来完成此操作。您也可以使用数据库应用程序以编程方式调用 `GetClusterCredentials` 操作，检索数据库用户凭证并连接到数据库。

如果您已在 Amazon 外部管理用户身份，您可以使用与安全断言标记语言 (SAML) 2.0 兼容的身份提供者 (IdP) 管理对 Amazon Redshift 资源的访问。配置您的 IdP 以允许联合身份用户访问 IAM 角色。通过使用该 IAM 角色，您可以生成临时数据库凭证并登录到 Amazon Redshift 数据库。

SQL 客户端需要具有权限才能为您调用 `GetClusterCredentials` 操作。您将通过创建 IAM 角色并附加 IAM 权限策略（该策略授权或限制对 `GetClusterCredentials` 操作和相关操作的访问）来管理这些权限。

该策略还授权或限制对特定资源 (例如，Amazon Redshift 集群、数据库、数据库用户名和用户组名称) 的访问。

> **Note**
>
> 我们建议使用 Amazon Redshift JDBC 或 ODBC 驱动程序来管理调用 `GetClusterCredentials` 操作并登录数据库的过程。为简单起见，我们在整个主题中假定您将 SQL 客户端与 JDBC 或 ODBC 驱动程序结合使用。
> 有关使用 `GetClusterCredentials` 操作或并行 `get-cluster-credentials` CLI 命令的具体详细信息和示例，请参阅 GetClusterCredentials 和 get-cluster-credentials。

为了集中管理身份验证和授权，Amazon Redshift 支持使用 IAM 进行数据库身份验证，从而通过企业联合进行用户身份验证。在使用这种方法时，您可以使用 Amazon Directory Service、企业用户目录或 Web 身份提供者中的现有身份，而不是创建 IAM 用户。这些用户被称为联合身份用户。在通过 IdP 请求访问权限时，Amazon 将为联合身份用户分配角色。

要为组织中的用户或客户端应用程序提供联合访问权限以调用 Amazon Redshift API 操作，您还可以使用具有 SAML 2.0 支持的 JDBC 或 ODBC 驱动程序请求从组织 IdP 中进行身份验证。在这种情况下，组织的用户没有 Amazon Redshift 的直接访问权限。

创建临时 IAM 用户凭证

在本节中，您可以了解如何配置系统以生成基于 IAM 的临时数据库用户凭证，并使用新凭证登录到数据库。

概括来说，流程如下所示：

1. 步骤 1：创建用于 IAM 单点登录访问的 IAM 角色 (p. 394)

   （可选）您可以将 IAM 身份验证和第三方身份提供者 (IdP) 进行集成，对访问 Amazon Redshift 数据库的用户进行身份验证。
2. 步骤 2：为 IdP 配置 SAML 断言 (p. 394)

   (可选) 要使用 IdP 进行 IAM 身份验证，您需要在 IdP 应用程序中定义一个声明规则，将组织中的用户或组映射到 IAM 角色。或者，您可以包含属性元素以设置 `GetClusterCredentials` 参数。
3. 步骤 3：创建有权调用 GetClusterCredentials 的 IAM 角色或用户 (p. 395)

   您的 SQL 客户端应用程序在调用 `GetClusterCredentials` 操作时代入 IAM 角色。如果您创建了用于身份提供者访问的 IAM 角色，则可向该角色添加必要权限。
4. 步骤 4：创建数据库用户和数据库组 (p. 397)

   （可选）默认情况下，`GetClusterCredentials` 返回凭证；如果用户名不存在，则会创建一个新用户。您也可以选择指定用户在登录时加入的用户组。默认情况下，数据库用户加入 PUBLIC 组。
5. 步骤 5：配置 JDBC 或 ODBC 连接以使用 IAM 凭证 (p. 397)

   要连接到您的 Amazon Redshift 数据库，可将 SQL 客户端配置为使用 Amazon Redshift JDBC 或 ODBC 驱动程序。

步骤 1：创建用于 IAM 单点登录访问的 IAM 角色

如果您未使用身份提供者进行单点登录访问，则可跳过此步骤。

如果您已在 Amazon 外部管理用户身份，则可将 IAM 身份验证和第三方 SAML-2.0 身份提供者 (IdP) 集成，对访问 Amazon Redshift 数据库的用户进行身份验证。

有关更多信息，请参阅 IAM 用户指南中的身份提供者和联合。

在使用 Amazon Redshift IdP 身份验证之前，请先创建一个 Amazon SAML 身份提供者。您可以在 IAM 控制台中创建一个 IdP，以向 Amazon 通知该 IdP 及其配置。这样将在您的 Amazon 账户和 IdP 之间建立信任。有关创建角色的步骤，请参阅 IAM 用户指南中的创建用于 SAML 2.0 联合的角色（控制台）。

步骤 2：为 IdP 配置 SAML 断言

在创建 IAM 角色后，您可以在 IdP 应用程序中定义一个声明规则，以将组织中的用户或组映射到 IAM 角色。有关更多信息，请参阅 IAM 用户指南中的为身份验证响应配置 SAML 断言。

如果选择使用可选的 `GetClusterCredentials` 参数 `DbUser`、`AutoCreate` 和 `DbGroups`，您有两个选择。您可以使用 JDBC 或 ODBC 连接设置这些参数的值，也可以将 SAML 属性元素添加到 IdP 以设置这些值。有关 `DbUser`、`AutoCreate` 和 `DbGroups` 参数的更多信息，请参阅步骤 5：配置 JDBC 或 ODBC 连接以使用 IAM 凭证 (p. 397)。

> **Note**
>
> 如果您使用 IAM 策略变量 `${redshift:DbUser}`（如GetClusterCredentials 的资源策略 (p. 380)中所述），则 `DbUser` 的值将被替换为由 API 操作的请求上下文检索的值。Amazon Redshift 驱动程序使用由连接 URL 提供的 `DbUser` 变量的值，而不是作为 SAML 属性提供的值。为了帮助保护该配置，我们建议您在 IAM 策略中使用一个条件以通过 `DbUser` 验证 `RoleSessionName` 值。您可以在 使用 GetClusterCredentials 的示例策略 (p. 385) 中找到如何使用 IAM 策略设置条件。

要配置 IdP 以设置 `DbUser`、`AutoCreate` 和 `DbGroups` 参数，请包含以下 `Attribute` 元素：

- `Attribute` 属性设置为“https://redshift.amazon.com/SAML/Attributes/DbUser”的 `Name` 元素

  将 `AttributeValue` 元素设置为要连接到 Amazon Redshift 数据库的用户的名称。

AttributeValue 元素中的值必须为小写形式，以字母开头，仅包含字母数字字符、下划线 (_)、加号 (+)、圆点 (.)、@ 符号或连字符 (-)，并且应少于 128 个字符。通常，用户名为用户 ID (例如，bobsmith) 或电子邮件地址 (例如，bobsmith@example.com)。此值不能包含空格 (例如，像 Bob Smith 这样的用户显示名称)。

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbUser">
    <AttributeValue>user-name</AttributeValue>
</Attribute>
```

- Name 属性设置为“https://redshift.amazon.com/SAML/Attributes/AutoCreate”的 Attribute 元素

  可以将 AttributeValue 元素设置为 true 以创建新的数据库用户（如果不存在）。将 AttributeValue 设置为 false 可指定数据库用户必须存在于 Amazon Redshift 数据库中。

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/AutoCreate">
    <AttributeValue>true</AttributeValue>
</Attribute>
```

- Attribute 属性设置为“https://redshift.amazon.com/SAML/Attributes/DbGroups”的 Name 元素

  该元素包含一个或多个 AttributeValue 元素。将每个 AttributeValue 元素设置为一个数据库组名称，DbUser 将在连接到 Amazon Redshift 数据库的会话期间加入该组。

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbGroups">
    <AttributeValue>group1</AttributeValue>
    <AttributeValue>group2</AttributeValue>
    <AttributeValue>group3</AttributeValue>
</Attribute>
```

步骤 3：创建有权调用 GetClusterCredentials 的 IAM 角色或用户

您的 SQL 客户端需要授权才能代表您调用 GetClusterCredentials 操作。要提供授权，可创建 IAM 用户或角色并附加授予必要权限的策略。

创建有权调用 GetClusterCredentials 的 IAM 角色

1. 利用 IAM 服务，可创建 IAM 用户或角色。您也可以使用现有用户或角色。例如，如果您创建了一个用于身份提供者访问的 IAM 角色，则可向该角色附加必要的 IAM 策略。
2. 附加有权调用 redshift:GetClusterCredentials 操作的权限策略。根据指定的可选参数，您还可在策略中允许或限制其他操作和资源：

   - 要允许您的 SQL 客户端检索 Redshift 集群资源的集群 ID、Amazon 区域和端口，可包含调用 redshift:DescribeClusters 操作的权限。
   - 如果您使用 AutoCreate 选项，请包含对 redshift:CreateClusterUser 资源调用 dbuser 的权限。以下 Amazon Resource Name (ARN) 指定 Amazon Redshift dbuser。将 *region*、*account-id* 和 *cluster-name* 替换为您的 Amazon 区域、账户和集群的相应值。对于 *dbuser-name*，指定用于登录到集群数据库的用户名。

     ```
     arn:aws:redshift:region:account-id:dbuser:cluster-name/dbuser-name
     ```

   - （可选）添加一个 ARN，以使用以下格式指定 Amazon Redshift dbname 资源。将 *region*、*account-id* 和 *cluster-name* 替换为您的 Amazon 区域、账户和集群的相应值。对于 *database-name*，指定用户将登录到的数据库的名称。

     ```
     arn:aws:redshift:region:account-id:dbname:cluster-name/database-name
     ```

- 如果您使用 DbGroups 选项，请使用以下格式包含对 Amazon Redshift dbgroup 资源调用 redshift:JoinGroup 操作的权限。将 *region*、*account-id* 和 *cluster-name* 替换为您的 Amazon 区域、账户和集群的相应值。对于 *dbgroup-name*，请指定用户在登录时加入的用户组的名称。

```
arn:aws:redshift:region:account-id:dbgroup:cluster-name/dbgroup-name
```

有关更多信息以及示例，请参阅 GetClusterCredentials 的资源策略 (p. 380)。

以下示例显示允许 IAM 角色调用 GetClusterCredentials 操作的策略。该策略指定，对于名为 examplecluster 的集群上的名为 temp_creds_user 的数据库用户，Amazon Redshift dbuser 资源为其授予角色访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
temp_creds_user"
  }
}
```

您可使用通配符 (*) 替换完整或部分集群名称、用户名和数据库组名称。以下示例允许指定账户中的任何集群上所有以 temp_ 开头的用户名调用。

Important

以下示例中的语句指定通配符 (*) 作为资源的值，以便策略允许以指定字符开头的任何资源。在 IAM 策略使用通配符可能过于宽松。作为最佳实践，我们建议对您的业务应用程序使用最严格的可行策略。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:*/temp_*"
  }
}
```

以下示例显示一个允许 IAM 角色调用 GetClusterCredentials 操作的策略，并提供了自动创建新用户和指定用户在登录时加入的组的选项。"Resource": "*" 子句向角色授予对任何资源 (包括集群、数据库用户或用户组) 的访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
              "redshift:GetClusterCredentials",
              "redshift:CreateClusterUser",
  "redshift:JoinGroup"
             ],
    "Resource": "*"
  }
}
```

有关更多信息，请参阅 Amazon Redshift ARN 语法。

步骤 4：创建数据库用户和数据库组

（可选）您可以创建一个用于登录到集群数据库的数据库用户。如果您为现有用户创建临时用户凭证，则可禁用此用户的密码以强制用户使用临时密码进行登录。（可选）您可以使用 `GetClusterCredentials` 选项自动创建新的数据库用户。

您可以创建希望 IAM 数据库用户在登录时加入的数据库用户组并提供相应的权限。在调用 `GetClusterCredentials` 操作时，您可以指定新用户在登录时加入的用户组名称列表。这些组成员资格仅对特定请求生成的凭证所创建的会话有效。

创建数据库用户和数据库组

1. 登录到 Amazon Redshift 数据库，并使用 CREATE USER 创建数据库用户或使用 ALTER USER 修改现有用户。
2. (可选) 指定 PASSWORD DISABLE 选项可阻止用户使用密码。在禁用用户的密码后，用户只能使用临时 IAM 用户凭证进行登录。如果未禁用密码，用户可使用密码或临时 IAM 用户凭证进行登录。您不能禁用超级用户的密码。

   以下示例创建一个已禁用密码的用户。

   ```
   create user temp_creds_user password disable;
   ```

   以下示例禁用现有用户的密码。

   ```
   alter user temp_creds_user password disable;
   ```
3. 使用 CREATE GROUP 创建数据库用户组。
4. 使用 GRANT 命令为组定义访问权限。

步骤 5：配置 JDBC 或 ODBC 连接以使用 IAM 凭证

您可以使用 Amazon Redshift JDBC 或 ODBC 驱动程序配置 SQL 客户端。此驱动程序管理创建数据库用户凭证以及在 SQL 客户端和 Amazon Redshift 数据库之间建立连接的过程。

如果您使用身份提供者进行身份验证，请指定凭证提供商插件名称。Amazon Redshift JDBC 和 ODBC 驱动程序包括以下基于 SAML 的身份提供者的插件：

- Active Directory 联合身份验证服务 (AD FS)
- PingOne
- Okta
- Microsoft Azure AD

  有关将 Microsoft Azure AD 设置为身份提供者的步骤，请参阅在 Microsoft Azure AD 中设置 JDBC 或 ODBC 单点登录身份验证 (p. 407)。

配置 JDBC 连接以使用 IAM 凭证

1. 从 为 Amazon Redshift 配置 JDBC 驱动程序版本 2.1 连接 (p. 136) 页面下载最新的 Amazon Redshift JDBC 驱动程序。
2. 使用下列格式之一创建包含 IAM 凭证选项的 JDBC URL。要使用 IAM 身份验证，请将 `iam:` 添加到 Amazon Redshift JDBC URL 中的 `jdbc:redshift:` 后面，如以下示例中所示。

   ```
   jdbc:redshift:iam://
   ```

添加 cluster-name、region 和 account-id。JDBC 驱动程序使用您的 IAM 账户信息和集群名称来检索集群 ID和 Amazon 区域。为此，您的 IAM 用户或角色必须有权针对指定集群调用 redshift:DescribeClusters 操作。如果您的 IAM 用户或角色无权调用 redshift:DescribeClusters 操作，请包含集群 ID、Amazon 区域和端口，如以下示例中所示。端口号是可选的。默认端口为 5439。

```
jdbc:redshift:iam://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/
dev
```

3. 添加 JDBC 选项可提供 IAM 凭证。使用不同的 JDBC 选项组合可提供 IAM 凭证。有关详细信息，请参阅用于创建数据库用户凭证的 JDBC 和 ODBC 选项 (p. 423)。

   以下 URL 为 IAM 用户指定 AccessKeyID 和 SecretAccessKey。

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
AccessKeyID=AKIAIOSFODNN7EXAMPLE&SecretAccessKey=wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY
```

   以下示例指定包含 IAM 凭证的命名配置文件。

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?Profile=user2
```

4. 添加 JDBC 驱动程序用来调用 GetClusterCredentials API 操作的 JDBC 选项。如果您以编程方式调用 GetClusterCredentials API 操作，请不要包括这些选项。

   以下示例包括 JDBC GetClusterCredentials 选项。

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
plugin_name=com.amazon.redshift.plugin.AzureCredentialsProvider&UID=user&PWD=password&idp_tenant=my
```

配置 ODBC 连接以使用 IAM 凭证

在以下过程中，您只能找到用于配置 IAM 身份验证的步骤。有关使用标准身份验证 (采用数据库用户名和密码) 的步骤，请参阅配置 ODBC 连接 (p. 207)。

1. 为您的操作系统安装和配置最新的 Amazon Redshift OBDC 驱动程序。有关更多信息，请参阅配置 ODBC 连接 (p. 207)页面。

   Important

   Amazon Redshift ODBC 驱动程序必须为版本 1.3.6.1000 或更高版本。

2. 根据您的操作系统选择配置连接设置需要遵循的步骤。

   有关更多信息，请参阅以下章节之一：

   - 在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 208)
   - 使用 ODBC 驱动程序管理器在 Linux 和 macOS X 操作系统上配置驱动程序 (p. 212)

3. 在 Microsoft Windows 操作系统上，访问 Amazon Redshift ODBC Driver DSN Setup（Amazon Redshift ODBC 驱动程序 DSN 设置）窗口。

   a. 在 Connection Settings 下，输入以下信息：

      - Data Source Name
      - Server (可选)
      - Port (可选)

- 数据库。

如果您的 IAM 用户或角色有权调用 `redshift:DescribeClusters` 操作，仅需要 Data Source Name（数据源名称）和 Database（数据库）。Amazon Redshift 通过调用 `DescribeCluster` 操作使用 ClusterId 和 Region（区域）来获取服务器和端口。

如果您的 IAM 用户或角色无权调用 `redshift:DescribeClusters` 操作，请指定 Server (服务器) 和 Port (端口)。默认端口为 5439。

b. 在 Authentication (身份验证) 下，为 Auth Type (身份验证类型) 选择一个值。

对于每种身份验证类型，请输入如下列出的值：

Amazon 配置文件

输入以下信息：

- ClusterID
- 区域
- 配置文件名称

  输入 Amazon config 文件中包含 ODBC 连接选项值的配置文件的名称。有关更多信息，请参阅使用配置文件 (p. 402)。

（可选）提供 ODBC 驱动程序用于调用 `GetClusterCredentials` API 操作的选项的详细信息：

- DbUser
- User AutoCreate
- DbGroups

  有关更多信息，请参阅用于创建数据库用户凭证的 JDBC 和 ODBC 选项 (p. 423)。

IAM 凭证

输入以下信息：

- ClusterID
- 区域
- AccessKeyID 和 SecretAccessKey

  为 IAM 数据库身份验证配置的 IAM 角色或 IAM 用户的访问密钥 ID 和秘密访问密钥。
- SessionToken

  对于具有临时凭证的 IAM 角色，SessionToken 是必填的。有关更多信息，请参阅临时安全凭证。

提供 ODBC 驱动程序用于调用 `GetClusterCredentials` API 操作的选项的详细信息：

- DbUser (必填)
- User AutoCreate (可选)
- DbGroups (可选)

  有关更多信息，请参阅用于创建数据库用户凭证的 JDBC 和 ODBC 选项 (p. 423)。

Identity Provider: AD FS

对于使用 AD FS 的 Windows 集成身份验证，请将 User 和 Password 保留为空。

提供 IdP 详细信息：

- IdP Host

  企业身份提供者主机的名称。此名称不应包含任何斜线 (/)。

- IdP Port (可选)

  身份提供者使用的端口。默认值为 443。

- Preferred Role

  SAML 断言中的 `AttributeValue` 属性的多值 `Role` 元素中的 IAM 角色 Amazon Resource Name (ARN)。请与 IdP 管理员一起查找适合首选角色的值。有关更多信息，请参阅为 IdP 配置 SAML 断言 (p. 394)。

（可选）提供 ODBC 驱动程序用于调用 `GetClusterCredentials` API 操作的选项的详细信息：

- DbUser
- User AutoCreate
- DbGroups

有关更多信息，请参阅用于创建数据库用户凭证的 JDBC 和 ODBC 选项 (p. 423)。

Identity Provider: PingFederate

对于 User (用户) 和 Password (密码)，键入您的 IdP 用户名和密码。

提供 IdP 详细信息：

- IdP Host

  企业身份提供者主机的名称。此名称不应包含任何斜线 (/)。

- IdP Port (可选)

  身份提供者使用的端口。默认值为 443。

- Preferred Role

  SAML 断言中的 `AttributeValue` 属性的多值 `Role` 元素中的 IAM 角色 Amazon Resource Name (ARN)。请与 IdP 管理员一起查找适合首选角色的值。有关更多信息，请参阅为 IdP 配置 SAML 断言 (p. 394)。

（可选）提供 ODBC 驱动程序用于调用 `GetClusterCredentials` API 操作的选项的详细信息：

- DbUser
- User AutoCreate
- DbGroups

有关更多信息，请参阅用于创建数据库用户凭证的 JDBC 和 ODBC 选项 (p. 423)。

Identity Provider: Okta

对于 User (用户) 和 Password (密码)，键入您的 IdP 用户名和密码。

提供 IdP 详细信息：

- IdP Host

  企业身份提供者主机的名称。此名称不应包含任何斜线 (/)。

- IdP Port

  Okta 不使用此值。

- Preferred Role

  SAML 断言中的 `AttributeValue` 属性的 `Role` 元素中的 IAM 角色 Amazon Resource Name (ARN)。请与 IdP 管理员一起查找适合首选角色的值。有关更多信息，请参阅为 IdP 配置 SAML 断言 (p. 394)。

- Okta App ID

  Okta 应用程序的 ID。应用程序 ID 的值位于 Okta 应用程序嵌入链接中的“amazon_aws”之后。与您的 IdP 管理员一起获取此值。

（可选）提供 ODBC 驱动程序用于调用 `GetClusterCredentials` API 操作的选项的详细信息：

- DbUser
- User AutoCreate
- DbGroups

有关更多信息，请参阅用于创建数据库用户凭证的 JDBC 和 ODBC 选项 (p. 423)。

身份提供者：Azure AD

对于 User (用户) 和 Password (密码)，键入您的 IdP 用户名和密码。

对于 Cluster ID（集群 ID）和 Region（区域），输入 Amazon Redshift 集群的集群 ID 和 Amazon 区域。

对于 Database（数据库），输入您为 Amazon Redshift 集群创建的数据库。

提供 IdP 详细信息：

- IdP Tenant (IdP 租户

  用于 Azure AD 的租户。

- Azure Client Secret (Azure 客户端密钥

  Azure 中的 Amazon Redshift 企业应用程序的客户端密钥。

- Azure Client ID (Azure 客户端 ID

  Azure 中的 Amazon Redshift 企业应用程序的客户端 ID（应用程序 ID）。

（可选）提供 ODBC 驱动程序用于调用 `GetClusterCredentials` API 操作的选项的详细信息：

- DbUser
- User AutoCreate
- DbGroups

有关更多信息，请参阅用于创建数据库用户凭证的 JDBC 和 ODBC 选项 (p. 423)。

用于提供 IAM 凭证的选项

要为 JDBC 或 ODBC 连接提供 IAM 凭证，请选择以下选项之一。

- Amazon 配置文件

作为以 JDBC 或 ODBC 设置形式提供凭证值的替代方案，您可在命名配置文件中放置这些值。有关更多信息，请参阅使用配置文件 (p. 402)。

- IAM 凭证

  以 JDBC 或 ODBC 设置形式提供 AccessKeyID、SecretAccessKey 和 (可选) SessionToken 的值。SessionToken 仅对于具有临时凭证的 IAM 角色是必填的。有关更多信息，请参阅用于提供 IAM 凭证的 JDBC 和 ODBC 选项 (p. 403)。

- 身份提供者联合

  在使用身份提供者联合以允许身份提供者中的用户在 Amazon Redshift 中进行身份验证时，请指定凭证提供商插件的名称。有关更多信息，请参阅使用凭证提供商插件 (p. 403)。

  Amazon Redshift JDBC 和 ODBC 驱动程序包括以下基于 SAML 的联合身份验证凭证提供商的插件：

  - Microsoft Active Directory 联合身份验证服务 (AD FS)
  - PingOne
  - Okta
  - Microsoft Azure Active Directory (Azure AD)

  您可以 JDBC 或 ODBC 设置格式提供或使用配置文件提供插件名称和相关值。有关更多信息，请参阅 JDBC 驱动程序版本 2.1 配置的选项 (p. 149) 和 配置 ODBC 驱动程序选项 (p. 216)。

有关更多信息，请参阅配置 JDBC 或 ODBC 连接以使用 IAM 凭证 (p. 397)。

使用配置文件

您可提供 IAM 凭证选项和 `GetClusterCredentials` 选项作为 Amazon 配置文件中的命名配置文件的设置。要提供配置文件名称，请使用配置文件 JDBC 选项。该配置存储在名为 `config` 的文件或位于主目录下面的名为 `credentials` 的文件夹中的名为 `.aws` 的文件中。

对于 Amazon Redshift JDBC 或 ODBC 驱动程序附带的基于 SAML 的凭证提供商插件，您可以使用 使用凭证提供商插件 (p. 403) 中前面所述的设置。如果未使用 `plugin_name`，则忽略其他选项。

下例所示为一个有两个配置文件的 ~/.aws/credentials 文件。

```
[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//////////
wEXAMPLEtc764bNrC9SAPBSM22wDOk4x4HIZ8j4FZTwdQWLWsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTflfKD8YUuwthAx7mSEI/
qkPpKPi/kMcGd
QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5VSXDvp75YU
9HFvlRd8Tx6q6fE8YQcHNVXAkiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fPOLn9FX9KSYvKTr4rvx3iSIlTJabIQwj2ICCR/oLxBA==
```

要使用 `user2` 示例的凭证，请在 JDBC URL 中指定 `Profile=user2`。

有关使用配置文件的更多信息，请参阅 Amazon Command Line Interface 用户指南中的命名配置文件。

有关为 JDBC 驱动程序使用配置文件的更多信息，请参阅 Amazon Redshift JDBC 驱动程序安装和配置指南。在中国（北京）区域中，使用以下链接：https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/jdbc/1.2.41.1065/Amazon+Redshift+JDBC+Driver+Install+Guide.pdf

有关为 ODBC 驱动程序使用配置文件的更多信息，请参阅 Amazon Redshift ODBC 驱动程序安装和配置指南。在 Amazon 中国区域中，使用以下链接：https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/odbc/1.4.10.1000/Amazon+Redshift+ODBC+Driver+Install+Guide.pdf

用于提供 IAM 凭证的 JDBC 和 ODBC 选项

下表列出了用于提供 IAM 凭证的 JDBC 和 ODBC 选项。

选项	描述
`Iam`	仅用于 ODBC 连接字符串。设置为 1 可使用 IAM 身份验证。

`AccessKeyID`
 	
`SecretAccessKey`
 	
`SessionToken`
	为 IAM 数据库身份验证配置的 IAM 角色或 IAM 用户的访问密钥 ID 和秘密访问密钥。`SessionToken` 仅对具有临时凭证的 IAM 角色是必需的。SessionToken 不用于 IAM 用户。有关更多信息，请参阅临时安全凭证。

`plugin_name`	实施凭证提供商的类的完全限定名称。Amazon Redshift JDBC 驱动程序包括基于 SAML 的凭证提供商插件。如果提供 `plugin_name`，您还可以提供其他相关选项。有关更多信息，请参阅使用凭证提供商插件 (p. 403)。
`Profile`	Amazon 凭证中配置文件的名称或包含 JDBC 连接选项值的 config 文件的名称。有关更多信息，请参阅使用配置文件 (p. 402)。

使用凭证提供商插件

Amazon Redshift 使用凭证提供商插件进行单点登录身份验证。

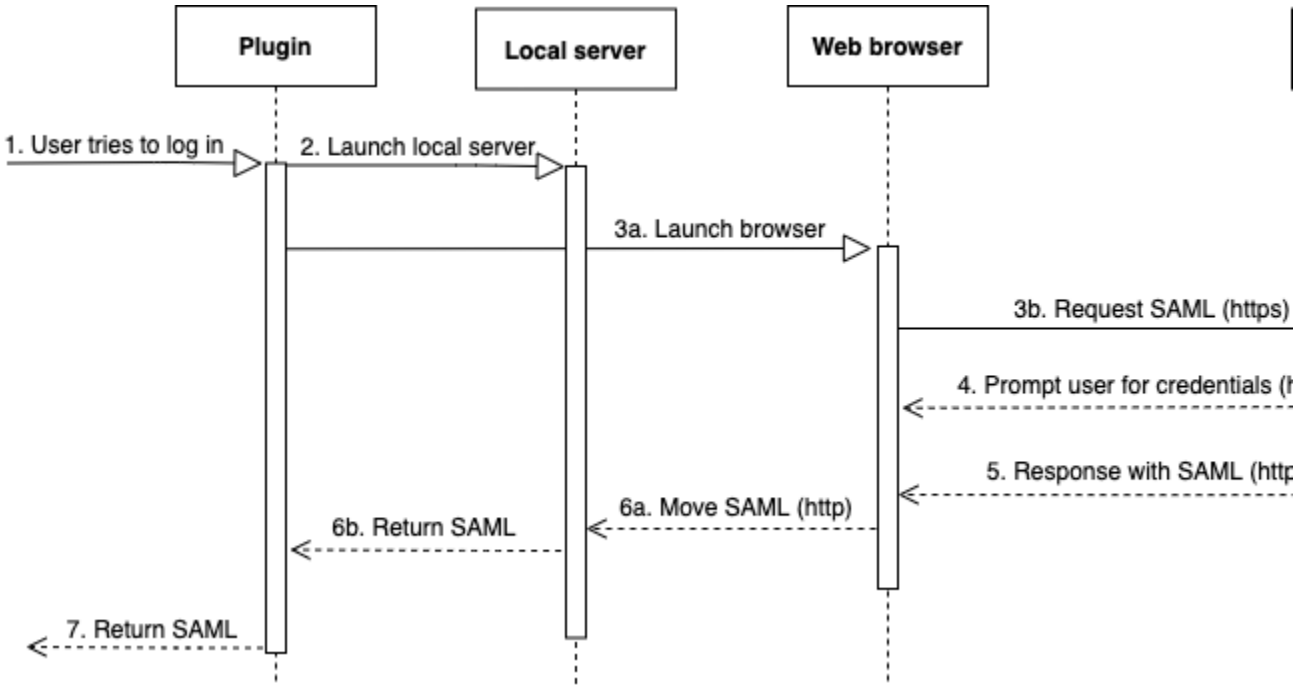
为了支持单点登录身份验证，Amazon Redshift 提供了适用于 Microsoft Azure Active Directory 的 Azure AD 插件。有关如何配置该插件的信息，请参阅在 Microsoft Azure AD 中设置 JDBC 或 ODBC 单点登录身份验证 (p. 407)。

设置 Multi-Factor Authentication

设置 Multi-Factor Authentication

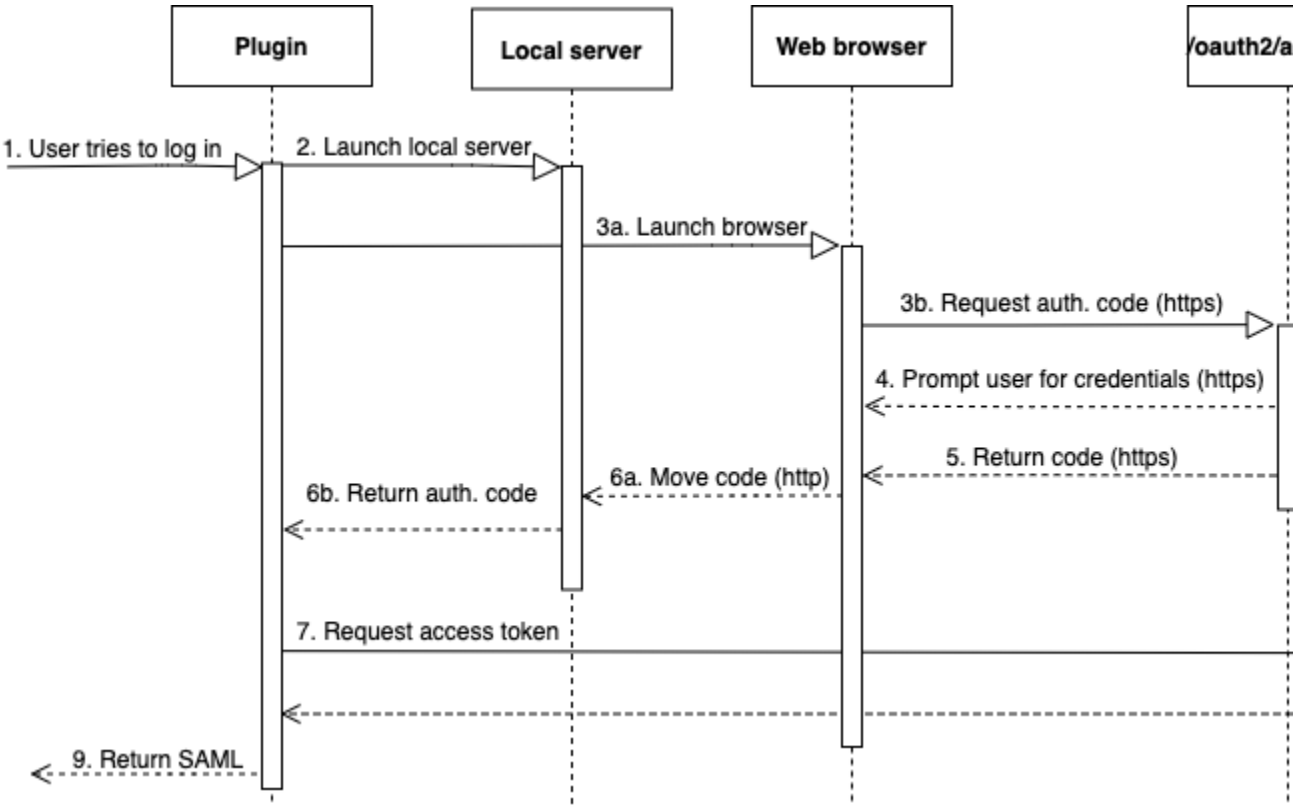
为了支持多重身份验证（MFA），Amazon Redshift 提供了基于浏览器的插件。请使用适用于 Okta、PingOne 的的浏览器 SAML 插件，以及适用于 Microsoft Azure Active Directory 的浏览器 Azure AD 插件。

在使用浏览器 SAML 插件时，SAML 身份验证流程如下所示：



1. 用户尝试登录。
2. 该插件启动本地服务器以侦听 localhost 上的传入连接。
3. 该插件启动 Web 浏览器，以通过 HTTPS 从指定的单点登录 URL 联合身份提供者端点请求 SAML 响应。
4. Web 浏览器访问该链接，并提示用户输入凭证。
5. 在用户进行身份验证并获得允许后，联合身份提供者端点通过 HTTPS 向 `redirect_uri` 指示的 URI 返回 SAML 响应。
6. Web 浏览器将包含 SAML 响应的响应消息传送到指示的 `redirect_uri`。
7. 本地服务器接受传入连接，该插件检索 SAML 响应并将其传送到 Amazon Redshift。

在使用浏览器 Azure AD 插件时，SAML 身份验证流程如下所示：



1. 用户尝试登录。
2. 该插件启动本地服务器以侦听 localhost 上的传入连接。
3. 该插件启动 Web 浏览器，以从 Azure AD `oauth2/authorize` 端点请求授权代码。
4. Web 浏览器通过 HTTPS 访问生成的链接，并提示用户输入凭证。该链接是使用配置属性（例如 tenant 和 client_id）生成的。
5. 在用户进行身份验证并获得允许后，Azure AD `oauth2/authorize` 端点通过 HTTPS 返回包含授权代码的响应并将其发送到指示的 `redirect_uri`。
6. Web 浏览器将包含 SAML 响应的响应消息传送到指示的 `redirect_uri`。
7. 本地服务器接受传入连接，该插件请求和检索授权代码，并将 POST 请求发送到 Azure AD `oauth2/token` 端点。
8. Azure AD `oauth2/token` 端点将包含访问令牌的响应返回到指示的 `redirect_uri`。
9. 该插件检索 SAML 响应并将其传送到 Amazon Redshift。

参阅以下部分：

- Active Directory 联合身份验证服务 (AD FS)

  有关更多信息，请参阅在 AD FS 中设置 JDBC 或 ODBC 单点登录身份验证 (p. 413)。
- PingOne (Ping)

  只有使用 Forms 身份验证预先确定的 PingOne IdP 适配器支持 Ping。

  有关更多信息，请参阅在 Ping Identity 中设置 JDBC 或 ODBC 单点登录身份验证 (p. 417)。
- Okta

  仅与 Amazon Web Services Management Console 一起使用的 Okta 提供的应用程序支持 Okta。

有关更多信息，请参阅在 Okta 中设置 JDBC 或 ODBC 单点登录身份验证 (p. 420)。

- Microsoft Azure Active Directory

  有关更多信息，请参阅在 Microsoft Azure AD 中设置 JDBC 或 ODBC 单点登录身份验证 (p. 407)。

配置插件选项

配置插件选项

要使用基于 SAML 的凭证提供商插件，请使用 JBDC 或 ODBC 选项，或在命名配置文件中指定以下选项。如果未指定 `plugin_name`，则忽略其他选项。

选项	描述

`plugin_name`	对于 JDBC，为实施凭证提供商的类名称。指定下列项之一：
	• 对于 Active Directory 联合身份验证服务
	`com.amazon.redshift.plugin.AdfsCredentialsProvider`
	• 对于 Okta
	`com.amazon.redshift.plugin.OktaCredentialsProvider`
	• 对于 PingFederate
	`com.amazon.redshift.plugin.PingCredentialsProvider`
	• 对于 Microsoft Azure Active Directory
	`com.amazon.redshift.plugin.AzureCredentialsProvider`
	• 对于 SAML MFA
	`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`
	• 对于具有 MFA 的 Microsoft Azure Active Directory 单点登录
	`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`
	
	对于 ODBC，指定下列项之一：
	• 对于 Active Directory 联合身份验证服务：`adfs`
	• 对于 Okta：`okta`
	• 对于 PingFederate：`ping`
	• 对于 Microsoft Azure Active Directory：`azure`
	• 对于 SAML MFA：`browser saml`
	• 对于具有 MFA 的 Microsoft Azure Active Directory 单点登录： `browser azure ad`

`idp_host`	企业身份提供者主机的名称。此名称不应包含任何斜线 (“/”)。对于 Okta 身份提供者，`idp_host` 的值应以 `.okta.com` 结尾。
`idp_port`	身份提供者使用的端口。默认值为 443。Okta 将忽略该端口。

选项	描述
preferred_role	SAML 断言中的 AttributeValue 属性的 Role 元素中的角色 Amazon Resource Name (ARN)。请与 IdP 管理员一起查找适合首选角色的值。有关更多信息，请参阅为 IdP 配置 SAML 断言 (p. 394)。
user	企业用户名，包括域 (如果适用)。例如，对于 Active Directory，域名的格式需为 domain \username。
密码	企业用户的密码。我们建议不使用此选项，而是使用您的 SQL 客户端提供密码。
app_id	Okta 应用程序的 ID。仅用于 Okta。app_id 的值位于 Okta 应用程序嵌入链接中的 amazon_aws 后面。与 IdP 管理员一起获取该值。以下是应用程序嵌入链接的示例：https://example.okta.com/home/amazon_aws/0oa2hylwrpM8UGehd1t7/272
idp_tenant	用于 Azure AD 的租户。仅与 Azure 一起使用。
client_id	Azure AD 中的 Amazon Redshift 企业应用程序的客户端 ID。仅与 Azure 一起使用。

在 Microsoft Azure AD 中设置 JDBC 或 ODBC 单点登录身份验证

您可以使用 Microsoft Azure AD 作为身份提供者 (IdP) 来访问 Amazon Redshift 集群。下面，您可以找到描述如何为此目的设置信任关系的过程。有关配置 Amazon 作为 IdP 的服务提供商的更多信息，请参阅 IAM 用户指南中的通过信赖方信任和添加陈述来配置 SAML 2.0 IdP。

> **Note**
>
> 要将 Azure AD 与 JDBC 一起使用，Amazon Redshift JDBC 驱动程序必须是版本 1.2.37.1061 或更高版本。要将 Azure AD 与 ODBC 一起使用，Amazon Redshift ODBC 驱动程序必须是版本 1.4.10.1000 或更高版本。

观看以下视频，了解如何通过 Microsoft Azure AD 单点登录进行联合 Amazon Redshift 访问：通过 Microsoft Azure AD 单点登录进行联合 Amazon Redshift 访问。

将 Azure AD 和您的 Amazon 账户设置为彼此信任

1. 创建或使用现有的 Amazon Redshift 集群，以使 Azure AD 用户连接到该集群。要配置连接，需要此集群的某些属性，例如集群标识符。有关更多信息，请参阅创建集群。
2. 在 Microsoft Azure 门户上设置用于 Amazon 的 Azure Active Directory、组、用户。
3. 在 Microsoft Azure 门户上添加 Amazon Redshift 以作为企业应用程序，以用于 Amazon 控制台单点登录和 Amazon Redshift 联合登录。选择 Enterprise application (企业应用程序)。
4. 选择 + New application (+ 新建应用程序)。将显示 Add an application (添加应用程序) 页面。
5. 在搜索字段中搜索 **AWS**。
6. 选择 Amazon Web Services (Amazon)，然后选择 Add (添加) 。将会创建 Amazon 应用程序。
7. 在 Manage (管理) 下面，选择 Single sign-on (单点登录)。
8. 选择 SAML。将显示 Amazon Web Services (Amazon) | SAML-based Sign-on (基于 SAML 的登录) 页面。
9. 选择 Yes (是) 以转到 Set up Single Sign-On with SAML (为 SAML 设置单点登录) 页面。该页面显示预配置的单点登录相关属性的列表。
10. 对于 Basic SAML Configuration (基本 SAML 配置)，请选择编辑图标，然后选择 Save (保存)。
11. 在配置多个应用程序时，请提供一个标识符值。例如，输入 ***https://signin.aws.amazon.com/saml#2***。请注意，从第二个应用程序开始，将该格式与 # 符号一起使用以指定唯一的 SPN 值。
12. 在 User Attributes and Claims (用户属性和声明) 部分中，选择编辑图标。

默认情况下，预配置了唯一用户标识符 (UID)、角色、RoleSessionName 和 SessionDuration 声明。

13. 选择 + Add new claim (+ 添加新的声明)，以便为数据库用户添加声明。

    对于 Name (名称)，请输入 **`DbUser`**。

    对于 Namespace (命名空间)，请输入 **`https://redshift.amazon.com/SAML/Attributes`**。

    对于 Source (源)，请选择 Attribute (属性)。

    对于 Source attribute (源属性)，请选择 user.userprincipalname。然后，选择 Save (保存)。
14. 选择 + Add new claim (+ 添加新的声明)，以便为 AutoCreate 添加声明。

    对于 Name (名称)，请输入 **`AutoCreate`**。

    对于 Namespace (命名空间)，请输入 **`https://redshift.amazon.com/SAML/Attributes`**。

    对于 Source (源)，请选择 Attribute (属性)。

    对于 Source attribute (源属性)，请选择 "true"。然后，选择 Save (保存)。

    此处，*`123456789012`* 是您 Amazon 账户，*`AzureSSO`* 是您创建的 IAM 角色，*`AzureADProvider`* 是 IAM 提供商。

声明名称	值
唯一用户标识符（名称 ID）	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. 在 App Registration (应用程序注册) > ***`your-application-name`*** > Authentication (身份验证) 下，添加 Mobile And Desktop Application (移动和桌面应用程序)。将 URL 指定为 http://localhost/redshift/。
16. 在 SAML Signing Certificate (SAML 签名证书) 部分中，选择 Download (下载) 以下载并保存联合元数据 XML 文件，以便在创建 IAM SAML 身份提供者时使用。该文件用于创建单点登录联合身份。
17. 在 IAM 控制台上创建 IAM SAML 身份提供者。您提供的元数据文档是您在设置 Azure 企业应用程序时保存的联合元数据 XML 文件。有关详细步骤，请参阅 IAM 用户指南中的创建和管理 IAM 身份提供者（控制台）。
18. 在 IAM 控制台上为 SAML 2.0 联合身份创建 IAM 角色。有关详细步骤，请参阅 IAM 用户指南中的创建用于 SAML 的角色。
19. 创建一个 IAM 策略，您可以将其附加到您在 IAM 控制台上为 SAML 2.0 联合身份验证创建的 IAM 角色。有关详细步骤，请参阅 IAM 用户指南中的创建 IAM 策略（控制台）。

为您的环境修改以下策略（JSON 格式）：

- 将集群的 Amazon 区域替换为 *us-west-1*。
- 将您的 Amazon 账户替换为 *123456789012*。
- 将您的集群标识符（或对于所有集群，则为 *）替换为 *cluster-identifier*。
- 将您的数据库（或对于所有集群，则为 *）替换为 *dev*。
- 将 IAM 角色的唯一标识符替换为 *AROAJ2UCCR6DPCEXAMPLE*。
- 将您的租户或公司电子邮件域替换为 *example.com*。
- 将您计划为其分配用户的数据库组替换为 *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": "*"
        }
    ]
}
```

此策略授予权限，如下所示：

- 第一部分授予执行 GetClusterCredentials API 操作的权限，以获取指定集群的临时凭证。在此示例中，资源是 *cluster-identifier*，所在的数据库为 *dev*，所在的账户为 *123456789012*，所在的 Amazon 区域为 *us-west-1*。${redshift:DbUser} 子句仅允许与在 Azure AD 中指定的 DbUser 值匹配的用户进行连接。

- 条件子句会强制只有特定用户能够获得临时凭证。这些用户是由角色唯一 ID *AROAJ2UCCR6DPCEXAMPLE* 指定的角色下的用户，该 ID 位于您公司的电子邮件域中的电子邮件地址所标识的 IAM 账户中。有关唯一 ID 的更多信息，请参阅 IAM 用户指南中的唯一 ID。

  您使用 IdP（在本例中为 Azure AD）进行的设置决定了条件子句的写入方式。如果员工的电子邮件是 `johndoe@example.com`，请首先将 `${redshift:DbUser}` 设置为与员工用户名 `johndoe` 匹配的超级用户字段。然后，要使该条件有效，请将 Amazon SAML `RoleSessionName` 字段设置为与员工电子邮件 `johndoe@example.com` 匹配的超级用户字段。使用这种方法时，请考虑以下几点：

  - 如果您将 `${redshift:DbUser}` 设置为员工的电子邮件，则删除示例 JSON 中的 `@example.com` 以匹配 `RoleSessionName`。
  - 如果您只是将 `RoleSessionId` 设置为员工的用户名，则删除示例中的 `@example.com` 以匹配 `RoleSessionName`。
  - 在示例 JSON 中，`${redshift:DbUser}` 和 `RoleSessionName` 都已设置为员工电子邮件。此示例 JSON 使用 Amazon Redshift 数据库用户名以及 `@example.com` 让用户登录以访问集群。
- 第二部分授予在指定集群中创建 `dbuser` 名称的权限。在此示例 JSON 中，它将创建限制为 `${redshift:DbUser}`。
- 第三部分授予指定用户可以加入 `dbgroup` 的权限。在此示例 JSON 中，用户可以加入指定集群中的 `my_dbgroup` 组。
- 第四部分授予用户可以对所有资源执行的操作的权限。在此示例 JSON 中，它允许用户调用 `redshift:DescribeClusters` 以获取集群信息，例如集群端点、Amazon 区域和端口。它还允许用户调用 `iam:ListRoles` 以检查用户可以代入哪些角色。

设置 JDBC 以在 Microsoft Azure AD 中进行身份验证

- 将数据库客户端配置为通过 JDBC 连接（使用 Azure AD 单点登录）到集群。

  您可以使用任何采用 JDBC 驱动程序的客户端通过 Azure AD 单点登录进行连接，也可以使用像 Java 这样的语言通过脚本进行连接。有关安装和配置信息，请参阅为 Amazon Redshift 配置 JDBC 驱动程序版本 2.1 连接 (p. 136)。

  例如，您可以使用 SQLWorkbench/J 作为客户端。当您配置 SQLWorkbench/J 时，数据库的 URL 使用以下格式。

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  如果您使用 SQLWorkbench/J 作为客户端，请执行以下步骤：

  a. 启动 SQL Workbench/J。在 Select Connection Profile（选择连接配置文件）页面上，添加一个称为 **`AzureAuth`** 的 Profile Group（配置文件组）。

  b. 对于 Connection Profile (连接配置文件)，请输入 **`Azure`**。

  c. 选择 Manage Drivers (管理驱动程序)，然后选择 Amazon Redshift。选择 Library（库）旁边的 Open Folder（打开文件夹）图标，然后选择适当的 JDBC .jar 文件。

  d. 在 Select Connection Profile (选择连接配置文件) 页面上，向连接配置文件添加信息，如下所示：

  - 对于 User (用户)，请输入 Microsoft Azure 用户名。这是您用于单点登录的 Microsoft Azure 账户的用户名，该账户有权限访问您在尝试进行身份验证时使用的集群。
  - 对于 Password (密码)，请输入您的 Microsoft Azure 密码。
  - 对于 Drivers (驱动程序)，请选择 Amazon Redshift (com.amazon.redshift.jdbc.Driver)。
  - 对于 URL，请输入 **`jdbc:redshift:iam//`*`your-cluster-identifier`*`:`*`your-cluster-region`*`/`*`your-database-name`**。

  e. 选择 Extended Properties (扩展属性) 以在连接属性中添加其他信息，如下所述。

  对于 Azure AD 单点登录配置，请添加附加信息，如下所示：

- 对于 plugin_name，请输入 **com.amazon.redshift.plugin.AzureCredentialsProvider**。该值指定驱动程序将 Azure AD 单点登录作为身份验证方法。
- 对于 idp_tenant，请输入 ***your-idp-tenant***。仅用于 Microsoft Azure AD。这是在 Azure AD 上为您的公司配置的租户名称。此值可以是租户名或带连字符的租户唯一 ID。
- 对于 client_secret，请输入 ***your-azure-redshift-application-client-secret***。仅用于 Microsoft Azure AD。这是您在设置 Azure 单点登录配置时创建的 Amazon Redshift 应用程序的客户端密钥。这仅适用于 com.amazon.redshift.plugin.AzureCredentialsProvider 插件。
- 对于 client_id，请输入 ***your-azure-redshift-application-client-id***。仅用于 Microsoft Azure AD。这是您在设置 Azure 单点登录配置时创建的 Amazon Redshift 应用程序的客户端 ID（带连字符）。

对于具有 MFA 的 Azure AD 单点登录配置，请在连接属性中添加附加信息，如下所示：

- 对于 plugin_name，请输入 **com.amazon.redshift.plugin.BrowserAzureCredentialsProvider**。此值指定驱动程序将具有 MFA 的 Azure 单点登录作为身份验证方法。
- 对于 idp_tenant，请输入 ***your-idp-tenant***。仅用于 Microsoft Azure AD。这是在 Azure AD 上为您的公司配置的租户名称。此值可以是租户名或带连字符的租户唯一 ID。
- 对于 client_id，请输入 ***your-azure-redshift-application-client-id***。此选项仅用于 Microsoft Azure AD。这是您在设置具有 MFA 的 Azure AD 单点登录配置时创建的 Amazon Redshift 应用程序的客户端 ID（带连字符）。
- 对于 listen_port (侦听端口)，请输入 ***your-listen-port***。这是本地服务器正在侦听的端口。默认值为 7890。
- 对于 idp_response_timeout，请输入 ***the-number-of-seconds***。这是 IdP 服务器发回响应时超时之前等待的秒数。最小秒数必须为 10。如果建立连接的用时长于此阈值，则连接将被中止。

设置 ODBC 以在 Microsoft Azure AD 中进行身份验证

- 将数据库客户端配置为通过 ODBC 连接（使用 Azure AD 单点登录）到集群。

  Amazon Redshift 提供了适用于 Linux、Windows 和 macOS 操作系统的 ODBC 驱动程序。在安装 ODBC 驱动程序之前，请确定您的 SQL 客户端工具是 32 位还是 64 位。安装符合 SQL 客户端工具要求的 ODBC 驱动程序。

  此外，为您的操作系统安装和配置最新的 Amazon Redshift OBDC 驱动程序，如下所示：

  - 对于 Windows，请参阅在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 208)。
  - 对于 macOS，请参阅 在 macOS X 上安装 Amazon Redshift ODBC 驱动程序 (p. 211)。
  - 对于 Linux，请参阅在 Linux 上安装 Amazon Redshift ODBC 驱动程序 (p. 210)。

  在 Windows 上的 Amazon Redshift ODBC Driver DSN Setup (Amazon Redshift ODBC 驱动程序 DSN 安装) 页的 Connection Settings (连接设置) 下，输入以下信息：

  - 对于 Data Source Name (数据源名称)，输入 ***your-DSN***。这将指定用作 ODBC 配置文件名称的数据源名称。
  - 对于 Azure AD 单点登录配置的 Auth type（身份验证类型），请选择 **Identity Provider: Azure AD**。这是 ODBC 驱动程序在通过 Azure 单点登录进行身份验证时使用的验证方法。
  - 对于具有 MMFA 的 Azure AD 单点登录配置的 Auth type（身份验证类型），请选择 **Identity Provider: Browser Azure AD**。这是 ODBC 驱动程序在通过 Azure 单点登录（采用 MFA）进行身份验证时使用的验证方法。

- 对于 Cluster ID (集群 ID)，请输入 ***your-cluster-identifier***。
- 对于 Region (区域)，请输入 ***your-cluster-region***。
- 对于 Database (数据库)，请输入 ***your-database-name***。
- 对于 User (用户)，请输入 ***your-azure-username***。这是您用于单点登录的 Microsoft Azure 账户的用户名，该账户有权限访问您在尝试进行身份验证时使用的集群。请仅将其用于 Auth Type (身份验证类型) 为 Identity Provider: Azure AD (身份提供者: Azure AD) 的情况。
- 对于 Password (密码)，请输入 ***your-azure-password***。请仅将其用于 Auth Type (身份验证类型) 为 Identity Provider: Azure AD (身份提供者: Azure AD) 的情况。
- 对于 IdP Tenant (IdP 租户)，请输入 ***your-idp-tenant***。这是在 IdP (Azure) 上配置的公司的租户名称。此值可以是租户名或带连字符的租户唯一 ID。
- 对于 Azure Client Secret (Azure 客户端密钥)，请输入 ***your-azure-redshift-application-client-secret***。这是您在设置 Azure 单点登录配置时创建的 Amazon Redshift 应用程序的客户端密钥。
- 对于 Azure Client ID (Azure 客户端 ID)，请输入 ***your-azure-redshift-application-client-id***。这是您在设置 Azure 单点登录配置时创建的 Amazon Redshift 应用程序的客户端 ID（带连字符）。
- 对于 Listen Port (侦听端口)，请输入 ***your-listen-port***。这是本地服务器正在侦听的默认侦听端口。默认值为 7890。这仅适用于浏览器 Azure AD 插件。
- 对于 Response Timeout (响应超时)，请输入 ***the-number-of-seconds***。这是 IdP 服务器发回响应时超时之前等待的秒数。最小秒数必须为 10。如果建立连接的用时长于此阈值，则连接将被中止。该选项仅适用于浏览器 Azure AD 插件。

在 macOS 和 Linux 上，按如下方式编辑 `odbc.ini` 文件：

Note

所有条目不区分大小写。

- 对于 clusterid，请输入 ***your-cluster-identifier***。这是已创建的 Amazon Redshift 集群的名称。
- 对于 region (区域)，请输入 ***your-cluster-region***。这是已创建的 Amazon Redshift 集群的 Amazon 区域。
- 对于 database (数据库)，请输入 ***your-database-name***。这是您尝试在 Amazon Redshift 集群上访问的数据库的名称。
- 对于 locale (区域设置)，请输入 **en-us**。这是显示错误消息的语言。
- 对于 iam，请输入 **1**。此值指定要使用 IAM 凭证进行身份验证的驱动程序。
- 对于 Azure AD 单点登录配置的 plugin_name（插件名称），请输入 **AzureAD**。这指定驱动程序使用 Azure 单点登录作为身份验证方法。
- 对于具有 MFA 的 Azure AD 单点登录配置的 plugin_name（插件名称），请输入 **BrowserAzureAD**。这指定驱动程序将 Azure 单点登录（采用 MFA）作为身份验证方法。
- 对于 uid，请输入 ***your-azure-username***。这是您用于单点登录的 Microsoft Azure 账户的用户名，该账户有权限访问您在尝试进行身份验证时使用的集群。请仅将其用于 plugin_name 为 AzureAD 的情况。
- 对于 pwd (密码)，请输入 ***your-azure-password***。请仅将其用于 plugin_name 为 AzureAD 的情况。
- 对于 idp_tenant，请输入 ***your-idp-tenant***。这是在 IdP (Azure) 上配置的公司的租户名称。此值可以是租户名或带连字符的租户唯一 ID。
- 对于 client_secret，请输入 ***your-azure-redshift-application-client-secret***。这是您在设置 Azure 单点登录配置时创建的 Amazon Redshift 应用程序的客户端密钥。
- 对于 client_id，请输入 ***your-azure-redshift-application-client-id***。这是您在设置 Azure 单点登录配置时创建的 Amazon Redshift 应用程序的客户端 ID（带连字符）。

- 对于 listen_port (侦听端口)，请输入 ***your-listen-port***。这是本地服务器正在侦听的端口。默认值为 7890。这适用于浏览器 Azure AD 插件。
- 对于 idp_response_timeout，请输入 ***the-number-of-seconds***。这是等待 Azure 响应的指定时间段（以秒为单位）。此选项适用于浏览器 Azure AD 插件。

在 macOS 和 Linux 上，还要编辑配置文件设置以添加以下导出。

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

解决浏览器 Azure AD 插件的问题

1. 要使用浏览器 Azure AD 插件，在请求中指定的回复 URL 必须与为应用程序配置的回复 URL 一致。

   导航到 Microsoft Azure 门户上的 Set up Single Sign-On with SAML (使用 SAML 设置单点登录) 页面。然后检查 Reply URL (回复 URL) 是否已设置为 http://localhost/redshift/。
2. 如果收到 IdP 租户错误，请验证 IdP Tenan (IdP 租户) 名称是否与最初在 Microsoft Azure 中设置 Active Directory 时所用的域名匹配。

   在 Windows 上，导航到 Amazon Redshift ODBC DSN Setup（Amazon Redshift ODBC DSN 设置）页面的 Connection Settings（连接设置）部分。然后检查在 IdP (Azure) 上配置的公司租户名称是否与最初在 Microsoft Azure 中设置 Active Directory 时所用的域名匹配。

   在 macOS 和 Linux 上，找到 odbc.ini 文件。然后检查在 IdP (Azure) 上配置的公司租户名称是否与最初在 Microsoft Azure 中设置 Active Directory 时所用的域名匹配。
3. 如果收到请求中指定的回复 URL 与为应用程序配置的回复 URL 不一致的错误，请验证 Redirect URIs (重定向 URI) 是否与回复 URL 相同。

   在 Microsoft Azure 门户上，导航到您的应用程序的 App registration (应用程序注册) 页面。然后检查重定向 URI 是否与回复 URL 一致。
4. 如果收到“未经授权错误”意外响应，请验证是否已完成 Mobile and desktop applications (移动和桌面应用程序) 配置。

   在 Microsoft Azure 门户上，导航到您的应用程序的 App registration (应用程序注册) 页面。然后导航到 Authentication (身份验证)，检查是否已将 Mobile and desktop applications (移动和桌面应用程序) 配置为使用 http://localhost/redshift/ 作为重定向 URI。

在 AD FS 中设置 JDBC 或 ODBC 单点登录身份验证

您可以将 AD FS 作为身份提供者 (IdP) 以访问 Amazon Redshift 集群。下面，您可以找到描述如何为此目的设置信任关系的过程。有关配置 Amazon 作为 AD FS 的服务提供商的更多信息，请参阅 IAM 用户指南中的通过信赖方信任和添加陈述来配置 SAML 2.0 IdP。

将 AD FS 和您的 Amazon 账户设置为相互信任

1. 创建或使用现有的 Amazon Redshift 集群，以使 AD FS 用户连接到该集群。要配置连接，需要此集群的某些属性，例如集群标识符。有关更多信息，请参阅创建集群。
2. 在 Microsoft 管理控制台上设置 AD FS 以控制 Amazon Redshift 访问：

   1. 选择 ADFS 2.0，然后选择添加信赖方信任。在添加信赖方信任向导页面上，选择开始。
   2. 在选择数据源页面上，选择导入有关在线或在本地网络上发布的信赖方的数据。

3. 对于联合元数据地址 (主机名或 URL)，请输入 **https://signin.aws.amazon.com/saml-metadata.xml**。元数据 XML 文件是将 Amazon 描述为信赖方的标准 SAML 元数据文档。
4. 在指定显示名称页面上，输入显示名称的值。
5. 在选择颁发授权规则页面上，选择一个颁发授权规则以允许或拒绝所有用户访问该信赖方。
6. 在准备好添加信任页面上，查看您的设置。
7. 在完成页面上，选择向导关闭时打开此信赖方信任的“编辑声明规则”对话框。
8. 在上下文（右键单击）菜单上，选择信赖方信任。
9. 对于您的信赖方，打开上下文（右键单击）菜单，然后选择编辑声明规则。在编辑声明规则页面上，选择添加规则。
10. 对于声明规则模板，请选择转换传入声明，然后在编辑规则 - NameId 页面上执行以下操作：
    - 对于声明规则名称，请输入 NameId。
    - 对于传入声明名称，请选择 Windows 账户名。
    - 对于传出声明名称，请选择名称 ID。
    - 对于传出名称 ID 格式，请选择持久性标识符。
    - 选择传递所有声明值。
11. 在编辑声明规则页面上，选择添加规则。在选择规则模板页面上，对于声明规则模板，请选择以声明方式发送 LDAP 特性。
12. 在配置规则页面上，执行以下操作：
    - 对于声明规则名称，请输入 RoleSessionName。
    - 对于特性存储，请选择 Active Directory。
    - 对于 LDAP 特性，请选择电子邮件地址。
    - 对于 Outgoing Claim Type（传出陈述名称），选择 https://aws.amazon.com/SAML/Attributes/RoleSessionName。
13. 在编辑声明规则页面上，选择添加规则。在选择规则模板页面上，对于声明规则模板，请选择使用自定义规则发送声明。
14. 在编辑规则 - 获取 AD 组页面上，对于声明规则名称，请输入获取 AD 组。
15. 对于自定义规则，请输入以下内容。

```
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. 在编辑声明规则页面上，选择添加规则。在选择规则模板页面上，对于声明规则模板，请选择使用自定义规则发送声明。
17. 在编辑规则 - 角色页面上，对于声明规则名称，请键入角色。
18. 对于自定义规则，请输入以下内容。

```
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-"));
```

请注意 SAML 提供商的 ARN 和要担任的角色。在该示例中，`arn:aws:iam:123456789012:saml-provider/ADFS` 是 SAML 提供商的 ARN，`arn:aws:iam:123456789012:role/ADFS-` 是角色的 ARN。

3. 确保您已下载 `federationmetadata.xml` 文件。检查以确认文档内容不包含无效的字符。这是在配置与 Amazon 的信任关系时使用的元数据文件。
4. 在 IAM 控制台上创建 IAM SAML 身份提供者。您提供的元数据文档是您在设置 Azure 企业应用程序时保存的联合元数据 XML 文件。有关详细步骤，请参阅 IAM 用户指南中的创建和管理 IAM 身份提供者（控制台）。
5. 在 IAM 控制台上为 SAML 2.0 联合身份创建 IAM 角色。有关详细步骤，请参阅 IAM 用户指南中的创建用于 SAML 的角色。
6. 创建一个 IAM 策略，您可以将其附加到您在 IAM 控制台上为 SAML 2.0 联合身份验证创建的 IAM 角色。有关详细步骤，请参阅 IAM 用户指南中的创建 IAM 策略（控制台）。有关 Azure AD 示例，请参阅在 Microsoft Azure AD 中设置 JDBC 或 ODBC 单点登录身份验证 (p. 407)。

设置 JDBC 以在 AD FS 中进行身份验证

- 将数据库客户端配置为通过 JDBC 并使用 AD FS 单点登录连接到集群。

  您可以使用任何采用 JDBC 驱动程序的客户端通过 AD FS 单点登录进行连接，也可以使用像 Java 这样的语言通过脚本进行连接。有关安装和配置信息，请参阅为 Amazon Redshift 配置 JDBC 驱动程序版本 2.1 连接 (p. 136)。

  例如，您可以使用 SQLWorkbench/J 作为客户端。当您配置 SQLWorkbench/J 时，数据库的 URL 使用以下格式。

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  如果您使用 SQLWorkbench/J 作为客户端，请执行以下步骤：

  a. 启动 SQL Workbench/J。在 Select Connection Profile（选择连接配置文件）页面中，添加一个 Profile Group（配置文件组），例如，**`ADFS`**。
  b. 对于 Connection Profile (连接配置文件)，请输入您的连接配置文件名称，例如 **`ADFS`**。
  c. 选择 Manage Drivers (管理驱动程序)，然后选择 Amazon Redshift。选择 Library（库）旁边的 Open Folder（打开文件夹）图标，然后选择适当的 JDBC .jar 文件。
  d. 在 Select Connection Profile (选择连接配置文件) 页面上，向连接配置文件添加信息，如下所示：
     - 对于 User (用户)，请输入您的 AD FS 用户名。这是您用于单点登录的账户的用户名，该账户有权限访问您在尝试进行身份验证时使用的集群。
     - 对于 Password (密码)，请输入您的 AD FS 密码。
     - 对于 Drivers (驱动程序)，请选择 Amazon Redshift (com.amazon.redshift.jdbc.Driver)。
     - 对于 URL，请输入 **`jdbc:redshift:iam//your-cluster-identifier:your-cluster-region/your-database-name`**。
  e. 选择 Extended Properties（扩展属性）。对于 plugin_name，请输入 **`com.amazon.redshift.plugin.AdfsCredentialsProvider`**。该值指定驱动程序将 AD FS 单点登录作为身份验证方法。

设置 ODBC 以在 AD FS 中进行身份验证

- 将数据库客户端配置为通过 ODBC 并使用 AD FS 单点登录连接到集群。

  Amazon Redshift 提供了适用于 Linux、Windows 和 macOS 操作系统的 ODBC 驱动程序。在安装 ODBC 驱动程序之前，请确定您的 SQL 客户端工具是 32 位还是 64 位。安装符合 SQL 客户端工具要求的 ODBC 驱动程序。

  此外，为您的操作系统安装和配置最新的 Amazon Redshift OBDC 驱动程序，如下所示：

- 对于 Windows，请参阅在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 208)。
- 对于 macOS，请参阅 在 macOS X 上安装 Amazon Redshift ODBC 驱动程序 (p. 211)。
- 对于 Linux，请参阅在 Linux 上安装 Amazon Redshift ODBC 驱动程序 (p. 210)。

在 Windows 上的 Amazon Redshift ODBC Driver DSN Setup (Amazon Redshift ODBC 驱动程序 DSN 安装) 页的 Connection Settings (连接设置) 下，输入以下信息：

- 对于 Data Source Name (数据源名称)，输入 ***your-DSN***。这将指定用作 ODBC 配置文件名称的数据源名称。
- 对于 Auth type（身份验证类型），选择 Identity Provider: SAML（身份提供者：SAML）。这是 ODBC 驱动程序在通过 AD FS 单点登录进行身份验证时使用的身份验证方法。
- 对于 Cluster ID (集群 ID)，请输入 ***your-cluster-identifier***。
- 对于 Region (区域)，请输入 ***your-cluster-region***。
- 对于 Database (数据库)，请输入 ***your-database-name***。
- 对于 User (用户)，请输入 ***your-adfs-username***。这是您用于单点登录的 AD FS 账户的用户名，该账户有权访问您在尝试进行身份验证时使用的集群。请仅将其用于 Auth type (身份验证类型) 为 Identity Provider: SAML (身份提供者: SAML) 的情况。
- 对于 Password (密码)，请输入 ***your-adfs-password***。请仅将其用于 Auth type (身份验证类型) 为 Identity Provider: SAML (身份提供者: SAML) 的情况。

在 macOS 和 Linux 上，按如下方式编辑 `odbc.ini` 文件：

> Note
>
> 所有条目不区分大小写。

- 对于 clusterid，请输入 ***your-cluster-identifier***。这是已创建的 Amazon Redshift 集群的名称。
- 对于 region (区域)，请输入 ***your-cluster-region***。这是已创建的 Amazon Redshift 集群的 Amazon 区域。
- 对于 database (数据库)，请输入 ***your-database-name***。这是您尝试在 Amazon Redshift 集群上访问的数据库的名称。
- 对于 locale (区域设置)，请输入 **en-us**。这是显示错误消息的语言。
- 对于 iam，请输入 **1**。此值指定要使用 IAM 凭证进行身份验证的驱动程序。
- 对于 plugin_name，请执行以下操作之一：
  - 对于具有 MFA 的 AD FS 单点登录配置，请输入 **BrowserSAML**。这是 ODBC 驱动程序在 AD FS 中进行身份验证时使用的身份验证方法。
  - 对于 AD FS 单点登录配置，请输入 **ADFS**。这是 ODBC 驱动程序在通过 Azure AD 单点登录进行身份验证时使用的身份验证方法。
- 对于 uid，请输入 ***your-adfs-username***。这是您用于单点登录的 Microsoft Azure 账户的用户名，该账户有权限访问您在尝试进行身份验证时使用的集群。请仅将其用于 plugin_name 为 ADFS 的情况。
- 对于 pwd (密码)，请输入 ***your-adfs-password***。请仅将其用于 plugin_name 为 ADFS 的情况。

在 macOS 和 Linux 上，还要编辑配置文件设置以添加以下导出。

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

在 Ping Identity 中设置 JDBC 或 ODBC 单点登录身份验证

您可以将 Ping Identity 作为身份提供者 (IdP) 以访问 Amazon Redshift 集群。下面，您可以找到描述如何使用 PingOne 门户为此目的设置信任关系的过程。有关配置 Amazon 作为 Ping 身份的服务提供商的更多信息，请参阅 IAM 用户指南中的通过信赖方信任和添加陈述来配置 SAML 2.0 IdP。

将 Ping 身份和您的 Amazon 账户设置为相互信任

1. 创建或使用现有的 Amazon Redshift 集群，以使 Ping 身份用户连接到该集群。要配置连接，需要此集群的某些属性，例如集群标识符。有关更多信息，请参阅创建集群。
2. 在 PingOne 门户上添加 Amazon Redshift 以作为新的 SAML 应用程序。有关详细步骤，请参阅 Ping Identity 文档。

    1. 转到 My Applications (我的应用程序)。
    2. 在 (Add Application添加应用程序) 下面，选择 New SAML Application (新建 SAML 应用程序)。
    3. 对于 Application Name (应用程序名称)，请输入 **`Amazon Redshift`**。
    4. 对于 Protocol Version (协议版本)，请选择 SAML v2.0。
    5. 对于 Category (类别)，请选择 ***`your-application-category`***。
    6. 对于 Assertion Consumer Service (ACS) (断言使用者服务 (ACS))，请键入 ***`your-redshift-local-host-url`***。这是 SAML 断言重定向到的本地主机和端口。
    7. 对于 Entity ID (实体 ID)，请输入 `urn:amazon:webservices`。
    8. 对于 Signing (签名)，请选择 Sign Assertion (签名断言)。
    9. 在 SSO Attribute Mapping (SSO 属性映射) 部分中，创建声明，如下表中所示。

应用程序属性	文本值的身份关联属性
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"
https://redshift.amazon.com/SAML/Attributes/DbUser	email
https://redshift.amazon.com/SAML/Attributes/DbGroups	“DbGroups”属性中的组包含 @directory 前缀。若要删除此项，请在 Identity bridge（身份关联）中，输入 memberOf。在 Function（函数）中，选择 ExtractByRegularExpression。在 Expression（表达式）中，输入 (.*)[\@](?:.*)。

3. 对于 Group Access (组访问权限)，请设置以下组访问权限（如果需要）：

    - 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. 查看设置，并在必要时进行更改。
5. 将 Initiate Single Sign-On (SSO) URL（启动单点登录 URL）作为浏览器 SAML 插件的登录 URL。
6. 在 IAM 控制台上创建 IAM SAML 身份提供者。您提供的元数据文档是您在设置 Ping Identity 时保存的联合元数据 XML 文件。有关详细步骤，请参阅 IAM 用户指南中的创建和管理 IAM 身份提供者（控制台）。
7. 在 IAM 控制台上为 SAML 2.0 联合身份创建 IAM 角色。有关详细步骤，请参阅 IAM 用户指南中的创建用于 SAML 的角色。
8. 创建一个 IAM 策略，您可以将其附加到您在 IAM 控制台上为 SAML 2.0 联合身份验证创建的 IAM 角色。有关详细步骤，请参阅 IAM 用户指南中的创建 IAM 策略（控制台）。有关 Azure AD 示例，请参阅在 Microsoft Azure AD 中设置 JDBC 或 ODBC 单点登录身份验证 (p. 407)。

设置 JDBC 以在 Ping Identity 中进行身份验证

- 配置数据库客户端以使用 Ping Identity 单点登录通过 JDBC 连接到集群。

  您可以使用任何采用 JDBC 驱动程序的客户端通过 Ping Identity 单点登录进行连接，也可以使用像 Java 这样的语言通过脚本进行连接。有关安装和配置信息，请参阅为 Amazon Redshift 配置 JDBC 驱动程序版本 2.1 连接 (p. 136)。

  例如，您可以使用 SQLWorkbench/J 作为客户端。当您配置 SQLWorkbench/J 时，数据库的 URL 使用以下格式。

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  如果您使用 SQLWorkbench/J 作为客户端，请执行以下步骤：

  a. 启动 SQL Workbench/J。在 Select Connection Profile（选择连接配置文件）页面中，添加一个 Profile Group（配置文件组），例如，**`Ping`**。
  b. 对于 Connection Profile (连接配置文件)，请输入 ***`your-connection-profile-name`***，例如，**`Ping`**。
  c. 选择 Manage Drivers (管理驱动程序)，然后选择 Amazon Redshift。选择 Library（库）旁边的 Open Folder（打开文件夹）图标，然后选择适当的 JDBC .jar 文件。
  d. 在 Select Connection Profile (选择连接配置文件) 页面上，向连接配置文件添加信息，如下所示：
     - 对于 User (用户)，请输入您的 PingOne 用户名。这是您用于单点登录的 PingOne 账户的用户名，该账户有权限访问您在尝试进行身份验证时使用的集群。
     - 对于 Password (密码)，请输入您的 PingOne 密码。
     - 对于 Drivers (驱动程序)，请选择 Amazon Redshift (com.amazon.redshift.jdbc.Driver)。
     - 对于 URL，请输入 **`jdbc:redshift:iam//`*`your-cluster-identifier`*`:`*`your-cluster-region`*`/`*`your-database-name`***。
  e. 选择 Extended Properties (扩展属性) 并执行以下操作之一：
     - 对于 login_url，请输入 ***`your-ping-sso-login-url`***。该值指定 URL 将单点登录用作登录时的身份验证方法。
     - 对于 Ping Identity，请为 plugin_name 输入 **`com.amazon.redshift.plugin.PingCredentialsProvider`**。此值指定驱动程序使用 Ping Identity 单点登录作为身份验证方法。
     - 对于具有单点登录的 Ping Identity，请为 plugin_name 输入 **`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`**。该值指定驱动程序将具有单点登录的 Ping Identity PingOne 用作身份验证方法。

设置 ODBC 以在 Ping Identity 中进行身份验证

- 配置数据库客户端以使用 Ping Identity PingOne 单点登录通过 ODBC 连接到集群。

  Amazon Redshift 提供了适用于 Linux、Windows 和 macOS 操作系统的 ODBC 驱动程序。在安装 ODBC 驱动程序之前，请确定您的 SQL 客户端工具是 32 位还是 64 位。安装符合 SQL 客户端工具要求的 ODBC 驱动程序。

  此外，为您的操作系统安装和配置最新的 Amazon Redshift OBDC 驱动程序，如下所示：

  - 对于 Windows，请参阅在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 208)。
  - 对于 macOS，请参阅 在 macOS X 上安装 Amazon Redshift ODBC 驱动程序 (p. 211)。
  - 对于 Linux，请参阅在 Linux 上安装 Amazon Redshift ODBC 驱动程序 (p. 210)。

  在 Windows 上的 Amazon Redshift ODBC Driver DSN Setup (Amazon Redshift ODBC 驱动程序 DSN 安装) 页的 Connection Settings (连接设置) 下，输入以下信息：

  - 对于 Data Source Name (数据源名称)，输入 ***your-DSN***。这将指定用作 ODBC 配置文件名称的数据源名称。
  - 对于 Auth type (身份验证类型)，请执行以下操作之一：
    - 对于 Ping Identity 配置，请选择身份提供者：Ping Federate。这是 ODBC 驱动程序在通过 Ping Identity 单点登录进行身份验证时使用的身份验证方法。
    - 对于具有单点登录的 Ping Identity 配置，请选择 Identity Provider: Browser SAML（身份提供者：浏览器 SAML）。这是 ODBC 驱动程序在使用具有单点登录的 Ping Identity 进行身份验证时使用的身份验证方法。
  - 对于 Cluster ID (集群 ID)，请输入 ***your-cluster-identifier***。
  - 对于 Region (区域)，请输入 ***your-cluster-region***。
  - 对于 Database (数据库)，请输入 ***your-database-name***。
  - 对于 User (用户)，请输入 ***your-ping-username***。这是您用于单点登录的 PingOne 账户的用户名，该账户有权访问您在尝试进行身份验证时使用的集群。请仅将其用于 Auth type (身份验证类型) 为 Identity Provider: PingFederate (身份提供者: PingFederate) 的情况。
  - 对于 Password (密码)，请输入 ***your-ping-password***。请仅将其用于 Auth type (身份验证类型) 为 Identity Provider: PingFederate (身份提供者: PingFederate) 的情况。
  - 对于 Listen Port (侦听端口)，请输入 ***your-listen-port***。这是本地服务器正在侦听的端口。默认值为 7890。这仅适用于浏览器 SAML 插件。
  - 对于 Response Timeout (响应超时)，请输入 ***the-number-of-seconds***。这是 IdP 服务器发回响应时超时之前等待的秒数。最小秒数必须为 10。如果建立连接的用时长于此阈值，则连接将被中止。这仅适用于浏览器 SAML 插件。
  - 对于 Login URL (登录 URL)，请输入 ***your-login-url***。这仅适用于浏览器 SAML 插件。

  在 macOS 和 Linux 上，按如下方式编辑 `odbc.ini` 文件：

  > **Note**
  >
  > 所有条目不区分大小写。

  - 对于 clusterid，请输入 ***your-cluster-identifier***。这是已创建的 Amazon Redshift 集群的名称。
  - 对于 region (区域)，请输入 ***your-cluster-region***。这是已创建的 Amazon Redshift 集群的 Amazon 区域。
  - 对于 database (数据库)，请输入 ***your-database-name***。这是您尝试在 Amazon Redshift 集群上访问的数据库的名称。

- 对于 locale (区域设置)，请输入 **en-us**。这是显示错误消息的语言。
- 对于 iam，请输入 **1**。此值指定要使用 IAM 凭证进行身份验证的驱动程序。
- 对于 plugin_name，请执行以下操作之一：
  - 对于 Ping Identity 配置，请输入 **BrowserSAML**。这是 ODBC 驱动程序在使用 Ping Identity 进行身份验证时所采用的身份验证方法。
  - 对于具有单点登录的 Ping Identity 配置，请输入 **Ping**。这是 ODBC 驱动程序在使用具有单点登录的 Ping Identity 进行身份验证时使用的身份验证方法。
- 对于 uid，请输入 ***your-ping-username***。这是您用于单点登录的 Microsoft Azure 账户的用户名，该账户有权限访问您在尝试进行身份验证时使用的集群。请仅将其用于 plugin_name 为 Ping 的情况。
- 对于 pwd (密码)，请输入 ***your-ping-password***。请仅将其用于 plugin_name 为 Ping 的情况。
- 对于 login_url，请输入 ***your-login-url***。这是返回 SAML 响应的启动单点登录 URL。这仅适用于浏览器 SAML 插件。
- 对于 idp_response_timeout，请输入 ***the-number-of-seconds***。这是等待 PingOne Identity 响应的指定时间段（以秒为单位）。这仅适用于浏览器 SAML 插件。
- 对于 listen_port (侦听端口)，请输入 ***your-listen-port***。这是本地服务器正在侦听的端口。默认值为 7890。这仅适用于浏览器 SAML 插件。

在 macOS 和 Linux 上，还要编辑配置文件设置以添加以下导出。

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

在 Okta 中设置 JDBC 或 ODBC 单点登录身份验证

您可以将 Okta 作为身份提供者 (IdP) 以访问 Amazon Redshift 集群。下面，您可以找到描述如何为此目的设置信任关系的过程。有关配置 Amazon 作为 Okta 的服务提供商的更多信息，请参阅 IAM 用户指南中的通过信赖方信任和添加陈述来配置 SAML 2.0 IdP。

将 Okta 和您的 Amazon 账户设置为相互信任

1. 创建或使用现有的 Amazon Redshift 集群，以使 Okta 用户连接到该集群。要配置连接，需要此集群的某些属性，例如集群标识符。有关更多信息，请参阅创建集群。
2. 在 Okta 门户上添加 Amazon Redshift 以作为新应用程序。有关详细步骤，请参阅 Okta 文档。
   - 选择 Add Application (添加应用程序)。
   - 在 Add Application (添加应用程序) 下面，选择 Create New App (创建新的应用程序)。
   - 在 Create a New Add Application Integration (创建新添加应用程序集成) 页面上，为 Platform (平台) 选择 Web。
   - 对于 Sign on method (登录方法)，请选择 SAML v2.0。
   - 在 General Settings (常规设置) 页面上，为 App name (应用程序名称) 输入 ***your-redshift-saml-sso-name***。这是您的应用程序的名称。
   - 在 SAML Settings（SAML 设置）页面上，为 Single sign on URL（单点登录 URL）输入 ***your-redshift-local-host-url***。这是 SAML 断言重定向到的本地主机和端口，例如 `http://localhost:7890/redshift/`。
3. 将 Single sign on URL（单点登录 URL）作为 Recipient URL（收件人 URL）和 Destination URL（目标 URL）。
4. 对于 Signing (签名)，请选择 Sign Assertion (签名断言)。

5. 对于 Audience URI (SP Entity ID) (受众 URI (SP 实体 ID) ，为声明输入 **`urn:amazon:webservices`**，如下表中所示。
6. 在 Advanced Settings (高级设置) 部分中，为 SAML Issuer ID (SAML 发布者 ID) 输入 ***`your-Identity-Provider-Issuer-ID`***；您可以在 View Setup Instructions (查看设置说明) 部分中找到该 ID。
7. 在 Attribute Statements (属性语句) 部分中，创建声明，如下表中所示。

声明名称	值
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. 在 App Embed Link (应用程序嵌入式链接) 部分中，找到可用作浏览器 SAML 插件登录 URL 的 URL。
9. 在 IAM 控制台上创建 IAM SAML 身份提供者。您提供的元数据文档是您在设置 Okta 时保存的联合元数据 XML 文件。有关详细步骤，请参阅 IAM 用户指南中的创建和管理 IAM 身份提供者 (控制台) 。
10. 在 IAM 控制台上为 SAML 2.0 联合身份创建 IAM 角色。有关详细步骤，请参阅 IAM 用户指南中的创建用于 SAML 的角色。
11. 创建一个 IAM 策略，您可以将其附加到您在 IAM 控制台上为 SAML 2.0 联合身份验证创建的 IAM 角色。有关详细步骤，请参阅 IAM 用户指南中的创建 IAM 策略 (控制台) 。有关 Azure AD 示例，请参阅在 Microsoft Azure AD 中设置 JDBC 或 ODBC 单点登录身份验证 (p. 407)。

设置 JDBC 以在 Okta 中进行身份验证

- 将数据库客户端配置为通过 JDBC 并使用 Okta 单点登录连接到集群。

  您可以使用任何采用 JDBC 驱动程序的客户端通过 Okta 单点登录进行连接，也可以使用像 Java 这样的语言通过脚本进行连接。有关安装和配置信息，请参阅为 Amazon Redshift 配置 JDBC 驱动程序版本 2.1 连接 (p. 136)。

  例如，您可以使用 SQLWorkbench/J 作为客户端。当您配置 SQLWorkbench/J 时，数据库的 URL 使用以下格式。

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  如果您使用 SQLWorkbench/J 作为客户端，请执行以下步骤：

  a. 启动 SQL Workbench/J。在 Select Connection Profile (选择连接配置文件) 页面中，添加一个 Profile Group (配置文件组) ，例如，**`Okta`**。
  b. 对于 Connection Profile (连接配置文件)，请输入 ***`your-connection-profile-name`***，例如，**`Okta`**。
  c. 选择 Manage Drivers (管理驱动程序)，然后选择 Amazon Redshift。选择 Library (库) 旁边的 Open Folder (打开文件夹) 图标，然后选择适当的 JDBC .jar 文件。
  d. 在 Select Connection Profile (选择连接配置文件) 页面上，向连接配置文件添加信息，如下所示：

- 对于 User (用户)，请输入您的 Okta 用户名。这是您用于单点登录的 Okta 账户的用户名，该账户有权限访问您在尝试进行身份验证时使用的集群。
- 对于 Password (密码)，请输入您的 Okta 密码。
- 对于 Drivers (驱动程序)，请选择 Amazon Redshift (com.amazon.redshift.jdbc.Driver)。
- 对于 URL，请输入 **jdbc:redshift:iam//*your-cluster-identifier*:*your-cluster-region*/*your-database-name***。

e. 选择 Extended Properties (扩展属性) 并执行以下操作之一：

- 对于 login_url，请输入 ***your-okta-sso-login-url***。该值指定 URL 将单点登录作为身份验证方法以登录到 Okta。
- 对于 Okta 单点登录，请为 plugin_name（插件名称）输入 **com.amazon.redshift.plugin.OktaCredentialsProvider**。此值指定驱动程序使用 Okta 单点登录作为身份验证方法。
- 对于具有 MFA 的 Okta 单点登录，请为 plugin_name（插件名称）输入 **com.amazon.redshift.plugin.BrowserSamlCredentialsProvider**。此值指定驱动程序将具有 MFA 的 Okta 单点登录作为身份验证方法。

设置 ODBC 以在 Okta 中进行身份验证

- 将数据库客户端配置为通过 ODBC 并使用 Okta 单点登录连接到集群。

  Amazon Redshift 提供了适用于 Linux、Windows 和 macOS 操作系统的 ODBC 驱动程序。在安装 ODBC 驱动程序之前，请确定您的 SQL 客户端工具是 32 位还是 64 位。安装符合 SQL 客户端工具要求的 ODBC 驱动程序。

  此外，为您的操作系统安装和配置最新的 Amazon Redshift OBDC 驱动程序，如下所示：

  - 对于 Windows，请参阅在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 208)。
  - 对于 macOS，请参阅 在 macOS X 上安装 Amazon Redshift ODBC 驱动程序 (p. 211)。
  - 对于 Linux，请参阅在 Linux 上安装 Amazon Redshift ODBC 驱动程序 (p. 210)。

  在 Windows 上的 Amazon Redshift ODBC Driver DSN Setup (Amazon Redshift ODBC 驱动程序 DSN 安装) 页的 Connection Settings (连接设置) 下，输入以下信息：

  - 对于 Data Source Name (数据源名称)，输入 ***your-DSN***。这将指定用作 ODBC 配置文件名称的数据源名称。
  - 对于 Auth type (身份验证类型)，请执行以下操作之一：
    - 对于 Okta 单点登录配置，请选择 **Identity Provider: Okta**。这是 ODBC 驱动程序在通过 Okta 单点登录进行身份验证时使用的身份验证方法。
    - 对于具有 MFA 的 Okta 单点登录配置，请选择 **Identity Provider: Browser SAML**。这是 ODBC 驱动程序在通过具有 MFMFA 的 Okta 单点登录进行身份验证时使用的身份验证方法。
  - 对于 Cluster ID (集群 ID)，请输入 ***your-cluster-identifier***。
  - 对于 Region (区域)，请输入 ***your-cluster-region***。
  - 对于 Database (数据库)，请输入 ***your-database-name***。
  - 对于 User (用户)，请输入 ***your-okta-username***。这是您用于单点登录的 Okta 账户的用户名，该账户有权访问您在尝试进行身份验证时使用的集群。请仅将其用于 Auth type (身份验证类型) 为 Identity Provider: Okta (身份提供者: Okta) 的情况。
  - 对于 Password (密码)，请输入 ***your-okta-password***。请仅将其用于 Auth type (身份验证类型) 为 Identity Provider: Okta (身份提供者: Okta) 的情况。

在 macOS 和 Linux 上，按如下方式编辑 `odbc.ini` 文件：

Note

所有条目不区分大小写。

- 对于 clusterid，请输入 ***your-cluster-identifier***。这是已创建的 Amazon Redshift 集群的名称。
- 对于 region (区域)，请输入 ***your-cluster-region***。这是已创建的 Amazon Redshift 集群的 Amazon 区域。
- 对于 database (数据库)，请输入 ***your-database-name***。这是您尝试在 Amazon Redshift 集群上访问的数据库的名称。
- 对于 locale (区域设置)，请输入 **en-us**。这是显示错误消息的语言。
- 对于 iam，请输入 **1**。此值指定要使用 IAM 凭证进行身份验证的驱动程序。
- 对于 plugin_name，请执行以下操作之一：
  - 对于具有 MFA 的 Okta 单点登录配置，请输入 **BrowserSAML**。这是 ODBC 驱动程序在通过具有 MFMFA 的 Okta 单点登录进行身份验证时使用的身份验证方法。
  - 对于 Okta 单点登录配置，请输入 **Okta**。这是 ODBC 驱动程序在通过 Okta 单点登录进行身份验证时使用的身份验证方法。
- 对于 uid，请输入 ***your-okta-username***。这是您用于单点登录的 Okta 账户的用户名，该账户有权访问您在尝试进行身份验证时使用的集群。请仅将其用于 plugin_name 为 Okta 的情况。
- 对于 pwd (密码)，请输入 ***your-okta-password***。请仅将其用于 plugin_name 为 Okta 的情况。
- 对于 login_url，请输入 ***your-login-url***。这是返回 SAML 响应的启动单点登录 URL。这仅适用于浏览器 SAML 插件。
- 对于 idp_response_timeout，请输入 ***the-number-of-seconds***。这是等待 PingOne 响应的指定时间段（以秒为单位）。这仅适用于浏览器 SAML 插件。
- 对于 listen_port (侦听端口)，请输入 ***your-listen-port***。这是本地服务器正在侦听的端口。默认值为 7890。这仅适用于浏览器 SAML 插件。

在 macOS 和 Linux 上，还要编辑配置文件设置以添加以下导出。

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

用于创建数据库用户凭证的 JDBC 和 ODBC 选项

要使用 Amazon Redshift JDBC 或 ODBC 驱动程序创建数据库用户凭证，请提供数据库用户名作为 JDBC 或 ODBC 选项。（可选）您可以让驱动程序创建新的数据库用户（如果不存在），并且可以指定用户在登录时加入的数据库用户组列表。

如果您使用身份提供者 (IdP)，请与 IdP 管理员一起确定这些选项的正确值。您的 IdP 管理员还可配置 IdP 来提供这些选项，这样一来，您将无需提供它们作为 JDBC 或 ODBC 选项。有关更多信息，请参阅为 IdP 配置 SAML 断言 (p. 394)。

Note

如果您使用 IAM 策略变量 `${redshift:DbUser}`（如GetClusterCredentials 的资源策略 (p. 380)中所述），则 `DbUser` 的值将被替换为由 API 操作的请求上下文检索的值。Amazon Redshift 驱动程序使用由连接 URL 提供的 `DbUser` 变量的值，而不是作为 SAML 属性提供的值。

为帮助保护此配置，我们建议您在 IAM 策略中使用一个使用来通过 `DbUser` 验证 `RoleSessionName` 值。您可以在 使用 GetClusterCredentials 的示例策略 (p. 385) 中找到如何使用 IAM 策略设置条件。

下表列出了用于创建数据库用户凭证的选项。

选项	描述
DbUser	数据库用户的名称。如果数据库中存在名为 DbUser 的用户，则临时用户凭证具有与现有用户相同的权限。如果数据库中不存在 DbUser 且 AutoCreate 为 true，则创建一个名为 DbUser 的新用户。(可选) 禁用现有用户的密码。有关更多信息，请参阅 ALTER_USER
AutoCreate	指定 `true` 以使用为 DbUser 指定的名称创建数据库用户（如果不存在）。默认为 false。
`DbGroups`	数据库用户在当前会话中加入的一个或多个现有数据库组的名称的逗号分隔列表。默认情况下，新用户仅添加到 PUBLIC。

使用 Amazon Redshift CLI 或 API 生成 IAM 数据库凭证

为了以编程方式生成临时数据库用户凭证，Amazon Redshift 提供适用于 Amazon Command Line Interface (Amazon CLI) 和 GetClusterCredentials API 操作的 get-cluster-credentials 命令。或者，您可以使用 Amazon Redshift JDBC 或 ODBC 驱动程序配置您的 SQL 客户端，这些驱动程序用于管理调用 `GetClusterCredentials` 操作，检索数据库用户凭证，并在您的 SQL 客户端与您的 Amazon Redshift 数据库之间建立连接的过程。有关更多信息，请参阅用于创建数据库用户凭证的 JDBC 和 ODBC 选项 (p. 423)。

Note

我们建议使用 Amazon Redshift JDBC 或 ODBC 驱动程序生成数据库用户凭证。

在此部分中，您可以找到用于以编程方式调用 `GetClusterCredentials` 操作或 get-cluster-credentials 命令，检索数据库用户凭证并连接到数据库的步骤。

生成和使用临时数据库凭证

1. 创建或修改具有所需权限的 IAM 用户或角色。有关 IAM 权限的更多信息，请参阅创建有权调用 GetClusterCredentials 的 IAM 角色或用户 (p. 395)。
2. 以您在上一步骤中授权的 IAM 用户或角色的身份，运行 get-cluster-credentials CLI 命令或调用 `GetClusterCredentials` API 操作并提供下列值：
   - 集群标识符 – 包含数据库的集群的名称。
   - 数据库用户名 – 现有的或新的数据库用户的名称。
     - 如果数据库中不存在此用户且 AutoCreate 为 true，则将创建一个已禁用 PASSWORD 的新用户。
     - 如果此用户不存在且 AutoCreate 为 false，则请求会失败。
     - 在此示例中，数据库用户名为 `temp_creds_user`。
   - Autocreate – （可选）如果数据库用户名不存在，则创建新用户。
   - 数据库名称 – （可选）授权用户登录的数据库的名称。如果未指定数据库名称，则用户可以登录到任何集群数据库。
   - 数据库组 – （可选）现有数据库用户组的列表。在成功登录后，数据库用户将添加到指定的用户组中。如果未指定组，则用户仅具有 PUBLIC 权限。此用户组名称必须与在附加到 IAM 用户或角色的 IAM 策略中指定的 dbgroup 资源 ARN 匹配。
   - 过期时间 – （可选）临时凭证过期之前经历的时间（以秒为单位）。您可指定一个介于 900 秒 (15 分钟) 和 3600 秒 (60 分钟) 之间的值。默认值为 900 秒。
3. Amazon Redshift 确认 IAM 用户是否有权使用指定资源来调用 `GetClusterCredentials` 操作。

4. Amazon Redshift 返回临时密码和数据库用户名。

   以下示例使用 Amazon Redshift CLI 为名为 `temp_creds_user` 的现有用户生成临时数据库凭证。

   ```
   aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
    temp_creds_user --db-name exampledb --duration-seconds 3600
   ```

   结果如下所示。

   ```
   {
     "DbUser": "IAM:temp_creds_user",
     "Expiration": "2016-12-08T21:12:53Z",
     "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpDHwXVPyJYBDm/
   gqX2Eeaq6P3DgTzgPg=="
   }
   ```

   以下示例使用 Amazon Redshift CLI 与 autocreate 为新用户生成临时数据库凭证并将此用户添加到组 `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
   ```

   结果如下所示。

   ```
   {
     "DbUser": "IAMA:temp_creds_user:example_group",
     "Expiration": "2016-12-08T21:12:53Z",
     "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpDHwXVPyJYBDm/
   gqX2Eeaq6P3DgTzgPg=="
   }
   ```

5. 建立到 Amazon Redshift 集群的安全套接字层 (SSL) 身份验证连接，并发送包含 `GetClusterCredentials` 响应中的用户名和密码的登录请求。请在用户名中包含 `IAM:` 或 `IAMA:` 前缀，例如，`IAM:temp_creds_user` 或 `IAMA:temp_creds_user`。

   Important

   将您的 SQL 客户端配置为需要 SSL。否则，如果您的 SQL 客户端自动尝试使用 SSL 进行连接，则可能会在出现任何故障时回退到非 SSL。在这种情况下，首次连接尝试可能因凭证过期或无效而失败，随后的另一次连接尝试可能因连接不是 SSL 而失败。如果出现这种情况，第一条错误消息可能会丢失。有关使用 SSL 连接到集群的更多信息，请参阅配置连接的安全选项 (p. 217)。

6. 如果连接未使用 SSL，则连接尝试可能失败。
7. 集群将向 SQL 客户端发送 `authentication` 请求。
8. 随后，SQL 客户端会向集群发送临时密码。
9. 如果密码有效且尚未到期，集群将完成连接。

授权 Amazon Redshift 代表您访问其他 Amazon 服务

某些 Amazon Redshift 功能要求 Amazon Redshift 代表您访问其他 Amazon 服务。例如，COPY 和 UNLOAD 命令可使用 Simple Storage Service（Amazon S3）存储桶将数据加载或卸载到您的 Amazon Redshift 集群中。CREATE EXTERNAL FUNCTION 命令可以使用标量 Lambda 用户定义的函数 (UDF) 调用 Amazon Lambda 函数。Amazon Redshift Spectrum 可以在 Amazon Athena 或 Amazon Glue 中使用数据目录。要让您的 Amazon Redshift 集群代表您执行操作，请为这些集群提供安全凭证。提供安全凭证的首

选方法是指定一个 Amazon Identity and Access Management (IAM) 角色。对于 COPY 和 UNLOAD，您可以提供 Amazon 访问密钥。

接下来，了解如何创建具有访问其他 Amazon 服务的适当权限的 IAM 角色。当您执行 Amazon Redshift 命令时，还需要将该角色与您的集群关联并指定角色的 Amazon Resource Name (ARN)。有关更多信息，请参阅使用 IAM 角色授权 COPY、UNLOAD、CREATE EXTERNAL FUNCTION 和 CREATE EXTERNAL SCHEMA 操作 (p. 430)。

此外，超级用户还可以向特定用户和组授予 ASSUMEROLE 权限，以便为 COPY 和 UNLOAD 操作提供对角色的访问权限。有关更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的 GRANT。

创建 IAM 角色以允许 Amazon Redshift 集群访问 Amazon 服务

要创建 IAM 角色以允许您的 Amazon Redshift 集群代表您与其他 Amazon 服务通信，请执行以下步骤。本节中使用的值是示例，您可以根据需要选择值。

要创建 IAM 角色以允许 Amazon Redshift 访问 Amazon 服务

1. 打开 IAM 控制台。
2. 在导航窗格中，选择 Roles (角色)。
3. 选择 Create role（创建角色）。
4. 选择 Amazon service（Amazon 服务），然后选择 Redshift。
5. 在 Select your use case 下，选择 Redshift - Customizable，然后选择 Next: Permissions。此时显示 Attach permissions policy 页面。
6. 对于使用 COPY 访问 Simple Storage Service（Amazon S3），作为示例，您可以使用 **`AmazonS3ReadOnlyAccess`** 并附加。要使用 COPY 或 UNLOAD 访问 Simple Storage Service（Amazon S3），我们建议您创建托管式策略，以相应地限制对所需存储桶和前缀的访问。对于读取和写入操作，我们建议强制执行最低权限，并仅限于 Amazon Redshift 要求的 Simple Storage Service（Amazon S3）存储桶和键前缀。

   要想为 CREATE EXTERNAL FUNCTION 命令调用 Lambda 函数，请添加 **`AWSLambdaRole`**。

   对于 Redshift Spectrum，除 Simple Storage Service（Amazon S3）访问以外，添加 **`AWSGlueConsoleFullAccess`** 或 **`AmazonAthenaFullAccess`**。

   选择 下一步：标签。
7. 此时将显示 Add tags (添加标签) 页面。您可以选择性地添加标签。选择 Next: Review (下一步：审核)。
8. 对于 Role name (角色名称)，键入一个角色名称，例如 **`RedshiftCopyUnload`**。选择 Create role（创建角色）。
9. 使用新角色的集群中的所有用户都可使用该角色。如需限制访问，只允许特定集群中的特定用户、或特定区域中的集群访问，请编辑该角色的信任关系。有关更多信息，请参阅限制对 IAM 角色的访问 (p. 426)。
10. 将角色与您的集群关联。您可以在创建集群时关联 IAM 角色，或将角色添加到现有集群中。有关更多信息，请参阅将 IAM 角色与集群相关联 (p. 431)。

    Note

    要限制对特定数据的访问，请使用授予所需最少权限的 IAM 角色。

限制对 IAM 角色的访问

预设情况下，对 Amazon Redshift 集群可用的 IAM 角色对集群上的所有用户都可用。您可选择将 IAM 角色限制为特定集群上的特定 Amazon Redshift 数据库用户，或限制为特定区域。

要仅允许特定数据库用户使用 IAM 角色，请执行以下步骤。

标识对 IAM 角色具有访问权限的特定数据库用户

1. 标识您的 Amazon Redshift 集群中的数据库用户的 Amazon Resource Name (ARN)。数据库用户的 ARN 采用以下格式：`arn:aws:redshift:region:account-id:dbuser:cluster-name/user-name`。
2. 通过以下网址打开 IAM 控制台：url="https://console.aws.amazon.com/。
3. 在导航窗格中，选择 Roles（角色）。
4. 选择要限制到特定 Amazon Redshift 数据库用户的 IAM 角色。
5. 选择 Trust Relationships 选项卡，然后选择 Edit Trust Relationship。允许 Amazon Redshift 代表您访问其他 Amazon 服务的新 IAM 角色具有以下信任关系：

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

6. 向信任关系的 `sts:AssumeRole` 操作部分添加一个条件以将 `sts:ExternalId` 字段限制为您指定的值。为您要授予对 IAM 角色的访问权限的每个数据库用户包含一个 ARN。外部 ID 可以是任何唯一的字符串。

   例如，以下信任关系指定只有区域 `user1` 中的集群 `user2` 上的数据库用户 `my-cluster` 和 `us-west-2` 有权使用此 IAM 角色。

```
{
  "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. 选择 Update Trust Policy。

将 IAM 角色限制为某个 Amazon 区域

您可将 IAM 角色限制为仅在某个特定 Amazon 区域中可访问。预设情况下，Amazon Redshift 的 IAM 角色不会限制到任何单一区域。

要按区域限制对 IAM 角色的使用，请执行以下步骤。

为 IAM 角色标识允许的区域

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/。
2. 在导航窗格中，选择 Roles（角色）。
3. 选择要用特定区域修改的角色。
4. 选择 Trust Relationships (信任关系) 选项卡，然后选择 Edit Trust Relationship (编辑信任关系)。允许 Amazon Redshift 代表您访问其他 Amazon 服务的新 IAM 角色具有以下信任关系：

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

5. 使用您要允许对其使用角色的特定区域的列表修改 `Service` 的 `Principal` 列表。`Service` 列表中的每个区域都必须采用以下格式：`redshift.region.amazonaws.com`。

   例如，以下编辑过的信任关系仅允许在 `us-east-1` 和 `us-west-2` 区域中使用 IAM 角色。

```
{
  "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. 选择 Update Trust Policy

在 Amazon Redshift 中串联 IAM 角色

当您将角色附加到集群时，集群可以代入该角色以您的名义访问 Simple Storage Service（Amazon S3）、Amazon Athena、Amazon Glue 和 Amazon Lambda。如果附加到集群的角色无法访问必要的资源，则可以串联到另一个角色 (可能属于其他账户)。然后，您的集群临时代入串联的角色来访问数据。您还可以通过串联角色来授予跨账户访问权限。链中的每个角色都会代入链中的下一个角色，直到集群承担位于链尾的角色。您可以关联的最大 IAM 角色数量受配额限制。有关更多信息，请参阅 Amazon Redshift 对象的配额 (p. 514)中的“Amazon Redshift 用于访问其他 Amazon 服务的集群 IAM 角色”。

例如，假设公司 A 想要访问属于公司 B 的 Simple Storage Service（Amazon S3）存储桶中的数据。公司 A 为 Amazon Redshift 创建一个名为 `RoleA` 的 Amazon 服务角色并将其附加到集群上。公司 B 创建一个名为 `RoleB` 的角色，该角色有权访问公司 B 存储桶中的数据。要访问公司 B 存储桶中的数据，公司 A 需要使用

串联 iam_role 和 RoleA 的 RoleB 参数运行 COPY 命令。在 COPY 操作的持续时间内，RoleA 将临时代入 RoleB 以访问 Simple Storage Service（Amazon S3）存储桶。

要串联角色，您可以在角色之间建立信任关系。代入其他角色的角色 (例如，RoleA) 必须具有允许其代入下一个串联的角色 (例如，RoleB) 的权限策略。反过来，传递权限的角色 (RoleB) 必须具有允许其将权限传递给上一个串联的角色 (RoleA) 的信任策略。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色。

链中的第一个角色必须是附加到集群的角色。第一个角色以及代入链中下一个角色的每个后续角色都必须具有包含特定语句的策略。该语句对 Allow操作以及 sts:AssumeRole 元素中的下一个角色的 Amazon Resource Name (ARN) 具有 Resource 效果。在我们的示例中，RoleA 具有允许其代入由 Amazon 账户 210987654321 所有的 RoleB 的以下权限策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1487639602000",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::210987654321:role/RoleB"
       }
    ]
}
```

传递给其他角色的角色必须与代入该角色的角色或拥有该角色的 Amazon 账户建立信任关系。在我们的示例中，RoleB 具有与 RoleA 建立信任关系的以下信任策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::role/RoleA"
      }
    }
  ]
}
```

以下信任策略与 RoleA、Amazon 账户 123456789012 的拥有者建立信任关系。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}
```

Note

要将角色串联授权限制给特定用户，请定义条件。有关更多信息，请参阅限制对 IAM 角色的访问 (p. 426)。

当您运行 UNLOAD、COPY、CREATE EXTERNAL FUNCTION 或 CREATE EXTERNAL SCHEMA 命令时，可以通过在 iam_role 参数中包括一个逗号分隔的角色 ARN 列表来串联角色。下面显示了在 iam_role 参数中串联角色的语法。

```
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

整个角色链用单引号括起来，不能包含空格。

在以下示例中，RoleA 将附加到属于 Amazon 账户 123456789012 的集群。属于账户 210987654321 的 RoleB 具有访问名为 s3://companyb/redshift/ 的存储桶的权限。以下示例将 RoleA 和 RoleB 进行串联以将数据卸载到 s3://companyb/redshift/ 存储桶。

```
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';
```

以下示例使用 COPY 命令加载已在上一个示例中卸载的数据。

```
copy venue
from 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

在以下示例中，CREATE EXTERNAL SCHEMA 使用串联的角色代入角色 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';
```

在以下示例中，CREATE EXTERNAL FUNCTION 使用串联的角色代入角色 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';
```

其他信息

有关更多信息，也请参阅使用 IAM 角色授权 COPY、UNLOAD、CREATE EXTERNAL FUNCTION 和 CREATE EXTERNAL SCHEMA 操作 (p. 430)。

使用 IAM 角色授权 COPY、UNLOAD、CREATE EXTERNAL FUNCTION 和 CREATE EXTERNAL SCHEMA 操作

您可使用 COPY 命令将数据加载（或导入）到 Amazon Redshift，使用 UNLOAD 命令从 Amazon Redshift 卸载（或导出）数据。您可以使用 CREATE EXTERNAL FUNCTION 命令创建用户定义的函数，这些函数从 Amazon Lambda 调用函数。

在使用 Amazon Redshift Spectrum 时，您要使用 CREATE EXTERNAL SCHEMA 命令来指定包含您的数据的 Simple Storage Service（Amazon S3）存储桶的位置。当您运行 COPY、UNLOAD 或 CREATE

EXTERNAL SCHEMA 命令时，会提供安全凭证。这些凭证授权您的 Amazon Redshift 集群在目标目的地 [如 Simple Storage Service（Amazon S3）存储桶] 中读取或写入数据。

运行 CREATE EXTERNAL FUNCTION 时，您可以使用 IAM 角色参数提供安全凭证。这些凭证授权您的 Amazon Redshift 集群从 Amazon Lambda 调用 Lambda 函数。提供安全凭证的首选方法是指定一个 Amazon Identity and Access Management (IAM) 角色。对于 COPY 和 UNLOAD，您可以提供 Amazon 访问密钥。有关创建 IAM 角色的信息，请参阅授权 Amazon Redshift 代表您访问其他 Amazon 服务 (p. 425)。

使用 IAM 角色的步骤如下所示：

- 创建要与您的 Amazon Redshift 集群结合使用的 IAM 角色。
- 将 IAM 角色与集群关联。
- 在调用 COPY、UNLOAD、CREATE EXTERNAL SCHEMA 或 CREATE EXTERNAL FUNCTION 命令时包含 IAM 角色的 ARN。

在本主题中，您将了解如何将 IAM 角色与 Amazon Redshift 集群关联。

将 IAM 角色与集群相关联

在您创建一个 IAM 角色以授权 Amazon Redshift 为您访问其他 Amazon 服务，必须将该角色与 Amazon Redshift 集群关联。在使用角色加载或卸载数据之前，您必须执行此操作。

将 IAM 角色与集群关联所需的权限

要将 IAM 角色与集群关联，IAM 用户必须具有针对该 IAM 角色的 `iam:PassRole` 权限。此权限允许管理员限制用户可关联到 Amazon Redshift 集群的 IAM 角色。

以下示例显示了一个 IAM policy，该策略可附加到 IAM 用户以允许该用户执行以下操作：

- 获取用户的账户拥有的所有 Amazon Redshift 集群的详细信息。
- 将三个 IAM 角色中的任一角色与两个 Amazon Redshift 集群中的任一集群关联。

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

当 IAM 用户具有相应的权限后，该用户可以将 IAM 角色与 Amazon Redshift 集群关联。随后，IAM 角色可以与 COPY 或 UNLOAD 命令或其他 Amazon Redshift 命令一起使用。

有关 IAM 策略的更多信息，请参阅 IAM 用户指南中的 IAM 策略概览。

管理 IAM 角色与集群的关联

您可以在创建集群时将该 IAM 角色与 Amazon Redshift 集群关联。或者您可以修改现有集群并添加或删除一个或多个 IAM 角色关联。

请注意以下事项：

- 您可以关联的最大 IAM 角色数量受配额限制。
- 一个 IAM 角色可与多个 Amazon Redshift 集群关联。
- 仅当 IAM 角色和集群都归同一 Amazon 账户拥有时，该角色才能与 Amazon Redshift 集群关联。

使用控制台管理 IAM 角色关联

您可通过以下程序，借助控制台管理集群的 IAM 角色关联。

要管理 IAM 角色关联

1. 登录到Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）,然后选择要更新的集群。
3. 对于 Actions（操作），选择 Manage IAM roles（管理 IAM 角色）以显示与集群关联的当前列表 IAM 角色。
4. 在 Manage IAM roles（管理 IAM 角色）页面上，选择要添加的可用 IAM 角色，然后选择 Add IAM role（添加 IAM 角色）。
5. 选择 Done（完成）以保存您的更改。

使用 Amazon CLI 管理 IAM 角色关联

您可以使用以下方法，通过 Amazon CLI 管理集群的 IAM 角色关联。

使用 Amazon CLI 将 IAM 角色与集群关联

要在创建集群后将 IAM 角色与其关联，请在 `--iam-role-arns` 命令的 `create-cluster` 参数中指定 IAM 角色的 Amazon Resource Name (ARN)。调用 `create-cluster` 命令时可以添加的最大 IAM 角色数量受配额限制。

将 IAM 角色与 Amazon Redshift 集群关联和解除两者之间的关联是一个异步过程。您可通过调用 `describe-clusters` 命令获取所有 IAM 角色集群关联的状态。

以下示例将两个 IAM 角色与新创建的名为 `my-redshift-cluster` 的集群关联。

```
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"
```

要将 IAM 角色与现有 Amazon Redshift 集群关联，请在 `modify-cluster-iam-roles` 命令的 `--add-iam-roles` 参数中指定 IAM 角色的 Amazon Resource Name (ARN)。调用 `modify-cluster-iam-roles` 命令时可以添加的最大 IAM 角色数量受配额限制。

以下示例将一个 IAM 角色与名为 `my-redshift-cluster` 的现有集群关联。

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier "my-redshift-cluster" \
    --add-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

使用 Amazon CLI 将 IAM 角色与集群取消关联

要取消 IAM 角色与集群的关联，请在 `modify-cluster-iam-roles` 命令的 `--remove-iam-roles` 参数中指定 IAM 角色的 ARN。`modify-cluster-iam-roles`调用 `modify-cluster-iam-roles` 命令时可以删除的最大 IAM 角色数量受配额限制。

以下示例从名为 `123456789012` 的集群中删除 `my-redshift-cluster` Amazon 账户的 IAM 角色的关联。

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier "my-redshift-cluster" \
    --remove-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

使用 Amazon CLI 列出集群的 IAM 角色关联

要列出与 Amazon Redshift 集群关联的所有 IAM 角色以及 IAM 角色关联的状态，请调用 `describe-clusters` 命令。与集群关联的每个 IAM 角色的 ARN 将在 `IamRoles` 列表中返回，如以下示例输出所示。

已与集群关联的角色将显示状态 `in-sync`。正在与集群关联的角色将显示状态 `adding`。正与集群解除关联的角色将显示状态 `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"
                }
            ],
            ...
        }
    ]
}
```

有关使用 Amazon CLI 的更多信息，请参阅 Amazon CLI 用户指南。

创建一个 IAM 角色作为 Amazon Redshift 的默认角色

当您通过 Redshift 控制台创建 IAM 角色时，Amazon Redshift 以编程方式在您的 Amazon Web Services 账户 中创建角色，并自动附上现有的 Amazon 托管式策略。这种方法意味着您可以留在 Redshift 控制台上，而不必切换到 IAM 控制台创建角色。要更精细地控制在 Amazon Redshift 控制台上创建的现有 IAM 角色的权限，您可以将自定义托管式策略附加至 IAM 角色。

在控制台上创建 IAM 角色概述

当您使用 Amazon Redshift 控制台创建 IAM 角色时，Amazon Redshift 会跟踪所有通过控制台创建的 IAM 角色。Amazon Redshift 预先选择最新的默认 IAM 角色来创建所有新集群，以及从快照中还原集群。

通过 Amazon Redshift 控制台创建一个 IAM 角色，该角色拥有的策略包括可运行 SQL 命令的权限。这些命令包括 COPY、UNLOAD、CREATE EXTERNAL FUNCTION、CREATE EXTERNAL TABLE、CREATE EXTERNAL SCHEMA、CREATE MODEL 或 CREATE LIBRARY。或者，您可以更精细地控制用户通过创建自定义策略并将其附加到 IAM 角色来进行对 Amazon 资源的访问。

当您使用控制台创建 IAM 角色并将其设置为集群的默认角色时，您无需提供 IAM 角色的 Amazon Resource Name（ARN）即可执行身份验证和授权。

在 IAM 控制台上创建角色。

您通过控制台为集群创建的 IAM 角色具有自动附加的 `AmazonRedshiftAllCommandsFullAccess` 托管式策略。此 IAM 角色允许 Amazon Redshift 为 Amazon IAM 账户中的资源复制、卸载、查询和分析数据。托管式策略提供对以下操作的访问权限：COPY、UNLOAD、CREATE EXTERNAL FUNCTION、CREATE EXTERNAL SCHEMA、CREATE MODEL 和 CREATE LIBRARY。此策略还授予权限，以便为相关 Amazon 服务运行 SELECT 语句，例如Simple Storage Service（Amazon S3）、Amazon CloudWatch Logs、Amazon SageMaker 和 Amazon Glue。

CREATE EXTERNAL FUNCTION、CREATE EXTERNAL SCHEMA、CREATE MODEL 和CREATE LIBRARY 命令都有 `default` 关键字。对于这些命令的此关键字，Amazon Redshift 使用在命令运行时与集群关联的默认 IAM 角色。您可以运行 DEFAULT_IAM_ROLE 命令来检查附加至集群的当前默认 IAM 角色。

要控制已有 IAM 角色（设置为 Redshift 集群默认角色）的访问权限，请使用 AUSMEROLE 权限。当数据库用户和组运行前面列出的命令时，此访问控制适用于这些数据库用户和组。向用户或组授予 IAM 角色的 ASSUMEROLE 权限后，该用户或组可以在运行命令时代入该角色。ASSUMEROLE 权限允许您根据需要授予用户相应命令的访问权限。

您可以使用 Amazon Redshift 控制台执行以下操作：

- 默认创建 IAM 角色 (p. 437)
- 从集群中删除 IAM 角色 (p. 438)
- 将 IAM 角色与集群关联 (p. 438)
- 将 IAM 角色设置为默认角色 (p. 438)
- 将 IAM 角色设置为不再是集群的默认角色 (p. 438)

AmazonRedshiftAllCommandsFullAccess 托管式策略的权限

以下示例显示了 AmazonRedshiftAllCommandsFullAccess 中的权限：托管式策略允许对集群默认的角色（IAM 角色）执行某些操作。附加了权限策略的 IAM 角色可以授权用户或组进行某些操作，以及不允许某些操作。使用这些权限，您可以从 Simple Storage Service（Amazon S3）运行 COPY 命令、运行 UNLOAD，然后使用 CREATE MODEL 命令。

```
{
            "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*/*"
            ]
}
```

以下示例显示了 AmazonRedshiftAllCommandsFullAccess 中的权限：托管式策略允许对集群默认的角色（IAM 角色）执行某些操作。附加了权限策略的 IAM 角色可以授权用户或组进行某些操作，以及不允许某些操作。如果有以下权限，您可以运行 CREATE EXTERNAL FUNCTION 命令。

```
{
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": "arn:aws:lambda:*:*:function:*redshift*"
}
```

以下示例显示了 AmazonRedshiftAllCommandsFullAccess 中的权限：托管式策略允许对集群默认的角色（IAM 角色）执行某些操作。附加了权限策略的 IAM 角色可以授权用户或组进行某些操作，以及不允许某些操作。如果具有以下权限，您可以运行 Amazon Redshift Spectrum 所需的 CREATE EXTERNAL SCHEMA 和 CREATE EXTERNAL TABLE 命令。

```
{
```

```
            "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*"
            ]
}
```

以下示例显示了 AmazonRedshiftAllCommandsFullAccess 中的权限：托管式策略允许对集群默认的角色（IAM 角色）执行某些操作。附加了权限策略的 IAM 角色可以授权用户或组进行某些操作，以及不允许某些操作。如果具有以下权限，您可以使用联合查询运行 CREATE EXTERNAL SCHEMA 命令。

```
{
            "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"
                }
            }
},
```

使用控制台管理为集群创建的 IAM 角色

要创建、修改和删除从 Amazon Redshift 控制台创建的 IAM 角色，请使用控制台上的 Clusters（集群）部分。

默认创建 IAM 角色

在控制台上，您可以为集群创建一个 IAM 角色，并自动为该角色附上 `AmazonRedshiftAllCommandsFullAccess` 策略。这个新角色让 Amazon Redshift 能够在您的 IAM 角色中复制、加载、查询和分析 Amazon 资源的数据。

一个集群只能有一个默认的 IAM 角色。如果现有 IAM 角色已设置为默认角色，当您创建另一个 IAM 角色并设置为集群默认角色时，新的 IAM 角色将替换现有的 IAM 角色成为默认角色。

创建新集群和 IAM 角色，并设置 IAM 角色为新集群的默认角色。

1. 登录Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。列出您的账户在当前 Amazon Web Services 区域 区域中的集群。列表中的各个列中显示了每个集群的一部分属性。
3. 选择 Create cluster（创建集群）以创建集群。
4. 按照控制台页面上的说明进行操作，为 Cluster configuration (集群配置) 输入属性。

   选择以下方法之一以调整集群的大小：

   Note

   以下步骤假定 Amazon 区域支持 RA3 节点类型。有关支持 RA3 节点类型的Amazon区域的列表，请参阅 Amazon Redshift 集群管理指南中的 RA3 节点类型概览。

   - 如果您的Amazon区域支持 RA3 节点类型，请选择 Production（生产）或 Free trial（免费试用）回答问题您打算将此集群用于什么？

     如果您的组织符合条件，您或许能够在 Amazon Redshift 免费试用计划下创建集群。为此，请选择 Free trial（免费试用）创建具有 dc2.large 节点类型的配置。有关选择免费试用的更多信息，请参阅 Amazon Redshift 免费试用。
   - 如果您不知道要将集群调整到多大，请选择 Help me choose（帮我选择）。执行此操作将启动大小调整计算器，该计算器将询问您有关计划存储在数据仓库中的数据的大小和查询特性的问题。

     如果您知道集群所需的大小（即节点类型和节点数），请选择 I'll choose（我会选择）。然后选择 Node Type（节点类型）和 Nodes（节点）数量来确定集群规模。
5. （可选）选择 Load sample data（加载示例数据），将示例数据集加载到您的 Amazon Redshift 集群，以便开始使用查询编辑器查询数据。

   如果您在防火墙的后面，则数据库端口必须是接受入站连接的开放端口。
6. 按照控制台页面上的说明操作，为 Cluster configuration（集群配置）输入属性。
7. 在 Cluster permissions（集群权限）下，从 Manage IAM roles（管理 IAM 角色）选择 Create IAM role（创建 IAM 角色）。
8. 指定一个 Simple Storage Service（Amazon S3）存储桶，让 IAM 角色通过以下方法访问：

   - 选择 No additional Simple Storage Service（Amazon S3）bucket [没有额外 Simple Storage Service（Amazon S3）存储桶]，在不指定特定 Simple Storage Service（Amazon S3）存储桶的情况下创建 IAM 角色。
   - 选择 Any Simple Storage Service（Amazon S3）bucket [任何 Simple Storage Service（Amazon S3）存储桶]，允许有权限访问您的 Amazon Redshift 集群的用户，也可以访问在您的 Amazon Web Services 账户 中的任何 Simple Storage Service（Amazon S3）存储桶及其内容.
   - 选择 Specific Simple Storage Service（Amazon S3）buckets [特定 Simple Storage Service（Amazon S3）存储桶]，为创建的 IAM 角色指定一个或多个 Simple Storage Service（Amazon S3）存储桶以供访问。然后从表中选择一个或多个 Simple Storage Service（Amazon S3）存储桶。
9. 选择 Create IAM role as default（创建 IAM 角色作为默认角色）。Amazon Redshift 会自动创建 IAM 角色并将其设置为集群的默认角色。

10. 选择 Create cluster（创建集群）以创建集群。集群可能需要几分钟才可以使用。

从集群中删除 IAM 角色

您可以从集群中移除一个或多个 IAM 角色。

从集群中删除 IAM 角色

1. 登录Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。列出您的账户在当前 Amazon Web Services 区域 区域中的集群。列表中的各个列中显示了每个集群的一部分属性。
3. 选择要从中删除的 IAM 角色的集群的名称。
4. 在 Cluster permissions（集群权限）下，选择要从集群中删除的一个或多个 IAM 角色。
5. 从 Manage IAM roles（管理 IAM 角色）中选择 Remove IAM roles（删除 IAM 角色）。

将 IAM 角色与集群关联

您可以将一个或多个 IAM 角色与集群关联。

将 IAM 角色与您的集群关联

1. 登录Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。列出您的账户在当前 Amazon Web Services 区域 区域中的集群。列表中的各个列中显示了每个集群的一部分属性。
3. 选择 IAM 角色需要关联的集群。
4. 在 Cluster permissions（集群权限）下，选择要与集群关联的一个或多个 IAM 角色。
5. 从 Manage IAM roles（管理 IAM 角色）中选择 Associate IAM roles（关联 IAM 角色）。
6. 选择一个或多个 IAM 角色并与您的集群关联。
7. 选择 Associate IAM role（关联 IAM 角色）。

将 IAM 角色设置为默认角色

您可以将 IAM 角色设置为集群的默认角色。

将 IAM 角色设置为集群的默认角色

1. 登录Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。列出您的账户在当前 Amazon Web Services 区域 区域中的集群。列表中的各个列中显示了每个集群的一部分属性。
3. 选择要为其设置默认 IAM 角色的集群。
4. 在 Cluster permissions（集群权限）下，从 Associated IAM roles（关联 IAM 角色）中选择要设置为集群默认角色的 IAM 角色。
5. 在 Set default（设置默认值）下选择 Make default（设为默认）。
6. 系统提示时，选择 Set default（设置默认值）以确认设置指定的 IAM 角色为默认角色。

将 IAM 角色设置为不再是集群的默认角色

您可以使 IAM 角色不再成为集群的默认角色。

清除 IAM 角色作为集群默认角色的设置

1. 登录Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群）。列出您的账户在当前 Amazon Web Services 区域 区域中的集群。列表中的各个列中显示了每个集群的一部分属性。
3. 选择 IAM 角色需要关联的集群。
4. 在 Cluster permissions（集群权限）下，从 Associated IAM roles（关联 IAM 角色）中选择要设置为集群默认角色的 IAM 角色。
5. 在 Set default（设置默认值）下，选择 Clear default（清除默认值）。
6. 系统提示时，选择 Clear default（清除默认值）以确指定的 IAM 角色不再是默认角色。

使用 Amazon CLI 管理在集群上创建的 IAM 角色

您可以使用 Amazon CLI 管理在集群上创建的 IAM 角色

创建默认设置为 IAM 角色的 Amazon Redshift 集群

要创建 Amazon Redshift 集群并将 IAM 角色设为其默认角色，请使用 `aws redshift create-cluster` Amazon CLI 命令。

以下 Amazon CLI 命令创建一个 Amazon Redshift 集群和名为 myrole1 的 IAM 角色。这个 Amazon CLI 命令还将 myrole1 设置为集群的默认值。

```
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'
```

以下代码片段是一个反应示例。

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

向 Amazon Redshift 集群添加一个或多个 IAM 角色

要添加与集群关联的一个或多个 IAM 角色，请使用 `aws redshift modify-cluster-iam-roles` Amazon CLI 命令。

以下 Amazon CLI 命令将 `myrole3` 和`myrole4` 添加到集群。

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3'
 'arn:aws:iam::012345678910:role/myrole4'
```

以下代码片段是一个反应示例。

```
{
    "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"
            }
        ],
        ...
    }
}
```

从 Amazon Redshift 集群中删除一个或多个 IAM 角色

要删除与集群关联的一个或多个 IAM 角色，请使用 `aws redshift modify-cluster-iam-roles` Amazon CLI 命令。

以下 Amazon CLI 命令从集群中删除 `myrole3` 和 `myrole4`。

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --remove-iam-roles 'arn:aws:iam::012345678910:role/myrole3'
 'arn:aws:iam::012345678910:role/myrole4'
```

以下代码片段是一个反应示例。

```
{
    "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"
            }
        ],
        ...
    }
}
```

将关联的 IAM 角色设置为集群的默认角色

要将关联的 IAM 角色设置为集群的默认角色，请使用 `aws redshift modify-cluster-iam-roles` Amazon CLI 命令。

以下 Amazon CLI 命令集设置 `myrole2` 为集群默认角色。

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole2'
```

以下代码片段是一个反应示例。

```
{
    "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"
            }
        ],
        ...
    }
}
```

将未关联的 IAM 角色设置为集群的默认角色

要将未关联的 IAM 角色设置为集群的默认角色，请使用 `aws redshift modify-cluster-iam-roles` Amazon CLI 命令。

以下 Amazon CLI 命令把 `myrole2` 添加到 Amazon Redshift 集群，然后将其设置为集群的默认角色。

```
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'
```

以下代码片段是一个反应示例。

```
{
    "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"
            }
        ],
        ...
    }
}
```

从快照还原集群，并将 IAM 角色设置为其默认角色

从快照还原集群时，您可以关联现有 IAM 角色，也可以创建一个新角色并将其设置为集群的默认角色。

要从快照还原 Amazon Redshift 集群，并将 IAM 角色设置为集群默认角色，请使用 `aws redshift restore-from-cluster-snapshot` Amazon CLI 命令。

以下 Amazon CLI 命令从快照还原集群，并将 `myrole2` 设置为集群默认角色。

```
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'
```

以下代码片段是一个反应示例。

```
{
    "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"
            }
        ],
        ...
    }
}
```

Amazon Redshift 中的日志记录和监控

监控是保持 Amazon Redshift 和您的 Amazon 解决方案的可靠性、可用性和性能的重要方面。您可以从 Amazon 解决方案的各个部分收集监控数据，以便您可以更轻松地调试多点故障（如果发生）。Amazon 提供了多种工具来监控您的 Amazon Redshift 资源并对潜在事件做出响应：

Amazon CloudWatch 警报

使用 Amazon CloudWatch 警报，您可以在指定时间段内监控某个指标。如果指标超过给定阈值，则会向 Amazon SNS 主题或 Amazon Auto Scaling 策略发送通知。CloudWatch 警报将不会调用操作，因为这些操作处于特定状态。而是必须在状态已改变并在指定的若干个时间段内保持不变后才调用。有关更多信息，请参阅管理警报 (p. 499)。有关 指标的列表，请参阅 使用 CloudWatch 指标监控 Amazon Redshift (p. 472)。

Amazon CloudTrail 日志

CloudTrail 提供了 IAM 用户、角色或 Amazon 服务在 Amazon Redshift 中所执行的 API 操作的记录。使用 CloudTrail 收集的信息，您可以确定向 Amazon Redshift 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。有关更多信息，请参阅使用 Cloudtrail 进行日志记录 (p. 450)。

数据库审计日志记录

Amazon Redshift 记录您的数据库中的连接和用户活动相关信息。这些日志有助于您监控数据库以确保安全并进行故障排除，该流程称为数据库审计。可以存储日志的位置包括：

- Amazon S3 存储桶 - 这为负责监控数据库中活动的用户提供了访问权限以及数据安全功能。
- Amazon CloudWatch - 您可以使用 CloudWatch 中内置的功能（例如可视化功能和设置操作）查看审计日志记录数据。

主题

- Amazon Redshift 日志 (p. 443)
- 启用日志记录 (p. 446)
- 将审计日志发送到 Amazon CloudWatch (p. 446)
- 在 Simple Storage Service (Amazon S3) 中管理日志文件 (p. 447)
- Simple Storage Service (Amazon S3) 中的 Amazon Redshift 审计日志记录故障排除 (p. 449)
- 使用 Amazon CloudTrail 记录 Amazon Redshift API 调用 (p. 450)
- 使用控制台配置审计 (p. 450)
- 使用 Amazon CLI 和 Amazon Redshift API 配置日志记录 (p. 450)

Amazon Redshift 日志

Amazon Redshift 在以下日志文件中记录信息：

- 连接日志 – 记录身份验证尝试以及连接与断开连接。

- 用户日志 – 记录与数据库用户定义更改相关的信息。
- 用户活动日志 – 记录在数据库中运行之前的每个查询。

连接日志和用户日志主要用于实现安全性。您可以使用连接日志来监控连接到数据库的用户信息以及相关的连接信息。这些信息可能是他们的 IP 地址、发出请求的时间以及使用的身份验证类型等。您可以使用用户日志来监控数据库用户定义更改。

用户活动日志主要用于进行故障排除。它会跟踪用户及系统在数据库中执行的查询类型的相关信息。

连接日志和用户日志均对应于数据库的系统表中存储的信息。您可以使用系统表获取相同的信息，但日志文件可提供更简单的检索和查看机制。日志文件依赖 Simple Storage Service（Amazon S3）权限（而非数据库权限）针对表执行查询。此外，通过查看日志文件中的信息（而非查询系统表），您可以减少与数据库互动产生的任何影响。

Note

日志文件没有基本系统日志表 STL_USERLOG 和 STL_CONNECTION_LOG 那么新。早于 (但不包括) 最新记录的记录将被复制到日志文件。

连接日志

记录身份验证尝试以及连接与断开连接。下表介绍了连接日志中的信息。有关这些字段的更多信息，请参阅《Amazon Redshift 数据库开发人员指南》中的 STL_CONNECTION_LOG。

列名称	描述
event	连接或身份验证事件。
recordtime	事件发生的时间。
remotehost	远程主机的名称或 IP 地址。
remoteport	远程主机的端口号。
pid	与语句关联的进程 ID。
dbname	数据库名称。
username	用户名。
authmethod	身份验证方法。
duration	连接的持续时间（单位为微秒）。
sslversion	安全套接字层 (SSL) 版本。
sslcipher	SSL 密码。
mtu	最大传输单元 (MTU)。
sslcompression	SSL 压缩类型。
sslexpansion	SSL 扩展类型。
iamauthguid	Amazon CloudTrail 请求的 Amazon Identity and Access Management（IAM）身份验证 ID。
application_name	会话应用程序的初始名称或更新名称。
driver_version	从第三方 SQL 客户端工具连接到 Amazon Redshift 集群的 ODBC 或 JDBC 驱动程序版本。

列名称	描述
os_version	连接到 Amazon Redshift 集群的客户端计算机上的操作系统版本。
plugin_name	用于连接到您的 Amazon Redshift 集群的插件名称。
protocol_version	Amazon Redshift 驱动程序在与服务器建立连接时使用的内部协议版本。
sessionid	当前会话的全局唯一标识符。

用户日志

记录数据库用户的以下更改的详细信息。

- 创建用户
- 删除用户
- 更改用户（重命名）
- 更改用户（更改属性）

列名称	描述
userid	受更改影响的用户的 ID。
username	受更改影响的用户的用户名称。
oldusername	对于重命名操作，这指的是原始用户名称。对于任何其他操作，此字段为空。
操作	发生的操作。有效值： • 更改 • 创建 • Drop • 重命名
usecreatedb	如果为 true (1)，则表示用户具有创建数据库的权限。
usesuper	如果为 true (1)，则表示用户为超级用户。
usecatupd	如果为 true (1)，则表示用户可更新系统目录。
valuntil	密码到期日期。
pid	进程 ID。
xid	事务 ID。
recordtime	查询开始的时间（采用 UTC 表示）。

用户活动日志

记录在数据库中运行之前的每个查询。

列名称	描述
recordtime	事件发生的时间。

列名称	描述
db	数据库名称。
user	用户名。
pid	与语句关联的进程 ID。
userid	用户 ID。
xid	事务 ID。
query	日志前缀：后跟查询的文字，包括换行符。

启用日志记录

在 Amazon Redshift 中，原定设置情况下审计日志记录处于未启用状态。当您针对集群打开日志记录时，Amazon Redshift 将日志导出到 Amazon CloudWatch 中，或创建日志并将其上载到 Simple Storage Service (Amazon S3) 中，以捕获从启用审计日志记录的时间到当前时间的数据。每个日志记录更新都是以前日志的延续。

在 CloudWatch 或 Simple Storage Service (Amazon S3) 中存储审计日志记录是一个可选流程。记录到数据表并非可选流程，而会自动发生。有关系统表日志记录的更多信息，请参阅 Amazon Redshift 数据库开发人员指南中的系统表参考。

您可以通过使用 Amazon Web Services Management Console、Amazon Redshift API 参考或 Amazon Command Line Interface (Amazon CLI) 一起启用连接日志、用户日志以及用户活动日志。对于用户活动日志，您还必须启用 `enable_user_activity_logging` 数据库参数。如果您仅启用审计日志记录功能，但不启用相关参数，则数据库审计日志将仅为连接日志和用户日志记录信息，而不为用户活动日志记录信息。`enable_user_activity_logging` 参数预设情况下未启用 (`false`)。您可以将它设置为 `true` 以启用用户活动日志。有关更多信息，请参阅Amazon Redshift 参数组 (p. 299)。

> Note
>
> 目前，您只能使用 Simple Storage Service（Amazon S3）托管密钥（SSE-S3）加密（AES-256）进行审计日志记录。

将审计日志发送到 Amazon CloudWatch

在对 CloudWatch 启用日志记录后，Amazon Redshift 将集群连接、用户和用户活动日志数据导出到 Amazon CloudWatch Logs 日志组。就 架构 而言，日志数据不会改变。CloudWatch 专为监控应用程序而构建，您可以使用它来执行实时分析或将其设置为采取措施。还可以使用 Amazon CloudWatch Logs 在持久性存储中存储日志记录。

使用 CloudWatch 查看日志是在 Simple Storage Service (Amazon S3)中存储日志文件的推荐替代方法。它不需要太多的配置，而且可能符合您的监控要求，尤其是如果您已经使用它来监控其他服务和应用程序。

Amazon CloudWatch 中的日志组和日志事件

在选择要导出的 Amazon Redshift 日志后，您可以在 Amazon CloudWatch Logs 中监控日志事件。将使用以下前缀为 Amazon Redshift 无服务器自动创建新的日志组，其中 `log_type` 表示日志类型。

```
/aws/redshift/cluster/<cluster_name>/<log_type>
```

例如，如果您选择导出连接日志，则日志数据将存储在以下日志组中。

```
/aws/redshift/cluster/cluster1/connectionlog
```

使用日志流将日志事件导出到日志组。要在无服务器端点的日志事件中搜索信息，请使用 Amazon CloudWatch Logs 控制台、Amazon CLI 或 Amazon CloudWatch Logs API。有关搜索和筛选日志数据的信息，请参阅使用筛选条件从日志事件创建指标。

在 CloudWatch 中，您可以使用所提供的旨在实现粒度和灵活性的查询语法搜索日志数据。有关更多信息，请参阅 CloudWatch Logs Insights 查询语法。

迁移到 Amazon CloudWatch 审计日志记录

在任何情况下，如果您要向 Simple Storage Service (Amazon S3) 发送日志并更改配置（例如向 CloudWatch 发送日志），保留在 Simple Storage Service (Amazon S3) 中的日志都不会受到影响。您仍可以在日志数据所在的 Simple Storage Service (Amazon S3) 存储桶中查询日志数据。

在 Simple Storage Service (Amazon S3) 中管理日志文件

Simple Storage Service（Amazon S3）中的 Amazon Redshift 日志文件的数量和大小在很大程度上取决于您集群中的活动。如果您有一个活动的集群生成了大量日志，则 Amazon Redshift 可能会更频繁地生成日志文件。对于同一类活动，您可能有一系列日志文件，例如同一个小时有多个连接日志。

当 Amazon Redshift 使用 Simple Storage Service (Amazon S3) 存储日志时，您需要为在 Simple Storage Service (Amazon S3) 中使用的存储支付相应费用。在对 Simple Storage Service (Amazon S3) 配置日志记录之前，应计划需存储日志文件的时长。在此过程中，请确定何时可根据审计需求删除或归档日志文件。您制定的计划在很大程度上取决于您存储的数据类型，例如需满足合规性或法规要求的数据。有关 Simple Storage Service（Amazon S3）定价的更多信息，请转至 Amazon Simple Storage Service（S3）定价。

Amazon Redshift 审计日志记录的存储桶权限

当您对 Simple Storage Service (Amazon S3) 启用日志记录时，Amazon Redshift 会收集日志记录信息并将其上载到 Simple Storage Service (Amazon S3) 中存储的日志文件。您可以使用现有存储桶或新存储桶。Amazon Redshift 需要对存储桶具备以下 IAM 权限：

- `s3:GetBucketAcl` 该服务要求对 Simple Storage Service（Amazon S3）存储桶具备读取权限，以便可以识别存储桶拥有者。
- `s3:PutObject` 该服务要求具备放置对象权限，以便上载日志。此外，启用日志记录的 IAM 用户或 IAM 角色必须具有对 Simple Storage Service（Amazon S3）存储桶的 `s3:PutObject` 权限。每次上传日志时，该服务就会确定当前存储桶拥有者与启用日志记录时的存储桶拥有者是否一致。如果这些拥有者不匹配，您将收到一条错误。

如果启用审计日志记录时，您选择了创建新存储桶的选项，则会对其应用正确的权限。不过，如果您在 Simple Storage Service（Amazon S3）中创建自己的存储桶或使用现有存储桶，请确保添加包含存储桶名称的存储桶策略。日志使用服务主体凭证传送。对于大多数 Amazon Web Services 区域，您可添加 Redshift 服务主体名称，*`redshift t.amazonaws.com`*。

Note

中国（北京）区域的 ARN 格式使用 `aws-cn` 标识符，而不是 `aws` 标识符，如以下策略示例所示。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
   "Sid": "Put bucket policy needed for audit logging",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws-cn:iam::111890595117:user/logs"
   },
   "Action": "s3:PutObject",
   "Resource": "arn:aws-cn:s3:::AuditLogs/*"
  },
```

```
  {
   "Sid": "Get bucket policy needed for audit logging ",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws-cn:iam::111890595117:user/logs"
   },
   "Action": "s3:GetBucketAcl",
   "Resource": "arn:aws-cn:s3:::AuditLogs"
  }
 ]
}
```

该存储桶策略使用以下格式。*ServiceName* 和 *BucketName* 是您自己的值的占位符。还可在存储桶策略中指定关联的操作和资源。

```
{
    "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/*"
            ]
        }
    ]
}
```

以下示例就是针对美国东部（弗吉尼亚北部）区域的存储桶策略，该存储桶名为 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/*"
            ]
        }
    ]
}
```

原定设置情况下未启用的区域（也称为“选择加入”区域）需要特定于区域的服务主体名称。对于这些内容，服务主体名称包括区域，格式为 redshift.*region*.amazonaws.com。例如，*redshift.ap-*

east-1.amazonaws.com 针对亚太地区（香港）区域。有关原定设置情况下未启用的区域列表，请参阅《Amazon 一般参考》中的管理 Amazon Web Services 区域。

Note

特定于区域的服务主体名称与集群所在的区域对应。

日志文件的最佳实践

当 Redshift 将日志文件上载到 Simple Storage Service（Amazon S3）时，可以分段上载大型文件。如果分段上载不成功，则文件的一部分可能会保留在 Simple Storage Service（Amazon S3）存储桶中。这可能会导致额外的存储成本，因此了解什么情况下分段上载会失败非常重要。有关审计日志的分段上载的详细说明，请参阅使用分段上载来上载和复制对象和中止分段上载。

有关创建 Simple Storage Service（Amazon S3）存储桶和添加存储桶策略的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的创建存储桶和编辑存储桶权限。

Amazon Redshift 审计日志记录的存储桶结构

预设情况下，Amazon Redshift 通过使用下列存储桶和对象结构在 Simple Storage Service（Amazon S3）存储桶中整理日志文件：

```
AWSLogs/AccountID/ServiceName/Region/Year/Month/Day/AccountID_ServiceName_Region_ClusterN
```

例如：`AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

如果您提供 Simple Storage Service（Amazon S3）键前缀，则该前缀放在密钥开头。

例如，如果指定前缀 myprefix：`myprefix/AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

Simple Storage Service（Amazon S3）键前缀不得超过 512 个字符。其中不得包含空格（ ）、双引号（“）、单引号（‘）、反斜杠（\）。此外还有很多不得使用的特殊字符和控制字符。这些字符的十六进制代码如下：

- x00 – x20
- x 22
- x 27
- x5c
- x7f 或更大

Simple Storage Service (Amazon S3) 中的 Amazon Redshift 审计日志记录故障排除

Amazon Redshift 审计日志记录可能会因如下原因而中断：

- Amazon Redshift 无权将日志上载到 Simple Storage Service（Amazon S3）存储桶中。验证相应存储桶是否配置了适当的 IAM 策略。有关更多信息，请参阅Amazon Redshift 审计日志记录的存储桶权限 (p. 447)。
- 存储桶拥有者发生变化。当 Amazon Redshift 上载日志时，它会验证存储桶拥有者与启用日志记录时的存储桶拥有者是否相同。如果存储桶拥有者发生变化，则在您配置其他存储桶以用于审计日志记录之前，Amazon Redshift 不会上载日志。
- 找不到存储桶。如果相应存储桶在 Simple Storage Service（Amazon S3）中已被删除，则 Amazon Redshift 无法上载日志。您必须重新创建该存储桶，或对 Amazon Redshift 进行配置以将日志上载到其他存储桶。

使用 Amazon CloudTrail 记录 Amazon Redshift API 调用

Amazon Redshift 与 Amazon CloudTrail 集成，后者是在 Amazon Redshift 中提供用户、角色或 Amazon 服务所采取操作的记录的服务。CloudTrail 将 Amazon Redshift 的所有 API 调用作为事件捕获。有关 Amazon Redshift 与 Amazon CloudTrail 集成的更多信息，请参阅使用 CloudTrail 进行日志记录。

您可以将 CloudTrail 与 Amazon Redshift 数据库审计日志记录一起使用，也可以单独使用前者。

要了解有关 CloudTrail 的更多信息，请参阅 Amazon CloudTrail 用户指南。

使用控制台配置审计

配置 Amazon Redshift 以导出审计日志数据。日志可以导出到 CloudWatch，也可以作为文件导出到 Simple Storage Service (Amazon S3) 存储桶。

使用控制台启用审计日志记录

控制台步骤

要启用集群的审计日志记录

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后选择要更新的集群。
3. 选择 Properties（属性）选项卡。在 Database configurations（数据库配置）面板中，依次选择 Edit（编辑）和 Edit audit logging（编辑审计日志记录）。
4. 在 Edit audit logging（编辑审计日志记录）页上，选择 Turn on（打开）并选择 S3 bucket（S3 存储桶）或 CloudWatch。我们建议使用 CloudWatch，因为管理很简单，而且它具有实现数据可视化的有用功能。
5. 选择要导出的日志。
6. 要保存您的选择，请选择 Save changes（保存更改）。

使用 Amazon CLI 和 Amazon Redshift API 配置日志记录

您可以通过以下 Amazon Redshift CLI 操作来配置审计日志记录：

- describe-logging-status
- disable-logging
- enable-logging

您可以通过以下 Amazon Redshift API 操作来配置审计日志记录：

- DescribeLoggingStatus
- DisableLogging
- EnableLogging

使用 Cloudtrail 进行日志记录

使用 Amazon CloudTrail 记录调用

Amazon Redshift、数据共享、Amazon Redshift Serverless 和 Amazon Redshift 数据 API 都与 Amazon CloudTrail 集成。CloudTrail 服务提供用户、角色或 Amazon 服务在 Amazon Redshift 中所执行的操作的记

录。CloudTrail 将 Amazon Redshift 的所有 API 调用作为事件捕获。捕获的调用包括通过 Redshift 控制台进行的调用以及对 Redshift 操作的代码调用。

如果您创建 CloudTrail 跟踪记录，则可以让 CloudTrail 事件持续传送到 Amazon S3 桶（包括 Redshift 的事件）。如果您不配置跟踪记录，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。通过使用 CloudTrail 收集的信息，您可以确定某些事项。这些事项包括向 Redshift 发出的请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间，以及其他详细信息。

您可以将 CloudTrail 与 Amazon Redshift 数据库审计日志记录一起使用，也可以单独使用前者。

要了解有关 CloudTrail 的更多信息，请参阅 Amazon CloudTrail 用户指南。

在 CloudTrail 中处理信息

在您创建账户时，您的 Amazon 账户中已启用 CloudTrail。发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 Amazon 服务事件一同保存在 Event history（事件历史记录）中。您可以在 Amazon 账户中查看、搜索和下载最新事件。有关更多信息，请参阅 Amazon CloudTrail 用户指南中的使用 CloudTrail 事件历史记录查看事件。

要持续记录 Amazon 账户中的事件（包括 Redshift 的事件），请创建跟踪记录。CloudTrail 使用跟踪记录将日志文件传送至 Amazon S3 桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 Amazon 区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）存储桶。此外，您可以配置其它Amazon服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅 Amazon CloudTrail 用户指南中的以下内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

所有 Amazon Redshift、Amazon Redshift Serverless、数据 API 和数据共享操作都由 CloudTrail 记录。例如，对 `AuthorizeDatashare`、`CreateNamespace` 和 `ExecuteStatement` 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 IAM 用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其它Amazon服务发出。

有关更多信息，请参阅 Amazon CloudTrail 用户指南中的 CloudTrail userIdentity 元素。

了解日志文件条目

跟踪记录 是一种配置，允许将事件作为日志文件传送到您指定的 Amazon S3 桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

Amazon Redshift 数据共享示例

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 `AuthorizeDataShare` 操作。

```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
                "arn": "arn:aws:sts::111122223333:user/janedoe",
                "accountId": "111122223333",
                "userName": "janedoe"
            },
            "attributes": {
                "creationDate": "2021-08-02T23:40:45Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-08-02T23:40:58Z",
    "eventSource": "redshift.amazonaws.com",
    "eventName": "AuthorizeDataShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.227.36.75",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "consumerIdentifier": "555555555555"
    },
    "responseElements": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "producerNamespaceArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "producerArn": "arn:aws:redshift:us-
east-1:111122223333:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "allowPubliclyAccessibleConsumers": true,
        "dataShareAssociations": [
            {
                "consumerIdentifier": "555555555555",
                "status": "AUTHORIZED",
                "createdDate": "Aug 2, 2021 11:40:56 PM",
                "statusChangeDate": "Aug 2, 2021 11:40:57 PM"
            }
        ]
    },
    "requestID": "87ee1c99-9e41-42be-a5c4-00495f928422",
    "eventID": "03a3d818-37c8-46a6-aad5-0151803bdb09",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Amazon Redshift Serverless 示例

Amazon Redshift Serverless 与 Amazon CloudTrail 集成，以提供在 Amazon Redshift Serverless 中执行的操作的记录。CloudTrail 将 Amazon Redshift Serverless 的所有 API 调用作为事件捕获。有关 Amazon Redshift Serverless 功能的更多信息，请参阅 Amazon Redshift Serverless 功能概览。

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 `CreateNamespace` 操作。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAKEOFPINEXAMPLE:admin",
        "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
        "accountId": "111111111111",
        "accessKeyId": "AAKEOFPINEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAKEOFPINEXAMPLE",
                "arn": "arn:aws:iam::111111111111:role/admin",
                "accountId": "111111111111",
                "userName": "admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-21T20:51:58Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-21T23:15:40Z",
    "eventSource": "redshift-serverless.amazonaws.com",
    "eventName": "CreateNamespace",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "56.23.155.33",
    "userAgent": "aws-cli/2.4.14 Python/3.8.8 Linux/5.4.181-109.354.amzn2int.x86_64 exe/
x86_64.amzn.2 prompt/off command/redshift-serverless.create-namespace",
    "requestParameters": {
        "adminUserPassword": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "adminUsername": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "dbName": "dev",
        "namespaceName": "testnamespace"
    },
    "responseElements": {
        "namespace": {
            "adminUsername": "HIDDEN_DUE_TO_SECURITY_REASONS",
            "creationDate": "Mar 21, 2022 11:15:40 PM",
            "defaultIamRoleArn": "",
            "iamRoles": [],
            "logExports": [],
            "namespaceArn": "arn:aws:redshift-serverless:us-east-1:111111111111:namespace/
befa5123-16c2-4449-afca-1d27cb40fc99",
            "namespaceId": "8b726a0c-16ca-4799-acca-1d27cb403599",
            "namespaceName": "testnamespace",
            "status": "AVAILABLE"
        }
    },
    "requestID": "ed4bb777-8127-4dae-aea3-bac009999163",
    "eventID": "1dbee944-f889-4beb-b228-7ad0f312464",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management",
}
```


Amazon Redshift 数据 API 示例

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 `ExecuteStatement` 操作。

```
{
    "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",
    "recipientAccountI":"123456789012"
}
```

Amazon CloudTrail 日志中的 Amazon Redshift 账户 ID

当 Amazon Redshift 为您调用其他 Amazon 服务时，该次调用将以属于 Amazon Redshift 的账户 ID 记录下来。它未以您的账户 ID 记录。例如，假设 Amazon Redshift 调用 Amazon Key Management Service（Amazon KMS）操作（如 `CreateGrant`、`Decrypt`、`Encrypt` 和 `RetireGrant`）以管理集群上的加密。在这种情况下，调用由 Amazon CloudTrail 使用 Amazon Redshift 账户 ID 记录。

当调用其他 Amazon 服务时，Amazon Redshift 使用下表中的账户 ID。

区域	区域	账户 ID
美国东部（弗吉尼亚北部）区域	us-east-1	368064434614
美国东部（俄亥俄）区域	us-east-2	790247189693
美国西部（加利福尼亚北部）区域	us-west-1	703715109447
美国西部（俄勒冈）区域	us-west-2	473191095985
Africa (Cape Town) Region	af-south-1	420376844563
亚太地区（香港）区域	ap-east-1	651179539253
亚太地区（雅加达）区域	ap-southeast-3	623197973179

区域	区域	账户 ID
亚太（孟买）区域	ap-south-1	408097707231
亚太地区（大阪）区域	ap-northeast-3	398671365691
亚太区域（首尔）	ap-northeast-2	713597048934
亚太区域（新加坡）	ap-southeast-1	960118270566
亚太区域（悉尼）	ap-southeast-2	485979073181
亚太区域（东京）	ap-northeast-1	615915377779
加拿大（中部）区域	ca-central-1	764870610256
中国（北京）区域	cn-north-1	066403562008
中国（宁夏）区域	cn-northwest-1	194116488714
欧洲（法兰克福）区域	eu-central-1	434091160558
欧洲（爱尔兰）区域	eu-west-1	246478207311
欧洲（伦敦）区域	eu-west-2	885798887673
Europe (Milan) Region	eu-south-1	041313461515
欧洲（巴黎）区域	eu-west-3	694668203235
欧洲（斯德哥尔摩）区域	eu-north-1	553461782468
Middle East (Bahrain) Region	me-south-1	051362938876
中东（阿联酋）区域	me-central-1	595013617770
南美洲（圣保罗）区域	sa-east-1	392442076723

以下示例显示了 Amazon Redshift 所调用的 Amazon KMS Decrypt 操作的 CloudTrail 日志条目。

```
{

    "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"

}
```


Amazon Redshift 的合规性验证

作为多个 Amazon 合规性计划的一部分，第三方审计员将评估 Amazon Redshift 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规性计划范围内的 Amazon 服务的列表，请参阅合规性计划范围内的 Amazon 服务。有关一般信息，请参阅 Amazon 合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅下载 Amazon Artifact 中的报告。

您在使用 Amazon Redshift 时的合规性责任由您数据的敏感性、您组织的合规性目标以及适用的法律法规决定。如果您对 Amazon Redshift 的使用需遵守 HIPAA、PCI 或 FedRAMP 等标准，Amazon 提供了以下实用资源：

- 安全性和合规性快速入门指南，介绍了架构注意事项，以及在 Amazon 上部署侧重于安全性和合规性的基准环境的步骤。
- 设计符合 HIPAA 安全性和合规性要求的架构白皮书，介绍公司如何使用 Amazon 创建符合 HIPAA 标准的应用程序。
- Amazon 合规性资源，这些业务手册和指南可能适用于您的行业和位置。
- Amazon Config，一项 Amazon 服务，可以评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub，一项 Amazon 服务，提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

以下合规性和安全性文档涵盖 Amazon Redshift，并可通过 Amazon Artifact 按需提供。有关更多信息，请参阅。Amazon Artifact

- 云计算合规性控制目录 (C5)
- ISO 27001:2013 适用性声明 (SoA)
- ISO 27001:2013 认证
- ISO 27017:2015 适用性声明 (SoA)
- ISO 27017:2015 认证
- ISO 27018:2015 适用性声明 (SoA)
- ISO 27018:2014 认证
- ISO 9001:2015 认证
- PCI DSS 合规证明 (AOC) 和责任摘要
- 服务组织控制 (SOC) 1 报告
- 服务组织控制 (SOC) 2 报告
- 服务组织控制 (SOC) 2 保密性报告

Amazon Redshift 中的恢复能力

Amazon 全球基础设施围绕 Amazon 区域和可用区 (AZ) 构建。Amazon区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个数据中心基础设施或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

几乎所有 Amazon 区域都有多个可用区和数据中心。您可以跨一个区域中的多个可用区部署您的应用来获得容错性和低延迟。

有关 Amazon 区域和可用区的更多信息，请参阅 Amazon 全球基础设施。

Amazon Redshift 中的基础设施安全性

作为一项托管服务，Amazon Redshift 由 Amazon Web Services：安全流程概述白皮书中所述的 Amazon 全球网络安全过程提供保护。

您可以使用 Amazon 发布的 API 调用通过网络访问 Amazon Redshift。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 Amazon Security Token Service (Amazon STS) 生成临时安全凭证来对请求进行签名。

您可以从任何网络位置调用这些 API 操作。此外，Amazon Redshift 支持基于资源的访问策略，其中可以包含基于源 IP 地址的限制。

网络隔离

基于 Amazon VPC 服务的 Virtual Private Cloud (VPC) 是您在Amazon云中的逻辑上隔离的私有网络。您可以通过执行以下步骤在 VPC 中部署 Amazon Redshift 集群：

- 在 Amazon 区域中创建 VPC。有关更多信息，请参阅 Amazon VPC 用户指南中的什么是 Amazon VPC？。
- 创建两个或更多私有 VPC 子网。有关更多信息，请参阅 Amazon VPC 用户指南中的 VPC 和子网。
- 部署 Amazon Redshift 集群。有关更多信息，请参阅Amazon Redshift 集群子网组 (p. 95)。

预设情况下，Amazon Redshift 集群在预置时被锁定。要允许来自 Amazon Redshift 客户端的入站网络流量，请将 VPC 安全组与 Amazon Redshift 集群相关联。有关更多信息，请参阅Amazon Redshift 集群子网组 (p. 95)。

要仅允许来往于特定 IP 地址范围的流量，请使用 VPC 更新安全组。例如，仅允许来自或流入公司网络的流量。

在配置与您的集群标记的子网关联的网络访问控制列表时，请确保将相应的 Amazon 区域的 S3 CIDR 范围添加到入口和出口规则的允许列表中。这样做可以让您在没有任何中断的情况下执行基于 S3 的操作，如 Redshift Spectrum、COPY 和 UNLOAD。

以下示例命令解析了 us-east-1 区域内的 Amazon S3 中使用的所有 IPv4 地址的 JSON 响应。

```
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
```

有关如何获取特定区域的 S3 IP 范围的说明，请参阅 Amazon IP 地址范围。

Amazon Redshift 支持将集群部署到专用租赁 VPC 中。有关更多信息，请参阅 Amazon EC2 用户指南中的专用实例。

Amazon Redshift 集群安全组

在您预置 Amazon Redshift 集群时，它默认处于锁定状态，因此任何人都无法访问。要为其他用户授予针对 Amazon Redshift 集群的入站访问权限，您可以将该集群与安全组关联起来。如果您处于 EC2-VPC 平台上，您可以使用现有的 Amazon VPC 安全组或者定义一个新的安全组，然后将其与集群关联。有关在 EC2-VPC 平台上管理集群的更多信息，请参阅在 VPC 中管理集群 (p. 92)。

如果您处于 EC2-Classic 平台上，您可以定义一个集群安全组，并将其与集群关联。EC2-Classic 平台将停用。我们建议您在 EC2-VPC 平台而不是 EC2-Classic 平台中启动集群。不过，您可以使用 Amazon Redshift 控制台将 EC2-Classic 快照还原到 EC2-VPC 集群。有关更多信息，请参阅从快照还原集群 (p. 328)。

使用接口 VPC 终端节点连接到 Amazon Redshift

您可以使用 Virtual Private Cloud（VPC）中的接口 VPC 终端节点 (Amazon PrivateLink) 直接连接到 Amazon Redshift API 服务，而不是通过 Internet 连接。有关 Amazon Redshift API 操作的信息，请参阅 Amazon Redshift API 参考中的操作。有关 Amazon PrivateLink 的更多信息，请参阅 Amazon VPC 用户指南中的接口 VPC 终端节点 (Amazon PrivateLink)。请注意，与集群的 JDBC/ODBC 连接不是 Amazon Redshift API 服务的一部分。

当您使用接口 VPC 终端节点时，您的 VPC 和 Amazon Redshift 之间的通信完全在 Amazon 网络内进行，从而可以提供更好的安全性。每个 VPC 终端节点都由您的 VPC 子网中一个或多个使用私有 IP 地址的弹性网络接口代表。有关弹性网络接口的更多信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中的弹性网络接口。

一个接口 VPC 终端节点将您的 VPC 直接连接到 Amazon Redshift。它不使用互联网网关、网络地址转换 (NAT) 设备、虚拟专用网络 (VPN) 连接或 Amazon Direct Connect 连接。VPC 中的实例不需要公有 IP 地址便可与 Amazon Redshift API 进行通信。

要在 VPC 中使用 Amazon Redshift，您有两种选择。一种是从 VPC 内的实例进行连接。另一种方法是将您的私有网络连接到您的 VPC，方法是使用 Amazon VPN 选项或 Amazon Direct Connect。有关 Amazon

VPN 选项的更多信息，请参阅 Amazon VPC 用户指南中的 VPN 连接。有关 Amazon Direct Connect 的信息,请参阅 Amazon Direct Connect 用户指南中的创建连接。

您可以创建接口 VPC 终端节点以使用 Amazon Web Services Management Console 或 Amazon Command Line Interface (Amazon CLI) 命令连接到 Amazon Redshift。有关更多信息，请参阅创建接口终端节点。

在创建接口 VPC 终端节点后，您可以为端点启用私有 DNS 主机名。当您执行此操作时，默认的 Amazon Redshift 端点 (`https://redshift.Region.amazonaws.com`) 解析为您的 VPC 终端节点。

如果您不启用私有 DNS 主机名，Amazon VPC 将提供一个您可以使用的 DNS 端点名称，格式如下。

```
VPC_endpoint_ID.redshift.Region.vpce.amazonaws.com
```

有关更多信息，请参阅 Amazon VPC 用户指南中的接口 VPC 终端节点 (Amazon PrivateLink)。

Amazon Redshift 支持调用您的 VPC 中的所有 API 操作。

您可以将 VPC 终端节点策略附加到 VPC 终端节点，以控制 Amazon Identity and Access Management (IAM) 委托人的访问权限。您还可以将安全组与 VPC 终端节点关联，以便根据网络流量的源和目标控制入站和出站访问。示例为 IP 地址的范围。有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 终端节点控制对服务的访问。

为 Amazon Redshift 创建 VPC 终端节点策略

您可以为 Amazon Redshift 的 VPC 终端节点创建一个策略，在该策略中指定以下内容：

- 可以或不能执行操作的委托人
- 可执行的操作
- 可对其执行操作的资源

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 终端节点控制对服务的访问权限。

接下来，您可以查找 VPC 终端节点策略示例。

主题

- 示例：用于拒绝来自指定 Amazon 账户的所有访问的 VPC 终端节点策略 (p. 459)
- 示例：仅允许 VPC 访问指定的 IAM 委托人（用户）的 VPC 终端节点策略 (p. 460)
- 示例：允许只读 Amazon Redshift 操作的 VPC 终端节点策略 (p. 460)
- 示例：拒绝访问指定集群的 VPC 终端节点策略 (p. 461)

示例：用于拒绝来自指定 Amazon 账户的所有访问的 VPC 终端节点策略

以下 VPC 终端节点策略会拒绝 Amazon 账户 *123456789012* 使用此端点访问资源的所有权限。

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
```

```
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

示例：仅允许 VPC 访问指定的 IAM 委托人（用户）的 VPC 终端节点策略

以下 VPC 终端节点策略仅允许对 Amazon 账户 *123456789012* 中的 IAM 用户 *redshiftadmin* 进行完全访问。使用端点拒绝所有其他 IAM 委托人进行访问。

```
  {
   "Statement": [
       {
           "Action": "*",
           "Effect": "Allow",
           "Resource": "*",
           "Principal": {
               "AWS": [
                   "arn:aws:iam::123456789012:user/redshiftadmin"
               ]
           }
       }]
}
```

示例：允许只读 Amazon Redshift 操作的 VPC 终端节点策略

以下 VPC 终端节点策略仅允许 Amazon 账户 *123456789012* 执行指定的 Amazon Redshift 操作。

指定的操作为 Amazon Redshift 提供等效的只读访问权限。针对指定账户拒绝 VPC 上的所有其它操作。同样，所有其他帐户都被拒绝进行任何访问。有关 Amazon Redshift 操作的列表，请参阅 IAM 用户指南中的 Amazon Redshift 的操作、资源和条件键。

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

示例：拒绝访问指定集群的 VPC 终端节点策略

以下 VPC 终端节点策略允许所有账户和委托人的完全访问权限。与此同时，它拒绝 Amazon 账户 *123456789012* 对于在具有集群 ID *my-redshift-cluster* 的 Amazon Redshift 集群上执行的操作的任何访问。仍然允许其他不支持集群资源级权限的 Amazon Redshift 操作。有关 Amazon Redshift 操作及其相应资源类型的列表，请参阅 IAM 用户指南中的 Amazon Redshift 的操作、资源和条件键。

```
 {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-
cluster",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Amazon Redshift 中的配置和漏洞分析

Amazon 负责处理来宾操作系统 (OS) 和数据库补丁、防火墙配置和灾难恢复 (DR) 等基本安全任务。这些流程已经过认证的第三方审计。有关更多信息，请参阅Amazon Redshift 的合规性验证 (p. 456)、责任共担模式和安全性、身份和合规性的最佳实践。

Amazon Redshift 会自动应用升级并修补您的数据仓库，以便您可以专注于您的应用程序，而不是应用程序的管理。补丁和升级在可配置的维护时段中应用。有关更多信息，请参阅维护时段 (p. 61)。

Amazon Redshift 查询编辑器 v2 是 Amazon 托管式应用程序。所有补丁和更新均由 Amazon 根据需要应用。

使用 Amazon Redshift 管理界面

Amazon Redshift 支持多种可用于创建、管理和删除 Amazon Redshift 集群的管理界面，其中包括 Amazon 开发工具包、 Amazon Command Line Interface (Amazon CLI) 和 Amazon Redshift 管理 API。

The Amazon Redshift API – 您可以通过提交请求来调用此 Amazon Redshift 管理 API。请求是 HTTP 或 HTTPS 请求，需要使用 HTTP 动词 `GET` 或 `POST` 以及一个名为 `Action` 的参数。调用 Amazon Redshift API 是访问 Amazon Redshift 服务的最直接方式。但是，此调用需要您的应用程序处理低级别的详细信息，例如进行错误处理以及生成哈希值以签署请求。

- 有关构建和签署查询 Amazon Redshift API 请求的信息，请参阅对 HTTP 请求进行签名 (p. 465)。
- 有关 Amazon Redshift API 操作和 Amazon Redshift 的数据类型的信息，请参阅 Amazon Redshift API 参考。

Amazon 开发工具包 – 您可以使用 Amazon 开发工具包执行与 Amazon Redshift 集群相关的操作。一些开发工具包库包含底层 Amazon Redshift API。他们将 API 功能集成到特定编程语言并处理许多低级别详细信息，如计算签名、处理请求重试和进行错误处理。调用开发工具包库中的包装函数可极大地简化编写用于管理 Amazon Redshift 集群的应用程序的流程。

- Amazon Redshift 受适用于 Java、.NET、PHP、Python、Ruby 和 Node.js 的 Amazon 开发工具包的支持。Amazon Redshift 的包装函数记录在每个开发工具包的参考手册中。有关 Amazon 开发工具包及其文档链接的列表，请参阅适用于 Amazon Web Services 的工具。
- 本指南提供通过 Java 开发工具包使用 Amazon Redshift 的示例。有关更多一般 Amazon 开发工具包代码示例，请参阅示例代码和库。

Amazon CLI – CLI 提供一组可用于从 Windows、Mac 和 Linux 计算机管理 Amazon 服务的命令行工具。Amazon CLI 包括基于 Amazon Redshift 查询 API 操作的命令。

- 有关安装和设置 Amazon Redshift CLI 的信息，请参阅设置 Amazon Redshift CLI (p. 467)。
- 有关 Amazon Redshift CLI 命令的参考资料，请参阅 Amazon CLI 参考中的 Amazon Redshift。

主题

- 结合使用 Amazon SDK for Java 与 Amazon Redshift (p. 463)
- 对 HTTP 请求进行签名 (p. 465)
- 设置 Amazon Redshift CLI (p. 467)

结合使用 Amazon SDK for Java 与 Amazon Redshift

Amazon SDK for Java 提供一个名为 `AmazonRedshiftClientBuilder` 的类，您可以使用它与 Amazon Redshift 进行交互。有关下载Amazon SDK for Java的信息，请转到Amazon SDK for Java。

> Note
>
> Amazon SDK for Java 提供了用于访问 Amazon Redshift 的线程安全客户端。应用程序应创建一个客户端并在线程之间重复使用此客户端，您应将此作为一项最佳实践。

您可以使用 `AmazonRedshiftClientBuilder` 和 `AwsClientBuilder` 类配置终端节点并创建 `AmazonRedshift` 客户端。然后，您可以使用客户端对象来创建 `Cluster` 对象的实例。`Cluster` 对

象包括映射到基础 Amazon Redshift 查询 API 操作的方法。（在 Amazon Redshift API 参考中介绍了这些操作。）调用某个方法时，您必须创建对应的请求对象。请求对象包含必须通过实际请求传递的信息。`Cluster` 对象提供从 Amazon Redshift 返回的信息来响应请求。

以下示例说明如何使用 `AmazonRedshiftClientBuilder` 类配置终端节点，然后创建由 2 个节点组成的 ds2.xlarge 集群。

```
String endpoint = "https://redshift.us-east-1.amazonaws.com/";
String region = "us-east-1";
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration(endpoint, region);
AmazonRedshiftClientBuilder clientBuilder = AmazonRedshiftClientBuilder.standard();
clientBuilder.setEndpointConfiguration(config);
AmazonRedshift client = clientBuilder.build();

CreateClusterRequest request = new CreateClusterRequest()
  .withClusterIdentifier("exampleclusterusingjava")
  .withMasterUsername("masteruser")
  .withMasterUserPassword("12345678Aa")
  .withNodeType("ds2.xlarge")
  .withNumberOfNodes(2);

Cluster createResponse = client.createCluster(request);
System.out.println("Created cluster " + createResponse.getClusterIdentifier());
```

使用 Eclipse 运行 Amazon Redshift 的 Java 示例

使用 Eclipse 运行 Java 代码示例的一般流程

1. 在 Eclipse 中创建一个新的 Amazon Java 项目。

   按 Amazon Toolkit for Eclipse 入门指南中的设置 Amazon Toolkit for Eclipse 中的步骤操作。
2. 复制本文档中您正在阅读的部分的示例代码，将其作为新的 Java 类文件粘贴到您的项目中。
3. 运行该代码。

从命令行中运行 Amazon Redshift 的 Java 示例

从命令行中运行 Java 代码示例的一般流程

1. 按照以下操作设置并测试您的环境：
   a. 创建一个工作目录，并在其中创建 `src`、`bin` 和 `sdk` 子文件夹。
   b. 下载 Amazon SDK for Java，并将它解压到您创建的 `sdk` 子文件夹中。解压开发工具包后，`sdk` 文件夹中应该会有四个子目录，包括 `lib` 和 `third-party` 文件夹。
   c. 为 SDK for Java 提供 Amazon 凭证。有关更多信息，请转至 Amazon SDK for Java 开发人员指南中的在 Amazon SDK for Java 中提供 Amazon 凭证。
   d. 确保您可以从工作目录运行 Java 程序编译器 (`javac`) 和 Java 应用程序启动器 (`java`)。您可以通过运行以下命令进行测试：

   ```
   javac -help
   java -help
   ```
2. 将您要运行的代码放入一个 .java 文件中，并将该文件保存在 `src` 文件夹中。为了说明此过程，我们使用了 使用 Amazon SDK for Java 管理集群 (p. 90) 中的代码，因此 `src` 目录中的文件是 `CreateAndModifyClusters.java`。

3. 编译该代码。

```
javac -cp sdk/lib/aws-java-sdk-1.3.18.jar -d bin src\CreateAndModifyClusters.java
```

如果您使用的是 Amazon SDK for Java 的其他版本，请调整您的版本的类路径 (-cp)。

4. 运行该代码。在下面的命令中，我们添加了换行符以便于阅读。

```
java -cp "bin;
          sdk/lib/*;
          sdk/third-party/commons-logging-1.1.1/*;
          sdk/third-party/httpcomponents-client-4.1.1/*;
          sdk/third-party/jackson-core-1.8/*"
          CreateAndModifyClusters
```

根据您的操作系统的需要更改类路径分隔符。例如，对于 Windows，分隔符是“;”（如示例所示），而对于 Unix，它是“:”。其他代码示例需要的库可能比此示例所示的要多，或者您使用的 Amazon 开发工具包版本可能具有不同的第三方文件夹名称。对于这些情况，请适当调整类路径 (-cp)。

要运行本文档中的示例，请使用支持 Amazon Redshift 的 Amazon 开发工具包版本。要获取最新版本的 Amazon SDK for Java，转到 Amazon SDK for Java。

设置终端节点

默认情况下，Amazon SDK for Java会使用终端节点 `https://redshift.us-east-1.amazonaws.com/`。您可以利用以下 Java 代码段中所示的 `client.setEndpoint` 方法明确设置终端节点。

Example

```
client = new AmazonRedshiftClient(credentials);
client.setEndpoint("https://redshift.us-east-1.amazonaws.com/");
```

有关您可以在其中预置集群的受支持 Amazon 区域列表，请转到 Amazon Web Services 术语表中的区域和端点部分。

对 HTTP 请求进行签名

Amazon Redshift 要求您发送到管理 API 的每个请求都必须使用签名进行身份验证。本主题介绍如何为请求签名。

如果您使用的是 Amazon 开发工具包 (SDK) 之一或 Amazon Command Line Interface，将自动为请求签名，因此您可以跳过本节。有关如何使用 Amazon 开发工具包的更多信息，请参阅使用 Amazon Redshift 管理界面 (p. 463)。有关使用 Amazon Redshift 命令行界面的更多信息，请转到 Amazon Redshift 命令行参考。

要为请求签名，可以使用加密哈希函数计算数字签名。加密哈希一种是根据输入内容返回唯一哈希值的函数。对哈希函数的输入内容包括您的请求文本和秘密访问密钥。哈希函数返回哈希值，您将该值包含在请求中，作为签名。该签名是您的请求的 `Authorization` 标头的一部分。

> Note
>
> 对于 API 访问，您需要访问密钥 ID 和秘密访问密钥。使用 IAM 用户访问密钥而不是Amazon Web Services 账户根用户访问密钥。有关创建访问密钥的更多信息，请参阅 IAM 用户指南 中的管理 IAM 用户的访问密钥。

Amazon Redshift 收到您的请求后，它将使用您在为请求签名时使用的相同哈希函数和输入来重新计算签名。如果得出的签名与请求中的签名相匹配，Amazon Redshift 会处理请求；否则请求将被拒绝。

Amazon Redshift 支持使用 Amazon 签名版本 4 进行身份验证。计算签名的流程包含三个任务。这些任务在下文的示例中有所说明。

- 任务 1：创建规范请求

  将您的 HTTP 请求重新排列为规范格式。必须使用规范格式，因为 Amazon Redshift 会使用同一规范格式计算要与您发送的签名进行比较的签名。
- 任务 2：创建要签名的字符串

  创建一个字符串，将该字符串用作您的加密哈希函数输入值中的一项。该字符串称为“待签字符串”，是哈希算法名称、请求日期、凭证范围字符串以及来自上一任务的规范化请求的结合。凭证范围字符串本身是日期、区域和服务信息的结合。
- 任务 3：创建签名

  使用加密哈希函数为您的请求创建签名，该函数接受两种输入字符串：待签字符串和派生密钥。派生密钥的计算方法是，以您的秘密访问密钥开头，并使用凭证范围字符串来创建一系列基于哈希的消息身份验证代码 (HMAC-SHA256)。

示例签名计算

以下示例将为您详细介绍为 CreateCluster 请求创建签名的过程。您可以使用该示例作为参考，检查您自己的签名计算方法。在 Amazon Web Services 术语表的签名版本 4 测试套件中包含其他参考计算。

您可以使用 GET 或 POST 请求将请求发送到 Amazon Redshift。这两者之间的区别是对于 GET 请求，您的参数作为查询字符串参数发送。对于 POST 请求，参数包含在请求正文中。以下示例显示的是 POST 请求。

示例假定以下各项：

- 请求的时间戳为 `Fri, 07 Dec 2012 00:00:00 GMT`。
- 终端节点为美国东部（弗吉尼亚北部）地区 (`us-east-1`)。

一般的请求语法为：

```
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
```

为任务 1：创建规范请求 (p. 466)计算的规范请求格式为：

```
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
```

规范请求的最后一行是请求正文的哈希值。因为没有针对此 API 的查询参数，所以规范请求的第三行是空的。

任务 2：创建待签字符串 (p. 466)的待签字符串为：

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

待签字符串的第一行是算法，第二行是时间戳，第三行是凭证范围，最后一行是来自任务 1：创建规范请求 (p. 466)的规范请求的哈希。要在凭证范围中使用的服务名称为 `redshift`。

对于任务 3：创建签名 (p. 466)，派生密钥可以表示为：

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

派生密钥是通过系列哈希函数计算的。从上面公式中最里面的 HMAC 语句开始，将短语 **`AWS4`** 与您的秘密访问密钥连接，并使用它作为键来对数据“us-east-1”进行哈希计算。该哈希计算的结果将成为下一个哈希函数的键。

计算派生密钥后，在接受两个输入字符串、待签字符串和派生密钥的哈希函数中使用它。例如，如果您使用秘密访问密钥 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY` 和前文提到的代签字符串，那么计算出的签名如下所示：

```
9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

最终步骤是构造 `Authorization` 标头。对于示例访问密钥 `AKIAIOSFODNN7EXAMPLE`，标头（为了便于阅读，添加了换行符）为：

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

设置 Amazon Redshift CLI

本部分介绍如何设置和运行用于管理 Amazon Redshift 的 Amazon CLI 命令行工具。Amazon Redshift 命令行工具在 Amazon Command Line Interface (Amazon CLI) 上运行，而后者使用 Python (https://www.python.org/)。Amazon CLI 可在支持 Python 的所有操作系统上运行。

安装说明

要开始使用 Amazon Redshift 命令行工具，首先要设置 Amazon CLI，然后添加用于定义 Amazon Redshift CLI 选项的配置文件。

如果您已为其他 Amazon CLI 服务安装并配置 Amazon，则可跳过该程序。

安装 Amazon Command Line Interface

1. 转到使用 Amazon 命令行界面进行设置，然后按照安装 Amazon CLI 的说明进行操作。

要进行 CLI 访问，您需要访问密钥 ID 和秘密访问密钥。如果可能，请使用临时凭证代替长期访问密钥。临时凭证包括访问密钥 ID、秘密访问密钥，以及一个指示凭证何时到期的安全令牌。有关更多信息，请参阅《Amazon 一般参考》中的管理 Amazon 访问密钥的最佳实践。

2. 创建包含访问密钥、默认区域和命令输出格式等配置信息的文件。然后，设置 `AWS_CONFIG_FILE` 环境变量以引用该文件。有关详细说明，请转到 Amazon Command Line Interface 用户指南中的配置 Amazon 命令行界面。
3. 运行一个测试命令以确认 Amazon CLI 界面可正常工作。例如，以下命令应该显示有关 Amazon CLI 的帮助信息：

```
aws help
```

以下命令应该显示有关 Amazon Redshift 的帮助信息：

```
aws redshift help
```

有关 Amazon Redshift CLI 命令的参考资料，请转至 Amazon CLI 参考中的 Amazon Redshift。

Amazon Command Line Interface入门

为了帮助您开始使用 Amazon Command Line Interface (Amazon CLI)，本节介绍如何为 Amazon Redshift 集群执行基本的管理任务。这些任务与 Amazon Redshift 入门指南中的任务非常相似，但这些任务专注于 Amazon CLI 而不是 Amazon Redshift 控制台。

本部分将引导您完成创建集群、创建数据库表、上传数据和测试查询的过程。您使用 Amazon CLI 预置集群并授予所需的访问权限。然后，您将使用 SQL Workbench 客户端连接到集群、创建示例表、上载示例数据并运行测试查询。

步骤 1：开始前的准备工作

如果您还没有 Amazon 账户，则必须先注册一个。然后，您需要设置 Amazon Redshift 命令行工具。最后，您需要下载客户端工具和驱动程序才能连接到您的集群。

第 1.1 步：注册 Amazon 账户

有关注册 Amazon 用户账户的信息，请参阅 Amazon Redshift 入门指南。

步骤 1.2：下载并安装 Amazon CLI

如果尚未安装 Amazon CLI，请参阅设置 Amazon Redshift CLI (p. 467)。

步骤 1.3：下载客户端工具和驱动程序

您可以使用任何 SQL 客户端工具并利用 PostgreSQL JDBC 或 ODBC 驱动程序连接到 Amazon Redshift 集群。如果您当前未安装此类软件，则可以使用 SQL Workbench，这是一款免费的跨平台工具，可用来查询 Amazon Redshift 集群中的表。本部分的示例将使用 SQL Workbench 客户端。

要下载 SQL Workbench 和 PostgreSQL 驱动程序，请参阅 Amazon Redshift 入门指南。

步骤 2：启动集群

现在，您可以使用 Amazon CLI 启动集群了。

Important

您即将启动的集群将是活跃的，且不在沙盒中运行。您需要为该集群支付标准的使用费，直到您终止该集群。有关定价信息，请参阅 Amazon Redshift 定价页面。
如果您一鼓作气完成此处说明的练习并在使用完毕后终止集群，则产生的全部费用将非常少。

`create-cluster` 命令有大量参数。在本练习中，您将使用下表中所述的参数值。在生产环境中创建集群之前，我们建议您查看所有的必需参数和可选参数，确保集群配置符合您的要求。有关更多信息，请参阅 create-cluster

参数名称	本练习的参数值
`cluster-identifier`	`examplecluster`
`master-username`	`adminuser`
`master-user-password`	`TopSecret1`
`node-type`	`ds2.xlarge` 或您想要使用的节点大小。有关更多信息，请参阅Amazon Redshift 中的集群和节点 (p. 50)。
`cluster-type`	`single-node`

要创建集群，请输入以下命令。

```
aws redshift create-cluster --cluster-identifier examplecluster --master-username
 masteruser --master-user-password TopSecret1 --node-type ds2.xlarge --cluster-type single-
node
```

完成集群创建过程需要几分钟的时间。要检查状态，请输入以下命令。

```
aws redshift describe-clusters --cluster-identifier examplecluster
```

输出将类似于以下内容。

```
{
    "Clusters": [
        {

       ...output omitted...

            "ClusterStatus": "creating",
            "ClusterIdentifier": "examplecluster",

       ...output omitted...

}
```

当 ClusterStatus 字段从 `creating` 变为 `available` 时，您的集群就可供使用了。

在下一个步骤中，您将授予访问权限，以便连接到集群。

步骤 3：授权入站流量以访问集群

您必须明确授予对客户端的入站访问权限才能连接到集群。您的客户端可以是 Amazon EC2 实例或外部计算机。

在上一个步骤中创建了集群后，由于您未指定安全组，因此您将默认集群安全组与该集群相关联。默认集群安全组不包含对集群授权任何入站流量的规则。要访问新集群，您必须针对流向集群安全组的入站流量添加相关规则（称为传入规则）。

Internet 上运行的应用程序的入口规则

如果您要通过 Internet 访问集群，则需要授予一个无类别域间路由 IP (CIDR/IP) 地址范围。在本示例中，我们将使用 192.0.2.0/24 的 CIDR/IP 规则；您需要修改此范围以反映您的实际 IP 地址和网络掩码。

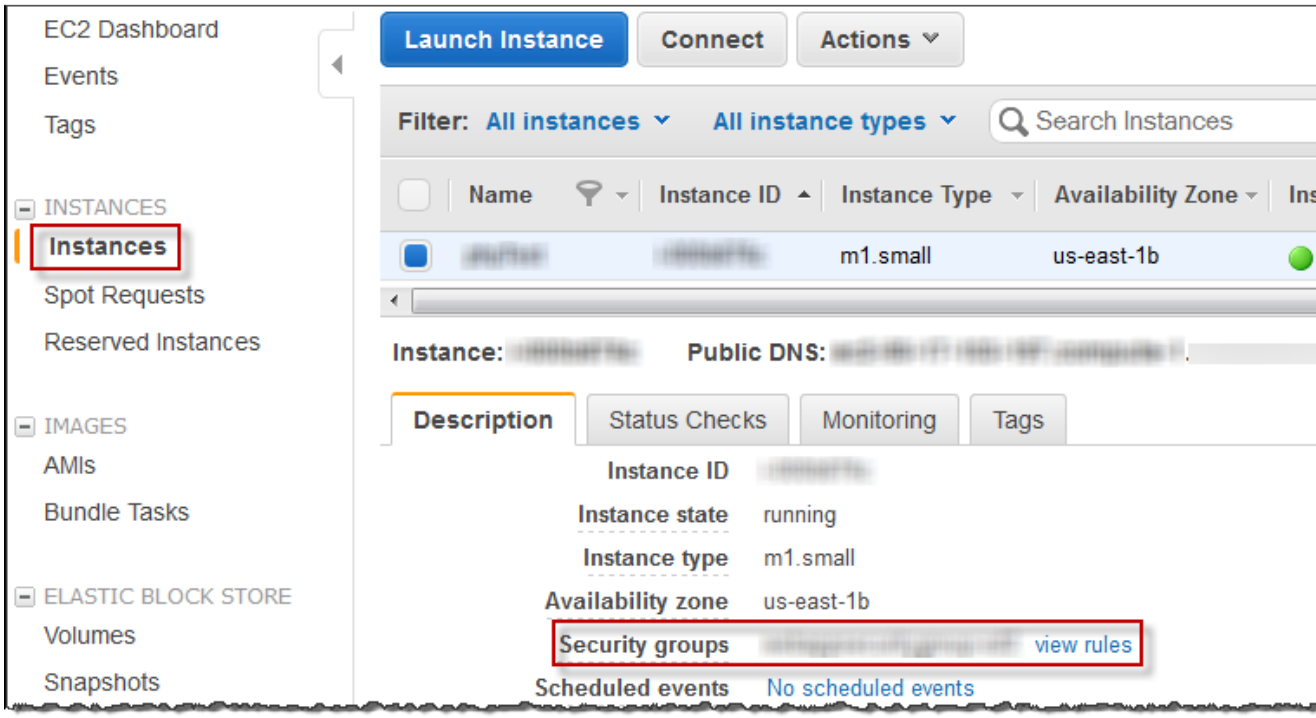
要允许网络进入集群，请输入以下命令。

```
aws redshift authorize-cluster-security-group-ingress --cluster-security-group-name default
 --cidrip 192.0.2.0/24
```

EC2 实例的入口规则

如果要通过 Amazon EC2 实例访问集群，您将需要授权 Amazon EC2 安全组。为此，您需要指定安全组名称，以及 EC2 安全组所有者的 12 位账号。

您可以使用 Amazon EC2 控制台来确定与您的实例关联的 EC2 安全组：



要查找您的 Amazon 账号，请转到 https://aws.amazon.com/，并登录 My Account（我的账户）页面。您的 Amazon 账号显示在该页面的右上角。

在本示例中，我们将使用 `myec2securitygroup` 作为 Amazon EC2 安全组名称，并使用 `123456789012` 作为账号。您可以根据自己的需要修改这些内容。

要允许网络进入集群，请输入以下命令。

```
aws redshift authorize-cluster-security-group-ingress --cluster-security-group-name
default --ec2-security-group-name myec2securitygroup --ec2-security-group-owner
123456789012
```

步骤 4：连接到集群

现在您已经为默认集群安全组添加了传入规则，从特定 CIDR/IP 或 EC2 安全组到 `examplecluster` 的传入连接已经获得授权。

现在，您可以连接到集群了。

有关连接到集群的信息，请转到 Amazon Redshift 入门指南。

步骤 5：创建表，上传数据并尝试示例查询

有关创建表、上载数据和发布查询的信息，请转到 Amazon Redshift 入门指南。

步骤 6：删除示例集群

在集群启动并可供使用之后，即使没有实际使用，您也需要根据集群的运行时间支付相应费用。当您不再需要集群时，可将其删除。

在删除集群时，您必须决定是否创建最终快照。由于这是一次练习，测试集群中不会有任何重要的数据，因此您无需创建最终快照。

要删除集群，请输入以下命令。

```
aws redshift delete-cluster --cluster-identifier examplecluster --skip-final-cluster-
snapshot
```

恭喜您！您已成功启动、授权访问、连接到并终止了集群。

监控 Amazon Redshift 集群性能

Amazon Redshift 提供性能指标和数据，以便您可以跟踪集群和数据库的运行状况及性能。在本部分中，我们将讨论您可以在 Amazon Redshift（尤其是 Amazon Redshift 控制台）中使用的数据类型。

主题

- 概览 (p. 472)
- 使用 CloudWatch 指标监控 Amazon Redshift (p. 472)
- 在 Amazon Redshift 控制台中使用性能数据 (p. 480)

概览

您可以在 Amazon Redshift 控制台中使用的性能数据分为两类：

- Amazon CloudWatch 指标 – Amazon CloudWatch 指标有助于您监控集群的物理方面，例如 CPU 使用率、延迟和吞吐量。指标数据直接显示在 Amazon Redshift 控制台中。您还可以在 CloudWatch 控制台中查看它。或者，您也可以通过处理指标的任何其他方式使用它，例如使用 Amazon CLI 或其中一个 Amazon 开发工具包。
- 查询/加载性能数据 – 性能数据可以帮助您监控数据库活动和性能。此类数据汇集于 Amazon Redshift 控制台中，有助于您轻松将通过 CloudWatch 指标了解的情况与特定数据库查询和加载事件相关联。您也可以创建自己的自定义性能查询，并直接在数据库上运行这些查询。查询和加载性能数据仅显示在 Amazon Redshift 控制台中。此类数据不会作为 CloudWatch 指标进行发布。

性能数据集成到 Amazon Redshift 控制台中，从而通过以下方式实现更丰富的体验：

- 当您查看某个集群时，与之关联的性能数据会根据具体情况显示出来，例如在您需要针对集群做出决策（例如调整大小）时。
- 与 CloudWatch 相比，某些性能指标以经过更适当换算的单位显示在 Amazon Redshift 控制台中。例如，`WriteThroughput` 以 GB/s 显示（而在 CloudWatch 中，则以 Bytes/s 显示），该单位与典型的节点存储空间的相关性更高。
- 您可以在同一图表上轻松地将集群节点的性能数据显示在一起。这样，您就可以轻松监控集群的所有节点的性能。您还可以查看每个节点的性能数据。

Amazon Redshift 提供性能数据（包括 CloudWatch 指标以及查询和加载数据），无需任何额外费用。系统会记录每分钟的性能数据。您可以通过 Amazon Redshift 控制台访问性能数据的历史值。有关使用 CloudWatch 访问作为 CloudWatch 指标公开的 Amazon Redshift 性能数据的详细信息，请参阅 Amazon CloudWatch 用户指南中的什么是 CloudWatch？。

使用 CloudWatch 指标监控 Amazon Redshift

利用 Amazon Redshift 的 CloudWatch 指标，您可以获取有关集群的运行状况和性能的信息，并查看节点级别的信息。在使用这些指标时，请注意，每个指标都有一个或多个维度与之关联。这些维度告诉您指标适用于什么，即指标的范围。Amazon Redshift 有以下两个维度。

- 拥有 `NodeID` 维度的指标指的是提供集群节点性能数据的指标，这组指标包括领导节点和计算节点。例如以下指标：`CPUUtilization`、`ReadIOPS` 和 `WriteIOPS`。
- 只有 `ClusterIdentifier` 维度的指标指的是提供集群性能数据的指标。例如以下指标：`HealthStatus` 和 `MaintenanceMode`。

Note

在使用某些指标时，特定于集群的指标表示节点行为的聚合。在这类情况下，由于领导节点的行为与计算节点聚合，在解释指标值时请小心谨慎。

有关 CloudWatch 指标和维度的一般信息，请参阅 Amazon CloudWatch 用户指南中的 CloudWatch 概念。

有关 Amazon Redshift 的 CloudWatch 指标的进一步说明，请参阅以下部分。

主题

- Amazon Redshift 指标 (p. 473)
- Amazon Redshift 指标的维度 (p. 478)
- Amazon Redshift 查询和加载性能数据 (p. 479)

Amazon Redshift 指标

AWS/Redshift 命名空间包括以下指标。除非另有说明，否则每隔 1 分钟收集一次指标。

Title

指标	描述
CommitQueueLength	在给定的时间点等待提交的事务数。 单位：计数 维度：ClusterIdentifier
ConcurrencyScalingActiveClusters	在任何给定时间主动处理查询的并发扩展集群的数量。 单位：计数 维度：ClusterIdentifier
ConcurrencyScalingSeconds	具有活动查询处理活动的并发扩展集群使用的秒数。 单位：总计 维度：ClusterIdentifier
CPUUtilization	CPU 使用百分率。对于集群，该指标代表所有节点 (领导节点和计算节点) CPU 使用率值的总和。 单位：百分比 维度: ClusterIdentifier, NodeID 维度：ClusterIdentifier
DatabaseConnections	集群中的数据库连接数量。 单位：计数 维度：ClusterIdentifier
HealthStatus	表示集群的运行状况检查。每分钟集群连接到其数据库并执行一次简单的查询。如果可以成功执行此操作，则表示集群的运行状况良好。

指标	描述
	否则，视为集群运行状况不佳。当数据库集群负载极重，或者集群上的数据库存在配置问题时，集群会出现运营状况不佳的情况。 Note 在 Amazon CloudWatch 中，此指标报告为 1 或 0，而在 Amazon Redshift 控制台中，为了方便起见，此指标显示为 HEALTHY 或 UNHEALTHY。当该指标在 Amazon Redshift 控制台中显示时，采样平均值会被忽略，仅显示 HEALTHY 或 UNHEALTHY。在 Amazon CloudWatch 中，由于采样问题，可能出现 1 和 0 以外的值。HealthStatus 的所有 1 以下的值均报告为 0 (UNHEALTHY)。 单位：计数 (1/0)（在 Amazon Redshift 控制台中为 HEALTHY/UNHEALTHY） 维度：ClusterIdentifier
MaintenanceMode	表示集群是否处于维护模式。 Note 在 Amazon CloudWatch 中，此指标报告为 1 或 0，而在 Amazon Redshift 控制台中，为了方便起见，此指标显示为 ON 或 OFF。当该指标在 Amazon Redshift 控制台中显示时，采样平均值会被忽略，仅显示 ON 或 OFF。在 Amazon CloudWatch 中，由于采样问题，可能出现 1 和 0 以外的值。MaintenanceMode 的所有 0 以上的值均报告为 1 (ON)。 单位：计数 (1/0)（在 Amazon Redshift 控制台中为 ONOFF）。 维度：ClusterIdentifier
MaxConfiguredConcurrencyScalingClusters	从参数组配置的最大并发扩展集群数。有关更多信息，请参阅Amazon Redshift 参数组 (p. 299)。 单位：计数 维度：ClusterIdentifier
NetworkReceiveThroughput	节点或集群接收数据的速率。 单位：字节/秒（在 Amazon Redshift 控制台为 MB/s） 维度: ClusterIdentifier, NodeID 维度：ClusterIdentifier
NetworkTransmitThroughput	节点或集群写入数据的速率。 单位：字节/秒（在 Amazon Redshift 控制台为 MB/s） 维度: ClusterIdentifier, NodeID 维度：ClusterIdentifier

指标	描述
PercentageDiskSpaceUsed	已使用磁盘空间的百分比。 单位：百分比 维度：ClusterIdentifier
QueriesCompletedPerSecond	每秒完成的平均查询数。每隔 5 分钟报告一次。 单位：计数/秒 维度: ClusterIdentifier, latency 维度: ClusterIdentifier, wlmid
QueryDuration	完成查询的平均时间量。每隔 5 分钟报告一次。 单位：微秒 维度：ClusterIdentifier、NodeID、latency 维度: ClusterIdentifier, latency 维度：ClusterIdentifier、NodeID、wlmid
QueryRuntimeBreakdown	查询在各个查询阶段运行所花费的总时间。每隔 5 分钟报告一次。 单位：毫秒 维度：ClusterIdentifier、NodeID、stage 维度：ClusterIdentifier、stage
ReadIOPS	每秒平均磁盘读取 操作数。 单位：计数/秒 维度: ClusterIdentifier, NodeID 维度：ClusterIdentifier
ReadLatency	磁盘读取 I/O 操作所需的平均时间。 单位：秒 维度: ClusterIdentifier, NodeID 维度：ClusterIdentifier
ReadThroughput	每秒从磁盘读取的平均字节数。 单位：字节（在 Amazon Redshift 控制台为 GB/s） 维度: ClusterIdentifier, NodeID 维度：ClusterIdentifier

指标	描述
RedshiftManagedStorageTotalCapacity	总托管式存储容量。 单位：MB 维度：ClusterIdentifier
TotalTableCount	在特定时间点打开的用户表的数量。此总数不包括 Amazon Redshift Spectrum 表。 单位：计数 维度：ClusterIdentifier
WLMQueueLength	等待进入工作负载管理 (WLM) 队列的查询数。 单位：计数 维度: ClusterIdentifier, service class 维度: ClusterIdentifier, QueueName
WLMQueueWaitTime	在工作负载管理 (WLM) 队列中等待的查询总时间。每隔 5 分钟报告一次。 单位：毫秒。 维度: ClusterIdentifier, QueryPriority 维度: ClusterIdentifier, wlmid 维度: ClusterIdentifier, QueueName
WLMQueriesCompletedPerSecond	每秒为工作负载管理 (WLM) 队列完成的平均查询数。每隔 5 分钟报告一次。 单位：计数/秒 维度: ClusterIdentifier, wlmid 维度: ClusterIdentifier, QueueName
WLMQueryDuration	为工作负载管理 (WLM) 队列完成查询的平均时间量。每隔 5 分钟报告一次。 单位：微秒 维度: ClusterIdentifier, wlmid 维度: ClusterIdentifier, QueueName
WLMRunningQueries	对于每个 WLM 队列，从主集群和并发扩展集群运行的查询数。 单位：计数 维度: ClusterIdentifier, wlmid 维度: ClusterIdentifier, QueueName

指标	描述
WriteIOPS	每秒平均磁盘写入操作数。 单位：计数/秒 维度: ClusterIdentifier, NodeID 维度：ClusterIdentifier
WriteLatency	磁盘写入 I/O 操作所需的平均时间。 单位：秒 维度: ClusterIdentifier, NodeID 维度：ClusterIdentifier
WriteThroughput	每秒写入磁盘的平均字节数。 单位：字节（在 Amazon Redshift 控制台为 GB/s） 维度: ClusterIdentifier, NodeID 维度：ClusterIdentifier
SchemaQuota	为 schema 配置的配额。 单位：MB 维度：ClusterIdentifier、DatabaseName、SchemaName 周期/推送：Periodic 频率：5 minutes 停止条件：已删除 Schema 或移除配额
NumExceededSchemaQuotas	超出配额的 schema 数。 单位：计数 维度：ClusterIdentifier 周期/推送：Periodic 频率：5 minutes 停止标准：不适用
StorageUsed	schema 使用的磁盘或存储空间。 单位：MB 维度：ClusterIdentifier、DatabaseName、SchemaName 周期/推送：Periodic 频率：5 minutes 停止条件：已删除 Schema 或移除配额

指标	描述
PercentageQuotaUsed	使用的磁盘或存储空间相对于配置的 schema 配额的百分比。 单位：百分比 维度：ClusterIdentifier、DatabaseName、SchemaName 周期/推送：Periodic 频率：5 minutes 停止条件：已删除 Schema 或移除配额

Amazon Redshift 指标的维度

可以按下表中的任意维度对 Amazon Redshift 数据进行筛选。

维度	描述
latency	可能值如下所示： • short – 不到 10 秒 • medium – 在 10 秒到 10 分钟之间 • long – 超过 10 分钟
NodeID	筛选条件请求的特定于集群节点的数据。NodeID 是“领导”、“共享”或“N 计算”，其中 N 是集群中节点的数目（0、1 等）。“共享”意味着集群只有一个节点，即领导节点和计算节点合并到了一起。 针对领导节点和计算节点报告的指标只适用于 CPUUtilization、NetworkTransmitThroughput 和 ReadIOPS。使用 NodeId 维度的其他指标只针对计算节点进行报告。
ClusterIdentifier	筛选条件请求的特定于集群的数据。特定于集群的指标包括 HealthStatus、MaintenanceMode 和 DatabaseConnections。此维度的一般指标 (例如，ReadIOPS) 同样是表示节点指标数据聚合的节点的指标。在解析这些指标时请小心，因为它们是领导节点和计算节点的聚合行为。
service class	WLM 服务类的标识符。
stage	查询的执行阶段。可能的值如下所示： • QueryPlanning：分析和优化 SQL 语句所花的时间。 • QueryWaiting：在 WLM 队列中等待所花的时间。 • QueryExecutingRead：执行读取查询所花的时间。 • QueryExecutingInsert：执行插入查询所花的时间。 • QueryExecutingDelete：执行删除查询所花的时间。 • QueryExecutingUpdate：执行更新查询所花的时间。 • QueryExecutingCtas：执行 create table as 查询所花的时间。 • QueryExecutingUnload：执行卸载查询所花的时间。 • QueryExecutingCopy：执行复制查询所花的时间。

维度	描述
	• QueryCommit：提交所花的时间。
wlmid	工作负载管理队列的标识符。
QueryPriority	查询的优先级。可能的值包括 CRITICAL、HIGHEST、HIGH、NORMAL、LOW 和 LOWEST。
QueueName	工作负载管理队列的名称。

Amazon Redshift 查询和加载性能数据

除了 CloudWatch 指标之外，Amazon Redshift 还提供查询和加载性能数据。查询和加载性能数据有助于您了解数据库性能和集群指标之间的关系。例如，如果您注意到集群的 CPU 达到峰值，则可以在集群 CPU 图表中找到相应峰值，并了解当时正在运行的查询。相反，如果您要查看特定查询，则相应指标数据（如 CPU）会根据具体情况显示出来，以便您了解查询对集群指标的影响。

查询和加载性能数据不会作为 CloudWatch 指标发布，而只能通过 Amazon Redshift 控制台查看。查询和加载性能数据通过查询数据库的系统表生成（有关更多信息，请参阅 Amazon Redshift 开发人员指南中的系统表参考）。您也可以生成自己的自定义数据库性能查询，不过我们建议您先从控制台中提供的查询和加载性能数据入手。有关自行测量和监控数据库性能的更多信息，请参阅 Amazon Redshift 开发人员指南中的管理性能。

下表介绍了您可以通过 Amazon Redshift 控制台访问的查询和加载数据的不同方面。

查询/加载数据	描述
查询摘要	指定时间段内的查询列表。此列表可以按查询 ID、查询运行时间和状态等值排序。在集群详细信息页面的 Query monitoring (查询监控) 选项卡中查看此数据。
查询详细信息	提供某个特定查询的详细信息，包括： • 查询属性，如查询 ID、类型、运行查询的集群和运行时间。 • 详细信息，例如查询的状态和错误数量。 • 运行的 SQL 语句。 • 说明计划（如果有）。 • 查询执行期间的集群性能数据（有关更多信息，请参阅查看查询历史记录 (p. 486)）。
加载摘要	列出指定时间段内的所有加载。此列表可以按查询 ID、查询运行时间和状态等值排序。在集群详细信息页面的 Query monitoring (查询监控) 选项卡中查看此数据。
加载详细信息	提供有关特定加载操作的详细信息，包括： • 加载属性，例如查询 ID、类型、运行查询的集群和运行时间。 • 详细信息，例如加载的状态和错误数量。 • 运行的 SQL 语句。 • 已加载的文件列表。 • 加载操作期间的集群性能数据（有关更多信息，请参阅查看查询历史记录 (p. 486)）。

在 Amazon Redshift 控制台中使用性能数据

您可以在本节中查找如何在 Amazon Redshift 控制台中查看性能数据，包括有关集群和查询性能的信息。此外，您可以直接通过 Amazon Redshift 控制台针对集群指标创建警报。

您可以在 Amazon Redshift 控制台中按集群查看性能数据。集群的性能数据图表旨在帮助您找到解答最常见性能问题的数据。对于某些性能数据（请参阅使用 CloudWatch 指标监控 Amazon Redshift (p. 472)），您还可以使用 CloudWatch 进一步自定义指标图表。例如，您可以选择较长的时间或跨集群组合指标。有关使用 CloudWatch 控制台的更多信息，请参阅在 CloudWatch 控制台中使用性能指标 (p. 500)。

观看以下视频以了解如何使用 Amazon Redshift 控制台上的查询监控功能监控、隔离和优化查询：使用 Amazon Redshift 查询监控。

主题

- 查看集群性能数据 (p. 480)
- 查看查询历史记录 (p. 486)
- 查看数据库性能数据 (p. 489)
- 查看工作负载并发和并发扩展数据 (p. 492)
- 查看查询和加载 (p. 494)
- 在加载操作期间查看集群指标 (p. 498)
- 分析工作负载性能 (p. 498)
- 管理警报 (p. 499)
- 在 CloudWatch 控制台中使用性能指标 (p. 500)

查看集群性能数据

通过使用 Amazon Redshift 中的集群指标，您可以执行以下常见性能任务：

- 判断集群指标在指定时间范围内是否异常；如果异常的话，则确定负责这种性能冲击的查询。
- 查看历史或当前查询是否对集群性能造成了影响。如果您识别出了一个有问题的查询，则可以在查询执行期间查看有关该查询的详细信息 (包括集群性能)。您可以使用此信息来诊断为何查询速度慢以及可以采取哪些措施来提高它的性能。

查看性能数据

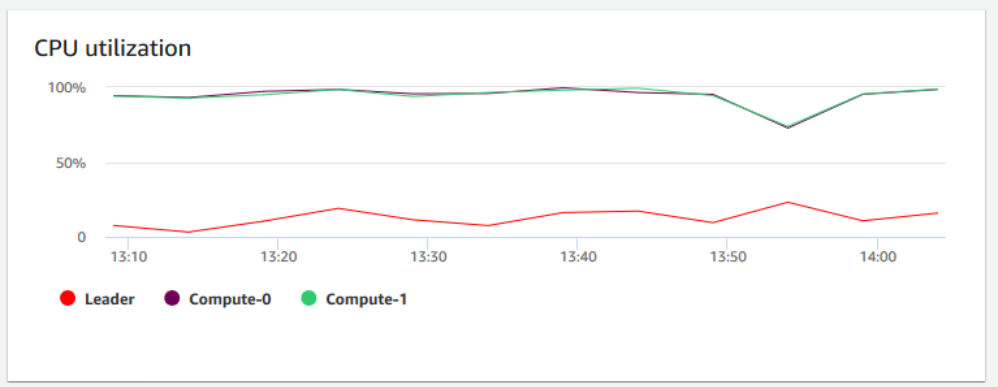
1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后从列表中选择集群名称以打开其详细信息。此时将显示集群的详细信息，其中包括 Cluster performance（集群性能）、Query monitoring（查询监控）、Databases（数据库）、Datashares（数据共享）、Schedules（计划）、Maintenance（维护）和 Properties（属性）选项卡。
3. 选择 Cluster performance (集群性能) 选项卡以查看性能信息，其中包括以下信息：
   - CPU 使用率
   - Percentage disk space used (已使用磁盘空间的百分比)
   - 数据库连接
   - 运行状况
   - Query duration (查询持续时间)
   - Query throughput (查询吞吐量)
   - Concurrency scaling activity (并发扩展活动)

此外，还提供了许多其他指标。要查看可用指标并选择要显示的指标，请选择 Preferences (首选项) 图标。

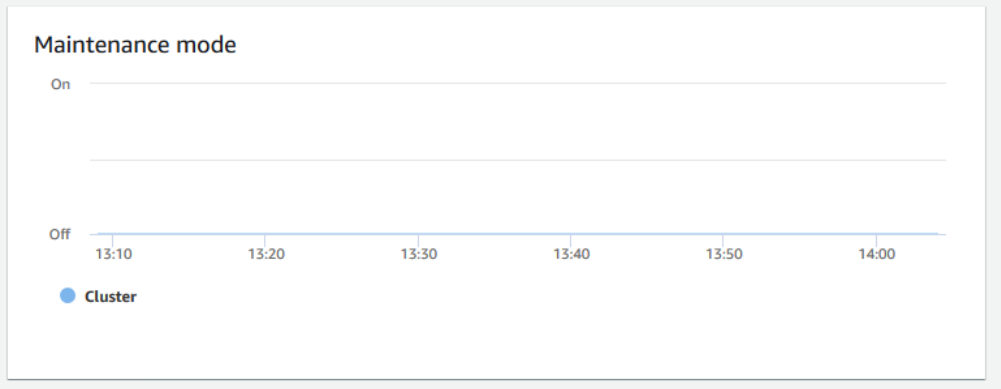
集群性能图表

以下示例显示新的 Amazon Redshift 控制台中显示的一些图表。

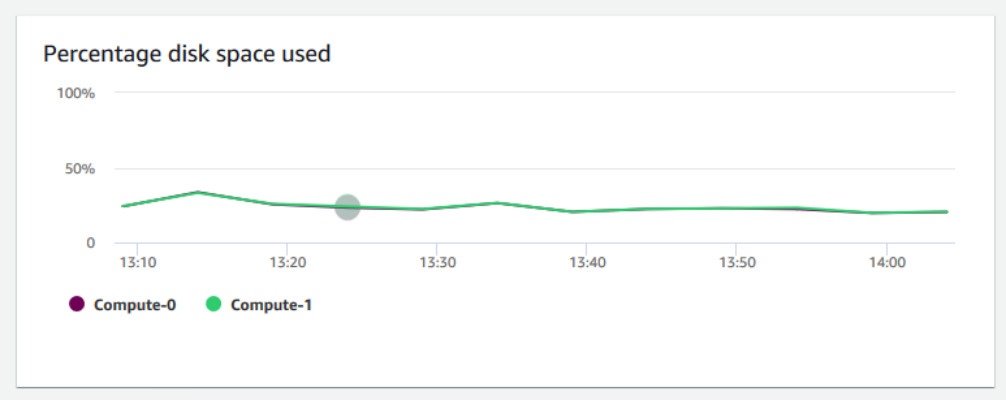
- CPU utilization（CPU 利用率）– 显示所有节点（领导节点和计算节点）的 CPU 利用率百分比。要在计划集群迁移或其他资源消耗型操作之前查找集群使用率最低的时间，请监控此图表以查看每个节点或所有节点的 CPU 使用率。



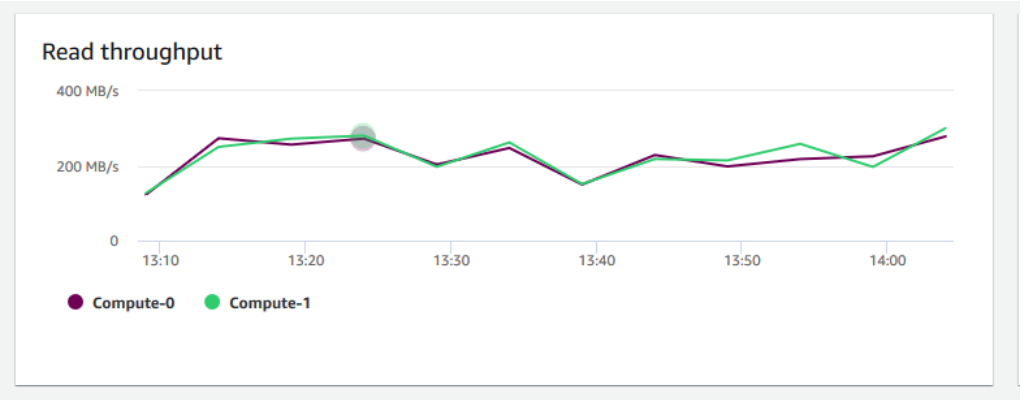
- Maintenance mode（维护模式）– 通过使用 `On` 和 `Off` 指示灯显示集群在所选时间是否处于维护模式。您可以查看集群正在进行维护的时间。然后，您可以将此时间与对集群执行的操作相关联，以估计其将来发生重复性事件的停机时间。



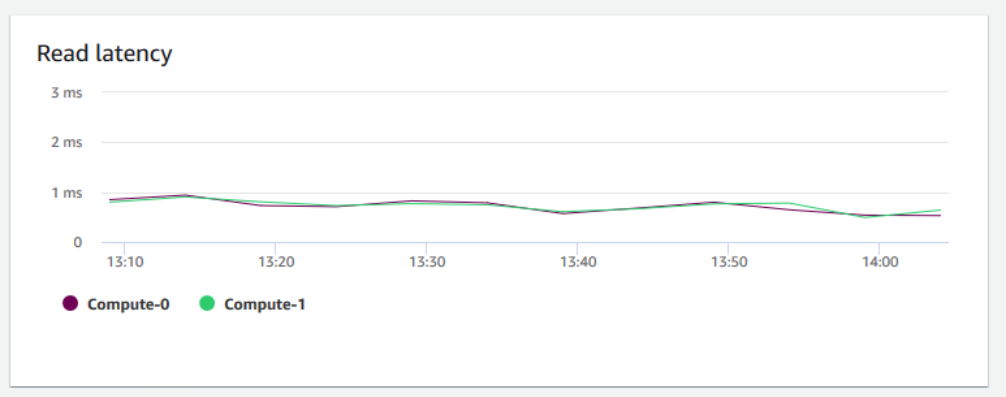
- Percentage disk space used（已使用磁盘空间的百分比）– 显示每个计算节点（而不是整个集群）的磁盘空间使用量百分比。您可以浏览此图表来监控磁盘利用率。VACUUM 和 COPY 等维护操作使用中间临时存储空间来执行排序操作，因此预计磁盘使用量会出现峰值。



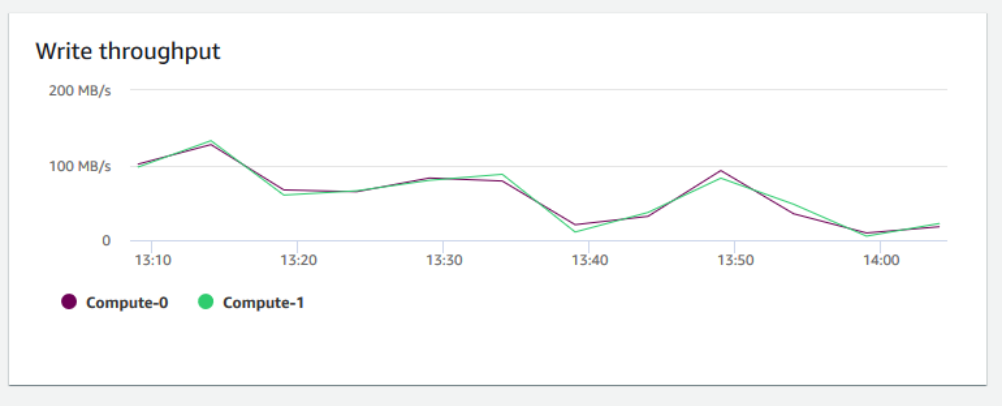
- Read throughput（读取吞吐量）– 显示每秒从磁盘读取的平均兆字节数。您可以评估此图表以监控集群的相应物理方面。此吞吐量不包括集群中的实例与集群的卷之间的网络流量。



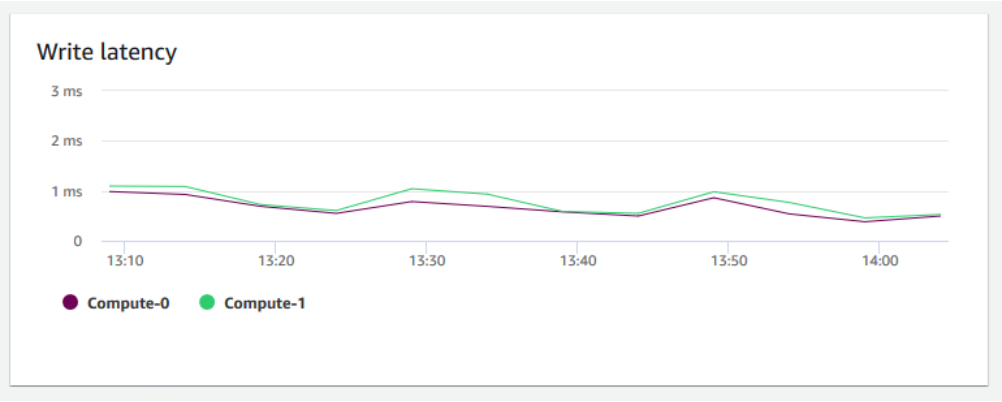
- Read latency（读取延迟）– 显示磁盘读取输入/输出操作所花费的平均时间（以毫秒为单位）。您可以查看要返回的数据的响应时间。当延迟很高时，这意味着发送方处于空闲状态的时间会更多（不发送任何新的数据包），这会降低吞吐量的增长速度。



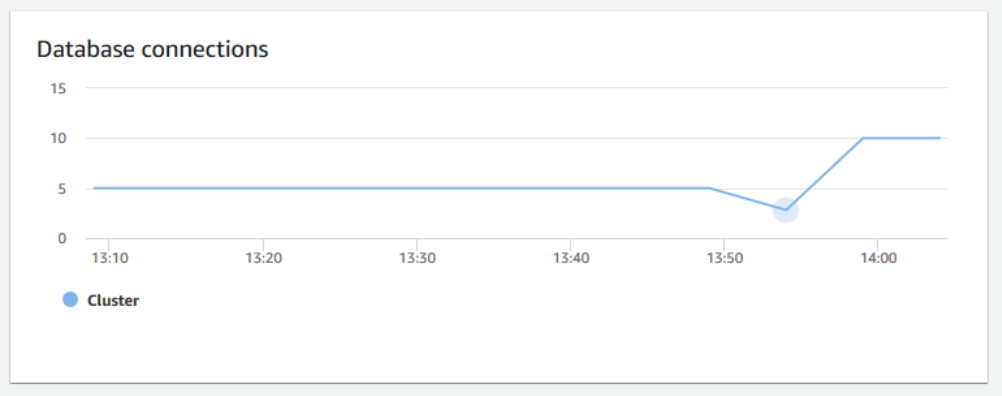
- Write throughput（写入吞吐量）– 显示每秒写入磁盘的平均兆字节数。您可以评估此指标，以监控集群的相应物理方面。此吞吐量不包括集群中的实例与集群的卷之间的网络流量。



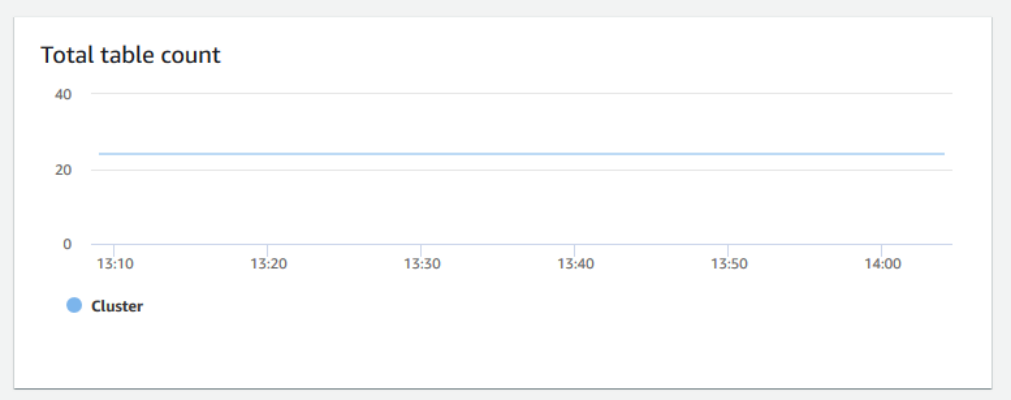
- Write latency（写入延迟）– 显示磁盘写入输入/输出操作所花费的平均时间（以毫秒为单位）。您可以评估返回写确认的时间。当延迟很高时，这意味着发送方处于空闲状态的时间会更多（不发送任何新的数据包），这会降低吞吐量的增长速度。



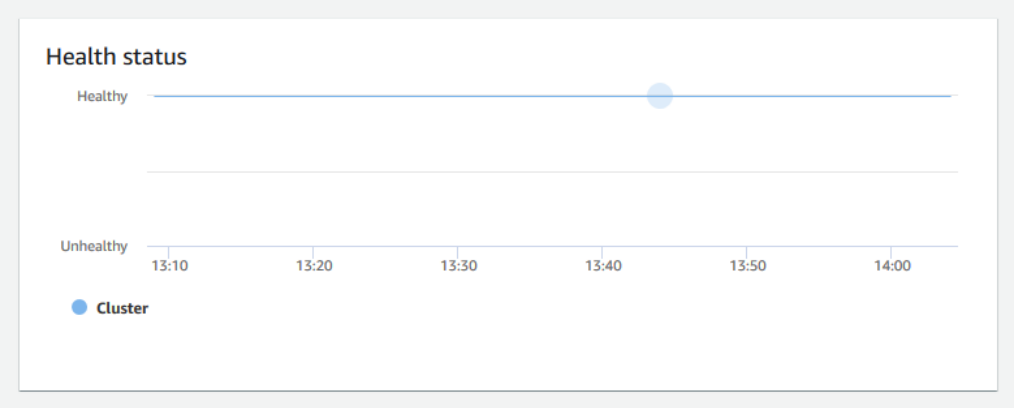
- Database connections（数据库连接数）– 显示到集群的数据库连接数。您可以使用此图表查看与数据库建立的连接数，并查找集群使用率最低的时间。



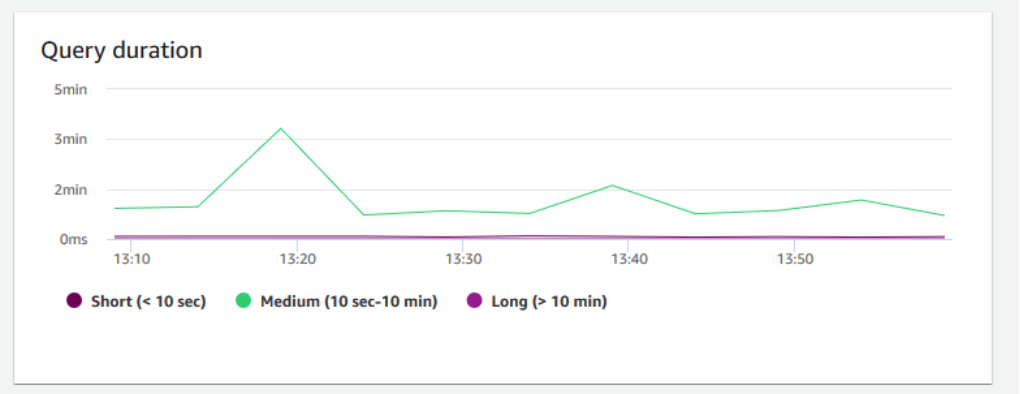
- Total table count（总的表计数）– 显示集群内在某个特定时间点打开的用户表的数量。您可以在打开的表计数较高时监控集群性能。



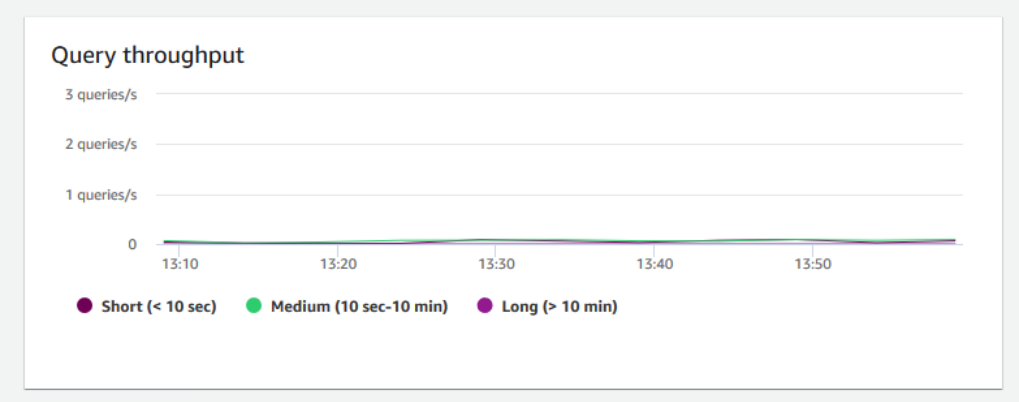
- Health status（运行状况）– 将集群的运行状况指示为 `Healthy` 或 `Unhealthy`。如果集群可以连接到其数据库并成功执行简单查询，则集群将被视为运行状况良好。否则，视为集群运行状况不佳。当数据库集群负载极重，或者集群上的数据库存在配置问题时，集群会出现运营状况不佳的情况。



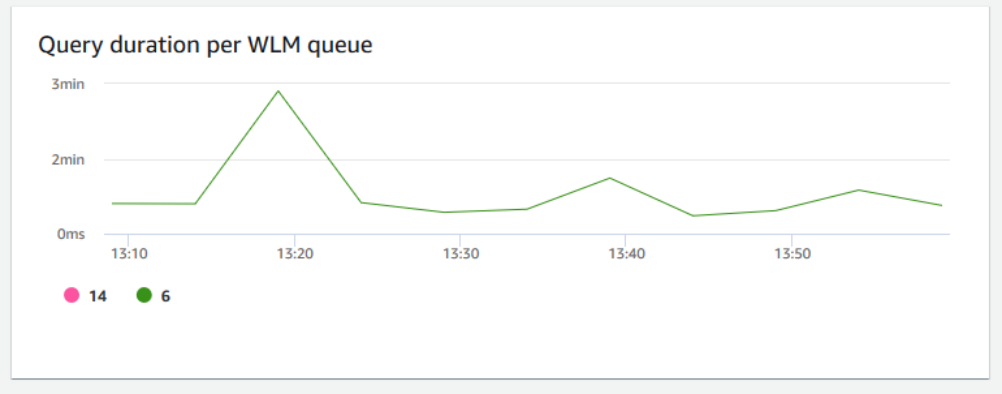
- Query duration（查询持续时间）– 显示完成查询的平均时间量（以微秒为单位）。您可以将此图表上的数据作为基准以衡量集群内的 I/O 性能，并在必要时调整其最耗时的查询。



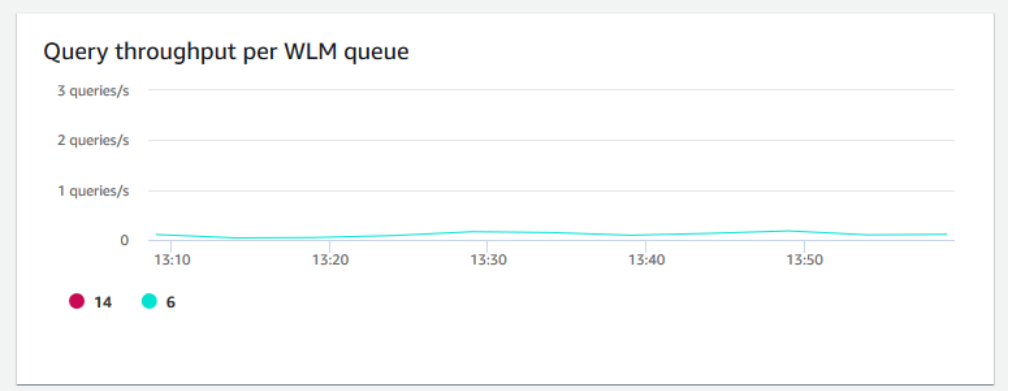
- Query throughput（查询吞吐量）– 显示每秒完成的查询的平均数。您可以分析此图表上的数据以衡量数据库性能，并表明系统以均衡的方式支持多用户工作负载的能力。



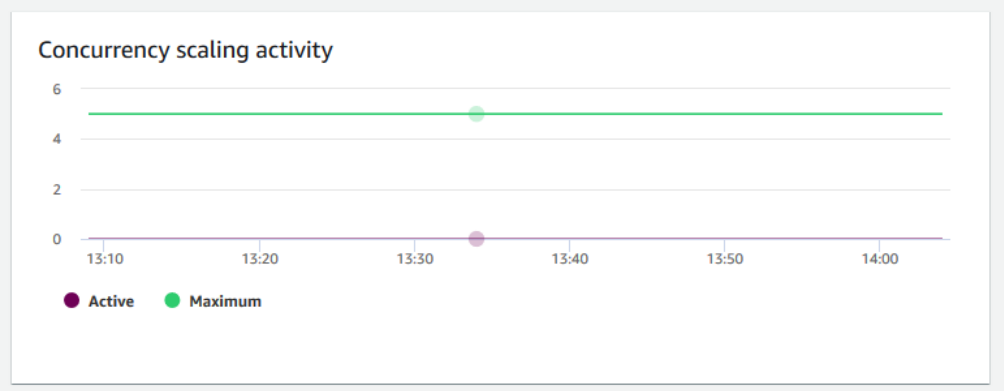
- Query duration per WLM queue（每个 WLM 队列的查询持续时间）– 显示完成查询的平均时间量（以微秒为单位）。您可以将此图表上的数据作为基准测试，以衡量每个 WLM 队列的 I/O 性能，并在必要时调整其最耗时的查询。



- Query throughput per WLM queue（每个 WLM 队列的查询吞吐量）– 显示每秒完成的查询的平均数。您可以分析此图表上的数据，以衡量每个 WLM 队列的数据库性能。



- Concurrency scaling activity（并发扩缩活动）– 显示活动的并发扩展集群的数量。启用并发扩展后，Amazon Redshift 会在需要时自动增加额外的集群容量来处理增多的并发读取查询。



查看查询历史记录

您可以使用 Amazon Redshift 中的查询历史记录指标执行以下操作：

- 隔离和诊断查询性能问题。
- 比较同一时间线上的查询运行时间指标和集群性能指标，以查看这两者之间可能相关的程度。这样做有助于识别性能不佳的查询，寻找瓶颈查询和确定您是否需要为您的工作负载调整集群大小。
- 通过在时间线中选择特定查询，向下钻取到该查询的详细信息。当 Query ID (查询 ID) 和其他属性显示在此图表下方的行中时，您可以选择查询以查看查询详细信息。详细信息包括如查询的 SQL 语句、执行详细信息和查询计划等。有关更多信息，请参阅查看查询详细信息 (p. 495)。
- 确定加载作业是否成功完成并满足服务等级协议 (SLA)。

显示查询历史记录数据

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后从列表中选择集群名称以打开其详细信息。此时将显示集群的详细信息，其中包括 Cluster performance（集群性能）、Query monitoring（查询监控）、Databases（数据库）、Datashares（数据共享）、Schedules（计划）、Maintenance（维护）和 Properties（属性）选项卡。
3. 为查询相关指标选择 Query monitoring (查询监控) 选项卡。
4. 在 Query monitoring (查询监控) 部分中，选择 Query history (查询历史记录) 选项卡。

   使用窗口上的控件，您可以在 Query list (查询列表) 和 Cluster metrics (集群指标) 之间切换。

   选择 Query list (查询列表) 时，该选项卡包括以下图表：

   - Query runtime（查询运行时间）– 时间线上的查询活动。使用此图表可查看哪些查询在同一时间范围内运行。选择查询以查看更多查询执行详细信息。x 轴显示选定的期间。您可以通过正在运行、已完成、加载等筛选图形化的查询。每个条形表示一个查询，条形的长度表示其运行时间（从条形开始到结束）。查询可以包括 SQL 数据操作语句（如 SELECT、INSERT、DELETE）和加载（如 COPY）。原定设置情况下，显示所选时间段内运行时间最长的前 100 个查询。
   - Queries and loads（查询和加载）– 集群上运行的查询和加载列表。此窗口包含一个选项，用于在查询当前正在运行时 Terminate query (终止查询)。

   选择 Cluster metrics (集群指标) 时，该选项卡包括以下图表：

   - Query runtime（查询运行时间）– 时间线上的查询活动。使用此图表可查看哪些查询在同一时间范围内运行。选择查询以查看更多查询执行详细信息。

- CPU utilization（CPU 利用率）– 按领导节点以及计算节点平均值分列的集群 CPU 利用率。
- Storage capacity used（已使用的存储容量）– 已使用的存储容量百分比。
- Active database connections（活动的数据库连接数）– 显示到集群的活动的数据库连接数。

处理查询历史记录图表时，请考虑以下事项：

- 选择一个在 Query runtime (查询运行时间) 图表上表示某特定查询的条形，以查看有关该查询的详细信息。也可以在 Queries and loads (查询和加载) 列表中选择查询 ID 以查看其详细信息。
- 您可以轻扫以选择 Query runtime (查询运行时间) 图表的某个部分进行放大以显示特定时间段。
- 在 Query runtime (查询运行时间) 图表上，要使所选筛选条件考虑所有数据，请向前翻动 Queries and loads (查询和加载) 列表中列出的所有页面。
- 您可以使用通过设置齿轮图标显示的首选项窗口更改显示在 Queries and loads（查询和加载）列表上的列和行数。
- Queries and loads（查询和加载）列表也可以通过从左侧导航器导航 Queries（查询）图标、Queries and loads（查询和加载）来显示。有关更多信息，请参阅查看查询和加载 (p. 494)。

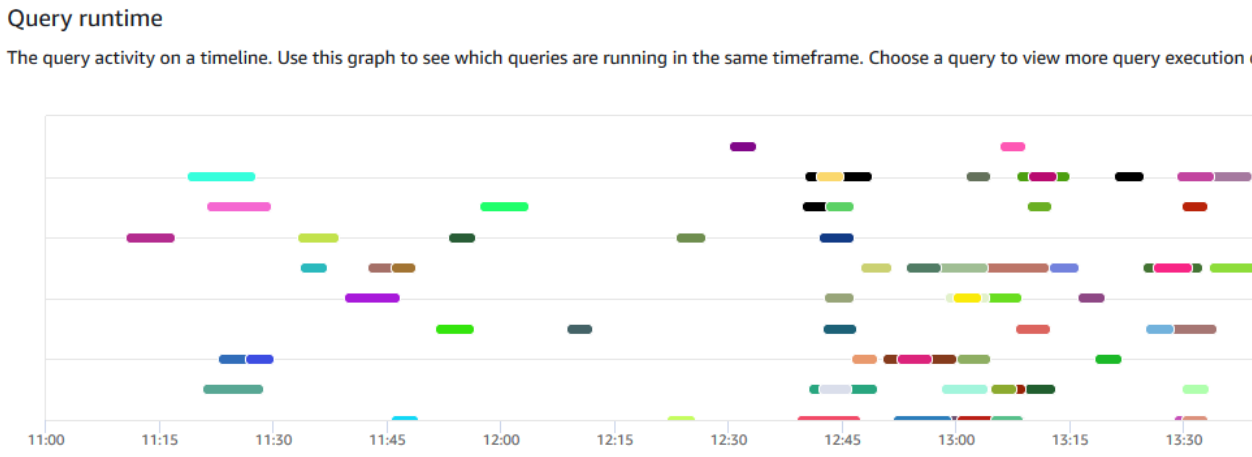
查询历史记录图表

以下示例显示新的 Amazon Redshift 控制台中显示的图表。

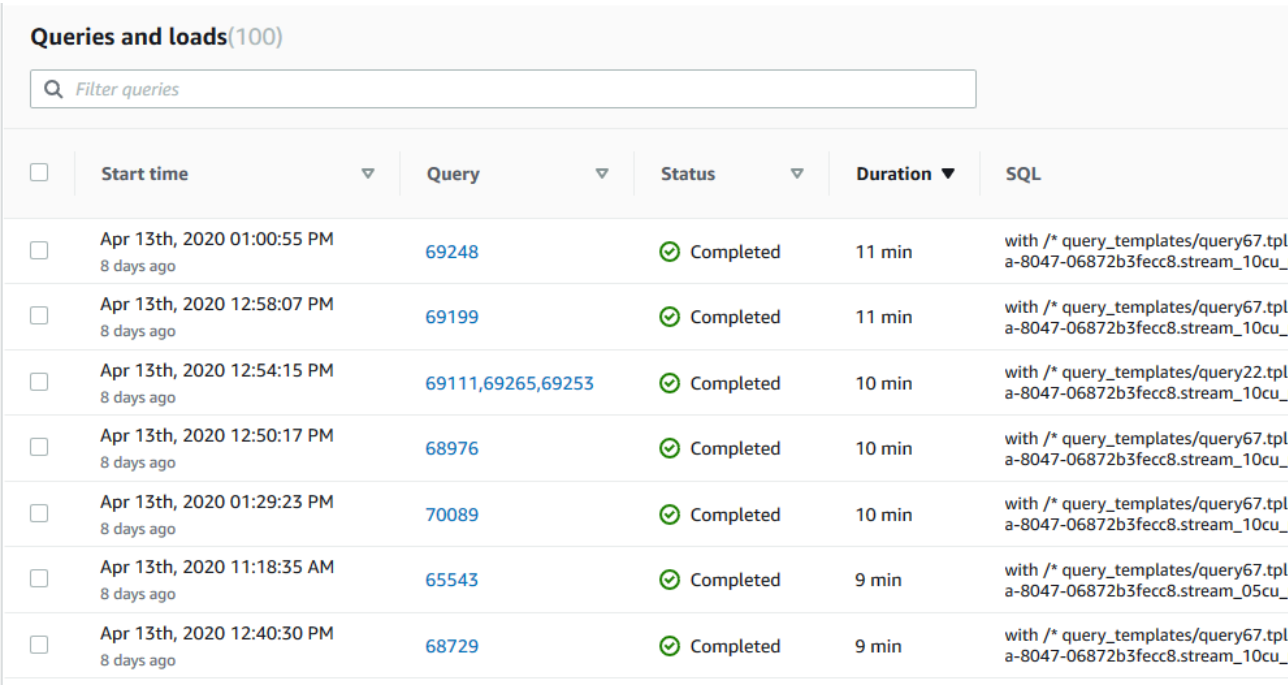
Note

Amazon Redshift 控制台图表仅包含最新 100000 个查询的数据。

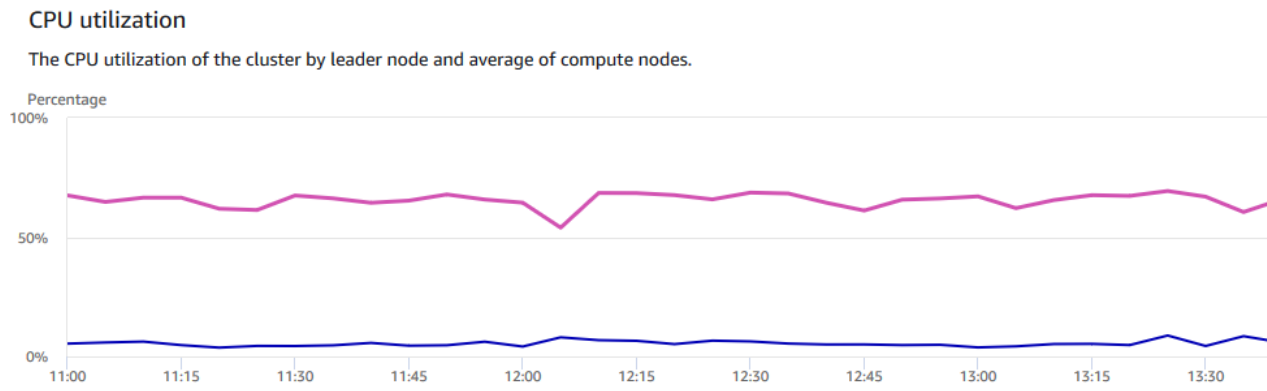
- Query runtime (查询运行时间)



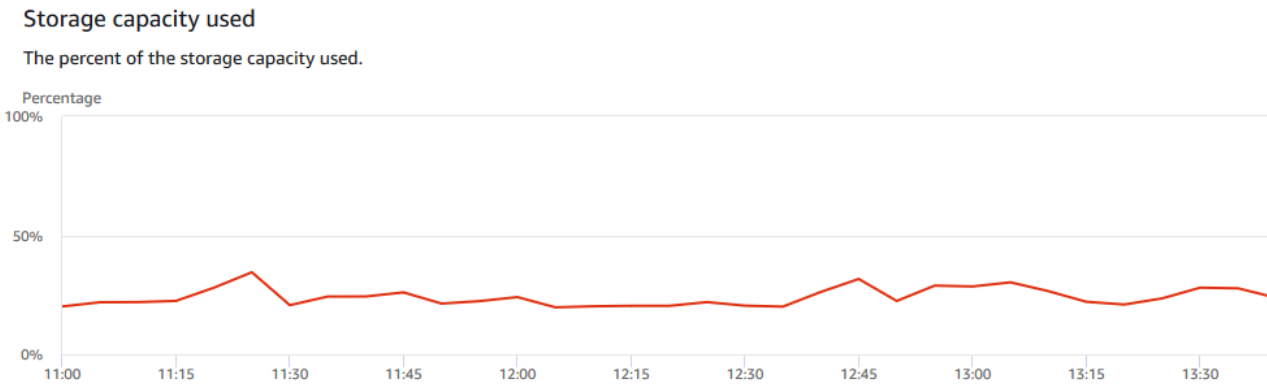
- Queries and loads (查询和加载)



- CPU 使用率



- Storage capacity used (已使用的存储容量)



- Active database connections (活动的数据库连接数)

查看数据库性能数据

您可以使用 Amazon Redshift 中的数据库性能指标执行以下操作：

- 按处理阶段分析查询所花费的时间。您可以在一个阶段花费的时间量中寻找不寻常的趋势。
- 按持续时间范围（短、中、长）分析查询的数量、查询的持续时间和吞吐量。
- 按查询优先级（“最低”、“低”、“正常”、“高”、“最高”、“临界”）查找查询等待时间的趋势。
- 按 WLM 队列查找查询持续时间、吞吐量或等待时间的趋势。

显示数据库性能数据

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后从列表中选择集群名称以打开其详细信息。此时将显示集群的详细信息，包括 Cluster performance（集群性能）、Query monitoring（查询监控）、Databases（数据库）、Datashares（数据共享）、Schedules（计划）、Maintenance（维护）和 Properties（属性）选项卡。
3. 为查询相关指标选择 Query monitoring (查询监控) 选项卡。
4. 在 Query monitoring (查询监控) 部分中，选择 Database performance (数据库性能) 选项卡。

   使用窗口上的控件，您可以在 Cluster metrics (集群指标) 和 WLM queue metrics (WLM 队列指标) 之间切换。

   选择 Cluster metrics (集群指标) 时，该选项卡包括以下图表：

   - Workload execution breakdown（工作负载执行细分）– 查询处理阶段使用的时间。
   - Queries by duration range（按持续时间范围列出的查询）– 短、中和长查询的数量。
   - Query throughput（查询吞吐量）– 每秒完成的平均查询数。
   - Query duration（查询持续时间）– 完成查询的平均时间量。
   - Average queue wait time by priority（按优先级排列的平均队列等待时间）– 按查询优先级排列的查询在 WLM 队列中等待所花费的总时间。

   选择 WLM queue metrics (WLM 队列指标) 时，该选项卡包括以下图表：

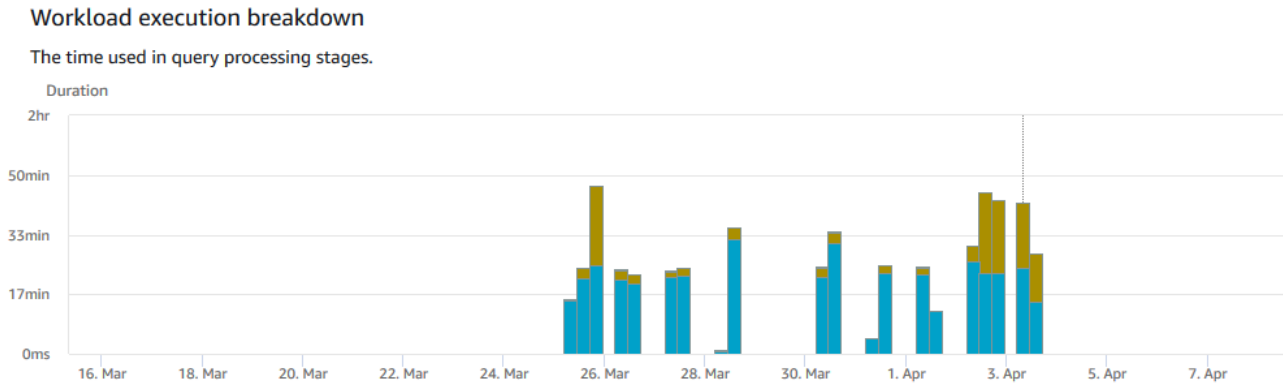
   - Query duration by queue（按队列列出的查询持续时间）– 按 WLM 队列列出的平均查询持续时间。
   - Query throughput by queue（按队列列出的查询吞吐量）– WLM 队列每秒完成的平均查询数。

- Query wait time by queue（按队列列出的查询等待时间）– WLM 队列等待查询所花费的平均持续时间。

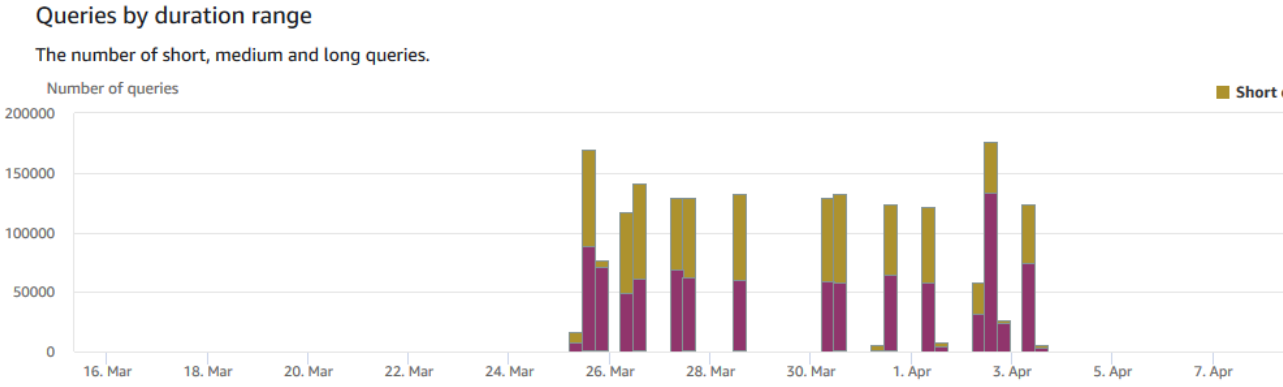
数据库性能图表

以下示例显示新的 Amazon Redshift 控制台中显示的图表。

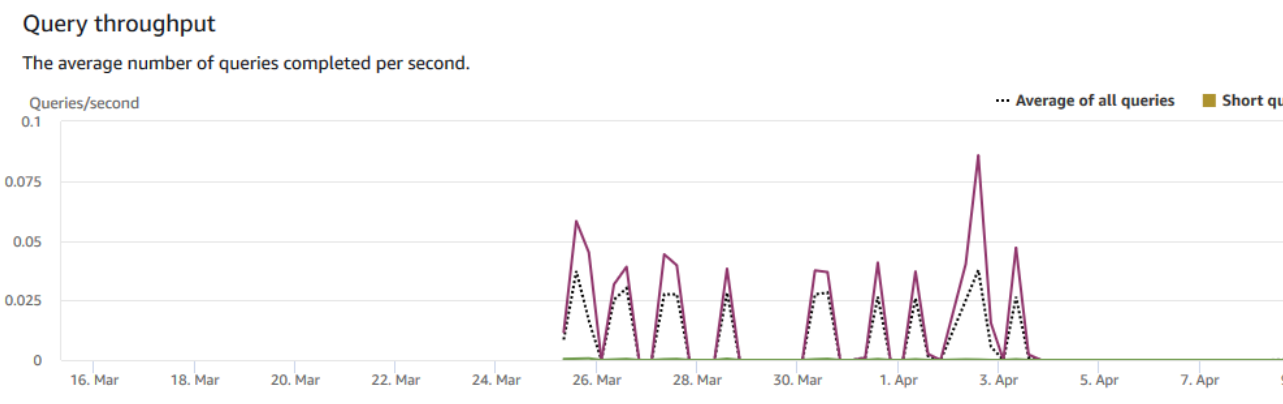
- Workload execution breakdown (工作负载执行细分)



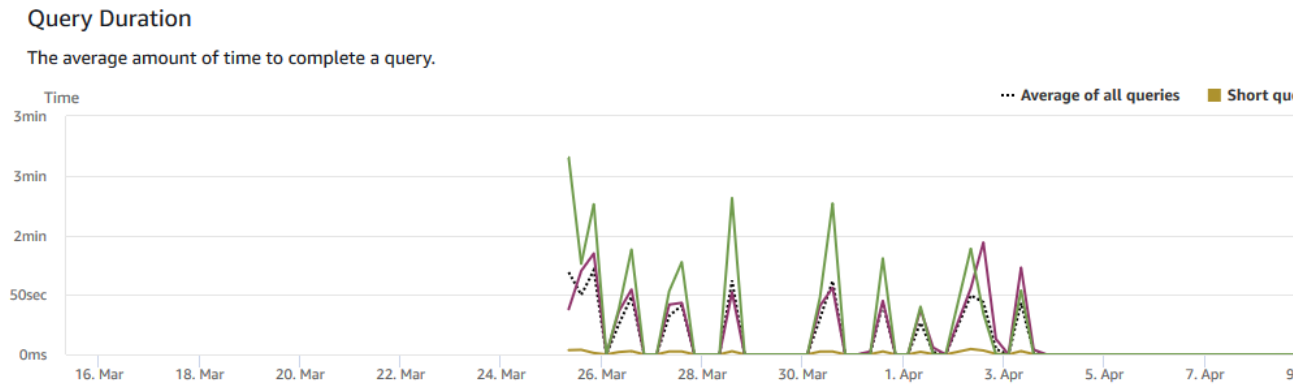
- Queries by duration range (按持续时间范围列出的查询)



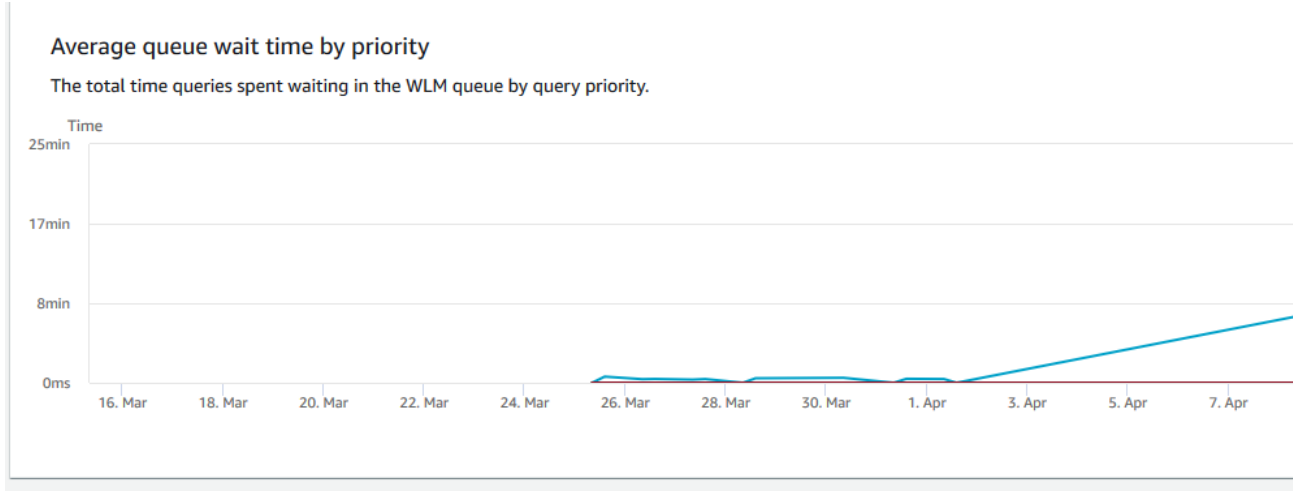
- Query throughput (查询吞吐量)



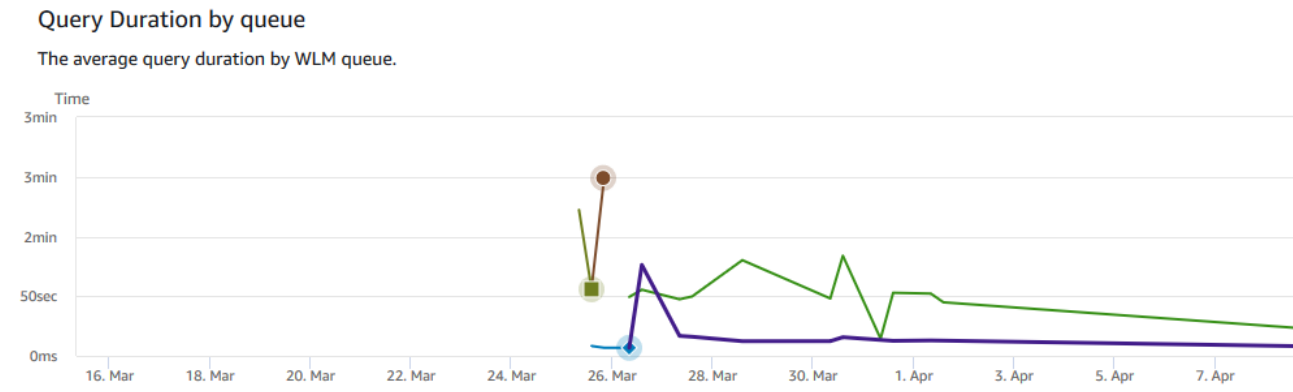
- Query duration (查询持续时间)



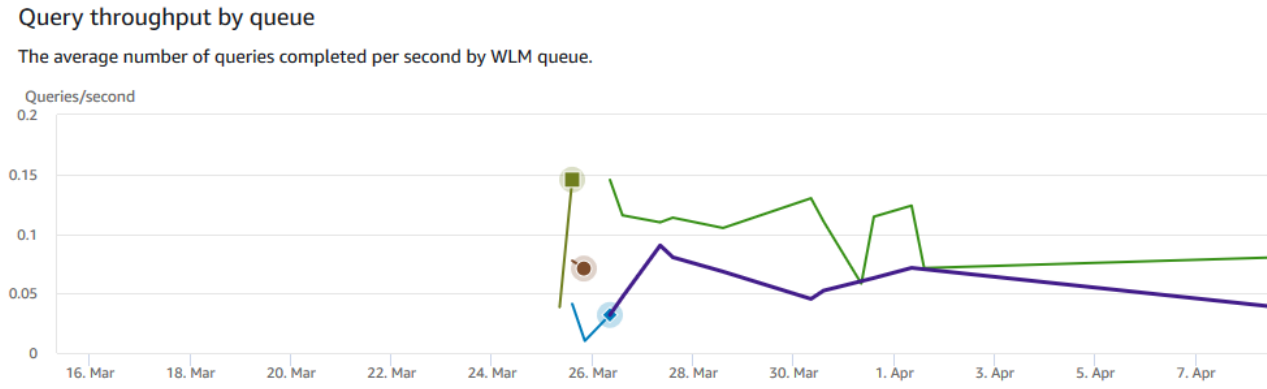
- Average queue wait time by priority (按优先级排列的平均队列等待时间)



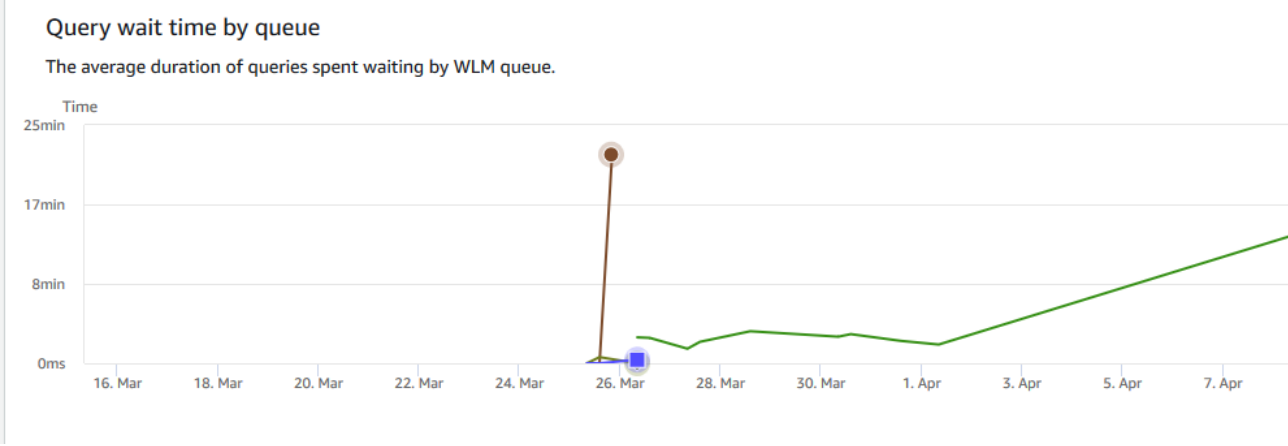
- Query duration by queue (按队列列出的查询持续时间)



- Query throughput by queue (按队列列出的查询吞吐量)



- Query wait time by queue (按队列列出的查询等待时间)



查看工作负载并发和并发扩展数据

通过在 Amazon Redshift 中使用并发扩展指标，您可以执行以下操作：

- 分析是否可以通过启用并发扩展来减少排队查询的数量。您可以按 WLM 队列或针对所有 WLM 队列进行比较。
- 查看并发扩展集群中的并发扩展活动。这可以告诉您并发扩展是否受 `max_concurrency_scaling_clusters` 限制。如果是，您可以选择增加数据库参数中的 `max_concurrency_scaling_clusters`。
- 查看所有并发扩展集群总计并发扩展的总使用率。

显示并发扩展数据

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后从列表中选择集群名称以打开其详细信息。此时将显示集群的详细信息，其中包括 Cluster performance（集群性能）、Query monitoring（查询监控）、Databases（数据库）、Datashares（数据共享）、Schedules（计划）、Maintenance（维护）和 Properties（属性）选项卡。
3. 为查询相关指标选择 Query monitoring (查询监控) 选项卡。
4. 在 Query monitoring (查询监控) 部分中，选择 Workload concurrency (工作负载并发)。

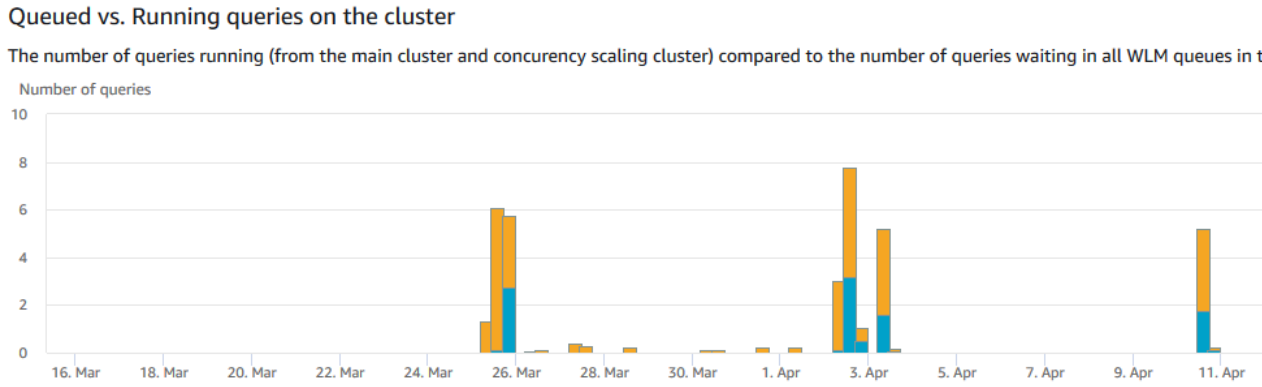
此选项卡包括以下图表：

- Queued vs. Running queries on the cluster（集群上排队的查询数与正在运行的查询数）– 与集群中所有 WLM 队列中等待的查询数量相比，正在运行的查询数量（来自主集群和并发扩展集群）。
- Queued vs. Running queries per queue（每个队列排队的查询数与正在运行的查询数）– 与每个 WLM 队列中等待的查询数量相比，正在运行的查询数量（来自主集群和并发扩展集群）。
- Concurrency scaling activity（并发扩缩活动）– 正在积极处理查询的并发扩展集群的数量。
- Concurrency scaling usage（并发扩展使用情况）– 具有活动的查询处理活动的并发扩展集群的使用情况。

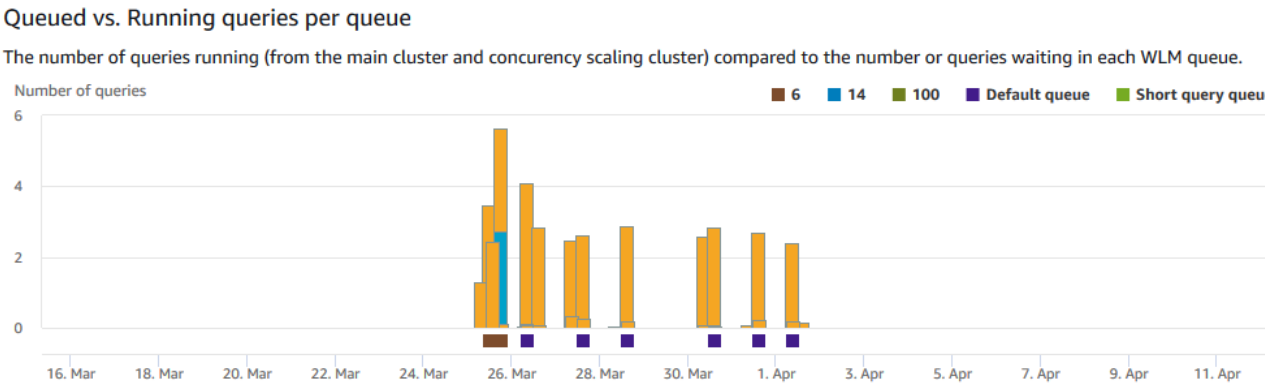
工作负载并发图表

以下示例显示新的 Amazon Redshift 控制台中显示的图表。

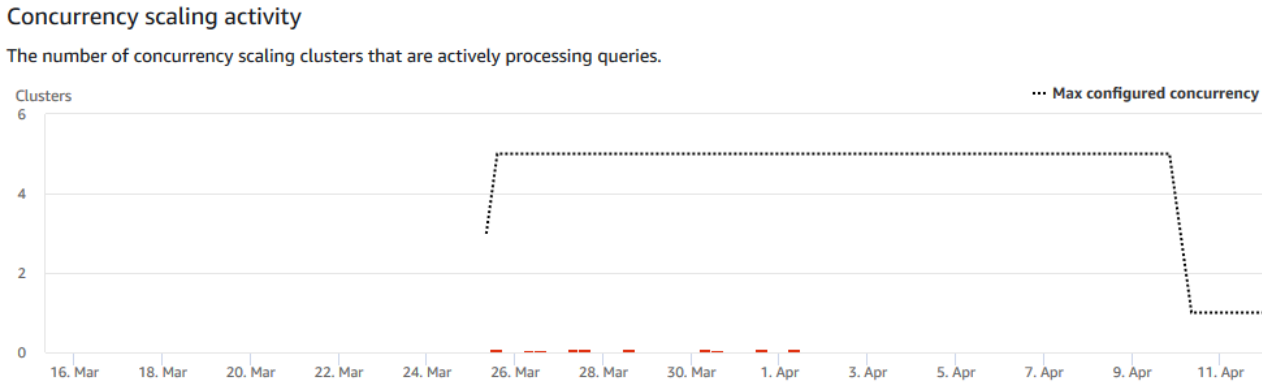
- Queued vs. Running queries on the cluster（集群上排队的查询数与正在运行的查询数）



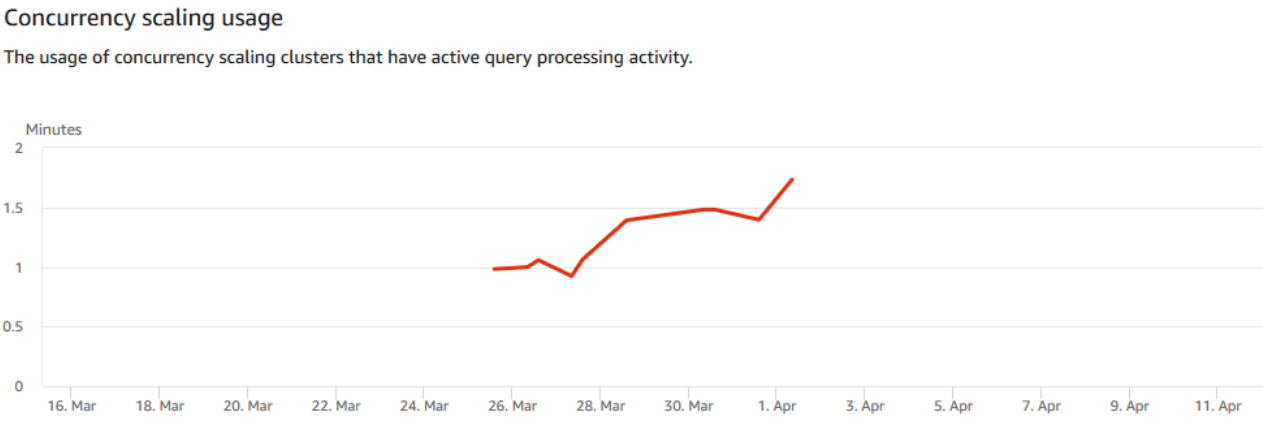
- Queued vs. Running queries per queue（每个队列排队的查询数与正在运行的查询数）



- Concurrency scaling activity (并发扩展活动)



- Concurrency scaling usage (并发扩展使用)



查看查询和加载

Amazon Redshift 控制台提供有关在数据库中运行的查询和加载的信息。您可以使用这些信息确定需要很长时间才能处理的查询以及制造瓶颈来阻止其他查询获得高效处理的查询，并进行问题排查。您可以在 Amazon Redshift 控制台中使用查询信息监控查询处理。

显示查询性能数据

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Queries and loads（查询和加载）以便显示您的账户的查询列表。

   原定设置情况下，该列表显示过去 24 小时中所有集群的查询。您可以在控制台中更改显示日期的范围。

   > **Important**
   >
   > Queries and loads (查询和加载) 选项卡显示系统中运行时间最长的查询，最多显示 100 个查询。

终止运行的查询

您也可以使用 Queries (查询) 页面终止当前正在运行的查询。

> Note
>
> 在 Amazon Redshift 控制台中终止查询和加载需要特定权限。如果您希望用户能够停止查询和加载，请确保将 `redshift:CancelQuerySession` 操作添加到您的 Amazon Identity and Access Management (IAM) 策略。无论您在 IAM 中选择 Amazon Redshift 只读 Amazon 托管策略还是创建自定义策略，此要求都适用。拥有 Amazon Redshift 完全访问策略的用户已具备终止查询和加载所需的权限。有关用于 Amazon Redshift 的 IAM 策略中的操作的更多信息，请参阅管理对资源的访问 (p. 360)。

终止正在运行的查询

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Queries and loads（查询和加载）以便显示您的账户的查询列表。
3. 在列表中选择要终止的正在运行的查询，然后选择 Terminate query (终止查询)。

查看查询详细信息

您可以在 Amazon Redshift 控制台上分析查询详细信息。使用查询标识符，您可以查看查询的详细信息。详细信息可以包括如查询的完成状态、持续时间、SQL 语句以及查询是用户查询还是由 Amazon Redshift 重写的查询。用户查询是从 SQL 客户端提交到 Amazon Redshift 或由业务智能工具生成的查询。Amazon Redshift 可能会重写查询来优化查询，这可能会导致产生多个重写的查询。尽管该过程是由 Amazon Redshift 完成的，但您可以在查询详细信息页面上看到重写的查询以及用户查询。

查看查询

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Queries and loads（查询和加载）以便显示您的账户的查询列表。您可能需要在该页面上更改设置才能找到您的查询。
3. 在列表中选择 Query (查询) 标识符以便显示 Query details (查询详细信息)。

   Query details (查询详细信息) 页面包含 Query details (查询详细信息) 和 Query plan (查询计划) 选项卡以及查询相关指标。

   指标包括有关查询的详细信息，如开始时间、查询 ID、状态和持续时间。其他详细信息包括查询是在主集群上运行还是在并发扩展集群上运行，以及查询是父查询还是重写的查询。

分析查询执行

分析查询

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Queries and loads（查询和加载）以便显示您的账户的查询列表。您可能需要在该页面上更改设置才能找到您的查询。
3. 在列表中选择 Query (查询) 标识符以便显示 Query details (查询详细信息)。

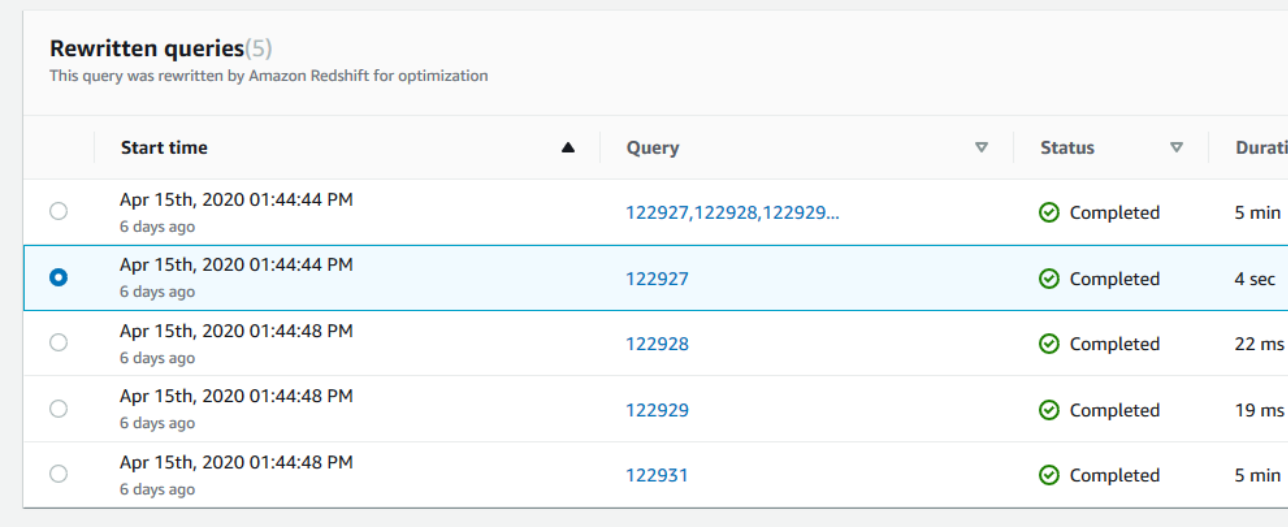
   Query details (查询详细信息) 页面包含 Query details (查询详细信息) 和 Query plan (查询计划) 选项卡以及查询相关指标。

Note

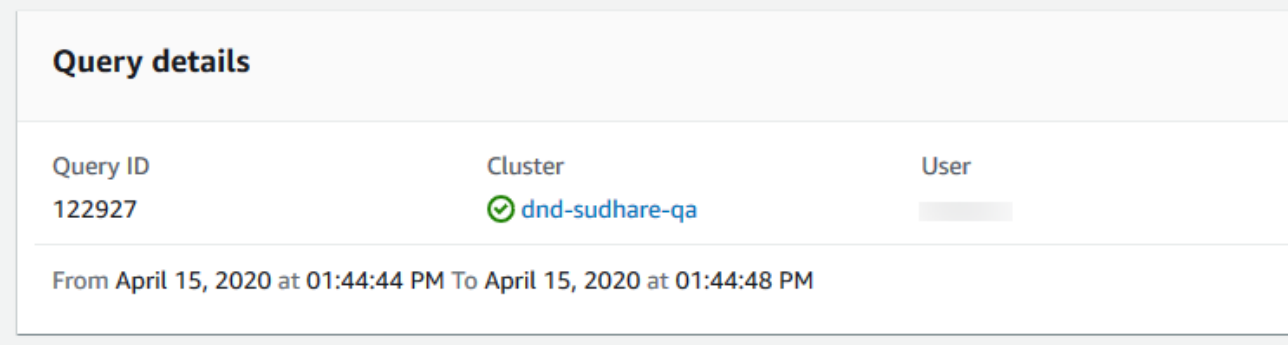
当您向下钻取 Query runtime（查询运行时间）图表中的查询时，您还可以从 Cluster details（集群详细信息）页面、Query history（查询历史记录）选项卡中导航至 Query details（查询详细信息）页面。

Query details (查询详细信息) 页面包含以下部分：

- Rewritten queries (重写查询) 的列表，如以下屏幕截图所示。

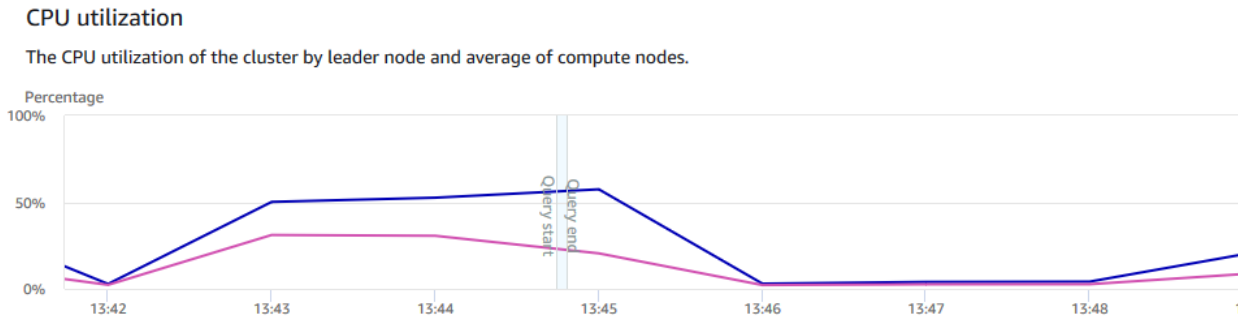


- Query details (查询详细信息) 部分，如以下屏幕截图所示。

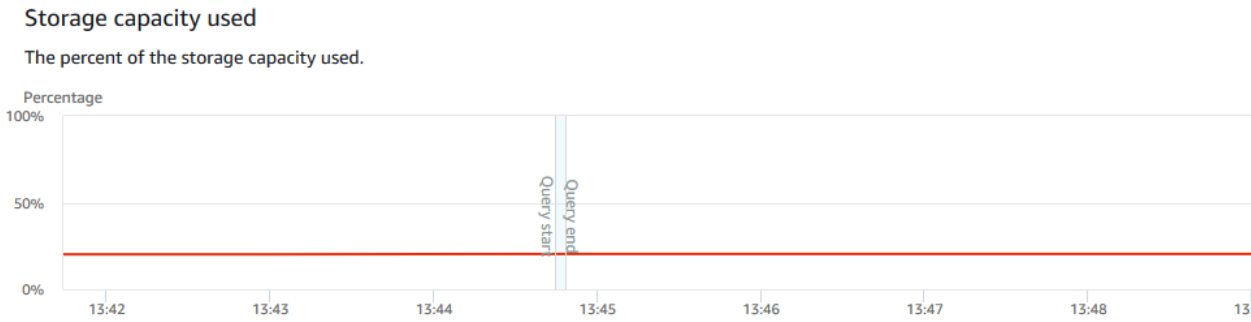


- Query details (查询详细信息) 选项卡，其中包含所运行的 SQL 和有关此运行的 Execution details (执行详细信息)。
- Query plan (查询计划) 选项卡，其中包含 Query plan (查询计划) 步骤和有关此查询计划的其他信息。此表还包含当查询运行时的集群的图表。
  - Cluster health status (集群运行状况)

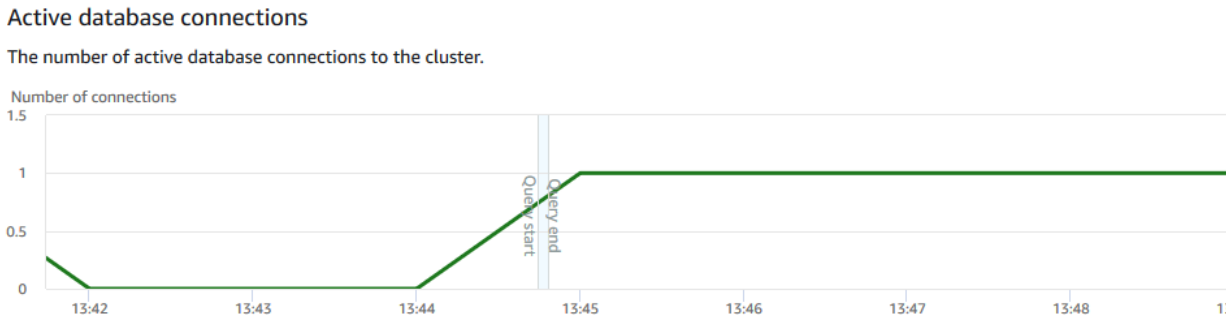
  - CPU 使用率



- Storage capacity used (已使用的存储容量)



- Active database connections (活动的数据库连接数)



查看查询运行时的集群性能

要显示查询运行时的集群性能

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后从列表中选择集群名称以打开其详细信息。此时将显示集群的详细信息，其中包括 Cluster performance（集群性能）、Query monitoring（查询监控）、Databases（数据库）、Datashares（数据共享）、Schedules（计划）、Maintenance（维护）和 Properties（属性）选项卡。
3. 选择 Query monitoring (查询监控) 选项卡以获取更多详细信息。

   有关更多信息，请参阅查看查询历史记录 (p. 486)。

在加载操作期间查看集群指标

在查看加载操作期间的集群性能时，您可以确定消耗资源的查询并采取适当的缓解措施。如果您不希望加载运行完成，则可以将其终止。

Note

在 Amazon Redshift 控制台中终止查询和加载需要特定权限。如果您希望用户能够停止查询和加载，请确保将 `redshift:CancelQuerySession` 操作添加到您的 Amazon Identity and Access Management (IAM) 策略。无论您在 IAM 中选择 Amazon Redshift 只读 Amazon 托管策略还是创建自定义策略，此要求都适用。拥有 Amazon Redshift 完全访问策略的用户已具备终止查询和加载所需的权限。有关用于 Amazon Redshift 的 IAM 策略中的操作的更多信息，请参阅管理对资源的访问 (p. 360)。

显示加载操作期间的集群性能

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后从列表中选择集群名称以打开其详细信息。此时将显示集群的详细信息，其中包括 Cluster performance（集群性能）、Query monitoring（查询监控）、Databases（数据库）、Datashares（数据共享）、Schedules（计划）、Maintenance（维护）和 Properties（属性）选项卡。
3. 选择 Query monitoring (查询监控) 选项卡以获取更多详细信息。
4. 在 Queries and loads (查询和加载) 部分中，选择 Loads (加载) 以便查看集群的加载操作。如果加载正在运行，通过选择 Terminate query (终止查询) 可以终止加载。

分析工作负载性能

您可以通过查看控制台中的工作负载执行细分图表，详细查看工作负载的性能。我们用 QueryRuntimeBreakdown 指标提供的数据生成图表。使用此图表，您可以看到查询在各个处理阶段（如等待和规划）中花费的时间。

Note

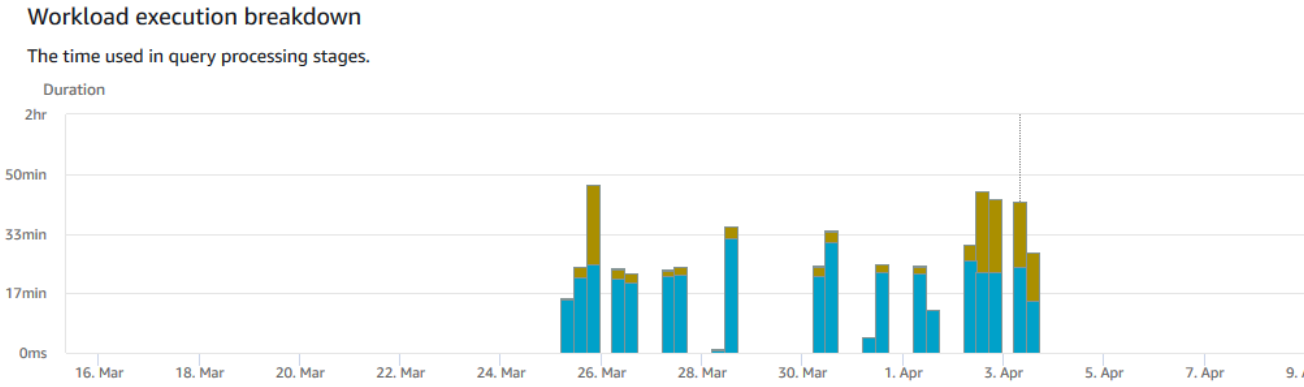
未显示单节点集群的工作负载执行细分图表。

下面的指标列表描述了各个处理阶段：

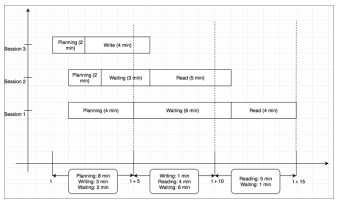
- `QueryPlanning`：分析和优化 SQL 语句所花的时间。
- `QueryWaiting`：在工作负载管理 (WLM) 队列中等待的时间。
- `QueryExecutingRead`：运行读取查询所花的时间。
- `QueryExecutingInsert`：运行插入查询所花的时间。
- `QueryExecutingDelete`：运行删除查询所花的时间。
- `QueryExecutingUpdate`：运行更新查询所花的时间。
- `QueryExecutingCtas`：运行 CREATE TABLE AS 查询所花的时间。
- `QueryExecutingUnload`：运行卸载查询所花的时间。
- `QueryExecutingCopy`：运行复制查询所花的时间。

例如，Amazon Redshift 控制台中的以下图表显示了查询在计划、等待、读取和写入阶段花费的时间量。您可以将此图表中的结果与其他指标组合以进行进一步分析。在某些情况下，您的图表可能显示具有较短持续时间（由 `QueryDuration` 指标度量）的查询在等待阶段花费了较长时间。在这些情况下，您可以增加特定队列的 WLM 并发速率以提高吞吐量。

以下是工作负载执行细分图的示例。在该图中，y 轴值是指定时间内每个阶段的平均持续时间，显示为堆叠条形图。



下图说明了 Amazon Redshift 如何聚合并发会话的查询处理。



显示集群工作负载细分图表

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Clusters（集群），然后从列表中选择集群名称以打开其详细信息。此时将显示集群的详细信息，其中包括 Cluster performance（集群性能）、Query monitoring（查询监控）、Databases（数据库）、Datashares（数据共享）、Schedules（计划）、Maintenance（维护）和 Properties（属性）选项卡。
3. 为查询相关指标选择 Query monitoring (查询监控) 选项卡。
4. 在 Query monitoring (查询监控) 部分中，选择 Database performance (数据库性能) 和 Cluster metrics (集群指标)。

   以堆积条形图的形式绘制以下指标在所选时间范围内的图形：

   - Plan (计划) 时间
   - Wait (等待) 时间
   - Commit (提交) 时间
   - Execution (执行) 时间

管理警报

您在 Amazon Redshift 控制台中创建的警报是 CloudWatch 警报。这些警报有助于您针对集群及其数据库做出积极主动的决策。您可以针对 使用 CloudWatch 指标监控 Amazon Redshift (p. 472)中列出的任意指标设置一个或多个警报。例如，针对集群节点设置高 `CPUUtilization` 警报有助于在该节点过度使用的情况下发出指示。同样，针对集群节点设置低 `CPUUtilization` 警报有助于在该节点未充分利用的情况下发出指示。

从 Actions（操作）中，您可以修改或删除警报。您还可以创建 chime 或 slack 提示，以通过指定 Slack 或 Amazon Chime Webhook URL 将提示从 CloudWatch 发送到 Slack 或 Amazon Chime。

在本节中，您可以了解如何使用 Amazon Redshift 控制台创建告警。您可使用 CloudWatch 控制台或您用于指标的任何其他方法（如使用 Amazon CLI 或 Amazon 开发工具包）创建告警。

要使用 Amazon Redshift 控制台创建 CloudWatch 告警

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单中，选择 Alarms（告警），然后选择 Create alarm（创建告警）。
3. 在 Create alarm（创建告警）页面上，输入相应属性以创建 CloudWatch 告警。
4. 选择Create alarm（创建警报）。

在 CloudWatch 控制台中使用性能指标

在 CloudWatch 控制台中使用 Amazon Redshift 指标时，请注意以下事项：

- 查询和加载性能数据只能通过 Amazon Redshift 控制台访问。
- CloudWatch 中的一些指标使用的单位与 Amazon Redshift 控制台不同。例如，`WriteThroughput` 以 GB/s 显示（而在 CloudWatch 中，则以 Bytes/s 显示），该单位与典型的节点存储空间的相关性更高。

使用 CloudWatch 控制台中的 Amazon Redshift 指标、命令行工具或 Amazon 开发工具包时，请注意以下概念：

1. 首先，指定使用的指标维度。维度是帮助您对某指标进行唯一标识的名称/值对。Amazon Redshift 的维度为 `ClusterIdentifier` 和 `NodeID`。CloudWatch 控制台中提供了 `Redshift Cluster` 和 `Redshift Node` 视图，以便您可以轻松选择特定于集群的维度和特定于节点的维度。有关维度的更多信息，请参阅 CloudWatch 开发人员指南中的维度。
2. 接下来，指定指标名称，例如 `ReadIOPS`。

下表总结了可供您使用的 Amazon Redshift 指标维度的类型。根据指标，每隔 1 分钟或 5 分钟免费提供一次数据。有关更多信息，请参阅Amazon Redshift 指标 (p. 473)。

CloudWatch 命名空间	维度	描述
`AWS/Redshift`	`NodeID`	筛选条件请求的特定于集群节点的数据。`NodeID` 是“领导”、“共享”或“N 计算”，其中 N 是集群中节点的数目（0、1 等）。“共享”意味着集群只有一个节点，即领导节点和计算节点合并到了一起。
	`ClusterIdentifie`	筛选条件请求的特定于集群的数据。特定于集群的指标包括 `HealthStatus`、`MaintenanceMode` 和 `DatabaseConnections`。此维度的一般指标 (例如，`ReadIOPS`) 同样是表示节点指标数据聚合的节点的指标。在解析这些指标时请小心，因为它们是领导节点和计算节点的聚合行为。

网关和卷指标的使用方式类似于其他服务指标。许多常见任务在 CloudWatch 文档中进行了概述，其中包括：

- 查看可用的指标
- 获取指标的统计数据
- 创建 CloudWatch 告警

Amazon Redshift 事件

主题

- Overview (p. 501)
- 使用控制台查看事件 (p. 501)
- 使用 Amazon SDK for Java 查看事件 (p. 501)
- 使用 Amazon CLI 和 Amazon Redshift API 查看事件 (p. 503)
- Amazon Redshift 事件通知 (p. 503)

Overview

Amazon Redshift 跟踪事件并在您的 Amazon 账户中将事件的相关信息保留几周。对于每个事件，Amazon Redshift 会报告事件发生日期、描述、事件源（例如，集群、参数组或快照）和源 ID 等信息。

Amazon Redshift 为某些事件提前提供通知。这些事件的事件类别是 `pending`。例如，如果集群中的一个节点需要硬件更新，我们会发送预先通知。您可以订阅与其他 Amazon Redshift 事件相同的待处理事件。有关更多信息，请参阅订阅 Amazon Redshift 事件通知 (p. 504)。

您可以使用 Amazon Redshift 管理控制台、Amazon Redshift API 或 Amazon 开发工具包以获取事件信息。您可以获取所有事件的列表，也可以应用筛选条件（如事件持续时间或开始和结束日期）以获取特定时间段的事件信息。

您还可以获取由特定源类型生成的事件，如集群事件或参数组事件。Source（源）列显示触发给定操作的资源名称和资源类型。

您可以创建 Amazon Redshift 事件通知订阅以指定一组事件筛选器。当发生与筛选条件匹配的事件时，Amazon Redshift 将使用 Amazon Simple Notification Service 主动通知您发生了该事件。

有关按源类型和类别筛选的 Amazon Redshift 事件列表，请参阅the section called “Amazon Redshift 事件类别和事件消息” (p. 505)

使用控制台查看事件

查看事件

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Events（事件）。

使用 Amazon SDK for Java 查看事件

以下示例列出了指定集群的事件以及指定事件源类型。本示例展示了如何使用分页。

有关运行以下示例的分步说明，请参阅 使用 Eclipse 运行 Amazon Redshift 的 Java 示例 (p. 464)。您需要更新代码并指定集群标识符和事件源类型。

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
```

```
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
*/

// snippet-sourcedescription:[ListEvents demonstrates how to list Amazon Redshift events.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[DescribeEvents]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-01-31]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.ListEvents.complete]

package com.amazonaws.services.redshift;

import java.util.Date;
import java.io.IOException;


import com.amazonaws.services.redshift.model.*;

public class ListEvents {

    public static AmazonRedshift client;
    public static String clusterIdentifier = "***provide cluster identifier***";
    public static String eventSourceType = "cluster"; // e.g. cluster-snapshot

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
 com.amazonaws.auth.DefaultAWSCredentialsProviderChain}

       client = AmazonRedshiftClientBuilder.defaultClient();

        try {
             listEvents();
        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }

    private static void listEvents() {
        long oneWeeksAgoMilli = (new Date()).getTime() - (7L*24L*60L*60L*1000L);
        Date oneWeekAgo = new Date();
        oneWeekAgo.setTime(oneWeeksAgoMilli);
        String marker = null;

        do {
            DescribeEventsRequest request = new DescribeEventsRequest()
            .withSourceIdentifier(clusterIdentifier)
            .withSourceType(eventSourceType)
            .withStartTime(oneWeekAgo)
            .withMaxRecords(20);
            DescribeEventsResult result = client.describeEvents(request);
            marker = result.getMarker();
            for (Event event : result.getEvents()) {
                printEvent(event);
```

```
            }
        } while (marker != null);


    }
    static void printEvent(Event event)
    {
        if (event == null)
        {
            System.out.println("\nEvent object is null.");
            return;
        }

        System.out.println("\nEvent metadata:\n");
        System.out.format("SourceID: %s\n", event.getSourceIdentifier());
        System.out.format("Type: %s\n", event.getSourceType());
        System.out.format("Message: %s\n", event.getMessage());
        System.out.format("Date: %s\n", event.getDate());
    }
}// snippet-end:[redshift.java.ListEvents.complete]
```

使用 Amazon CLI 和 Amazon Redshift API 查看事件

您可以通过以下 Amazon Redshift CLI 操作来管理事件。

- describe-events

Amazon Redshift 提供以下 API 来查看事件。

- DescribeEvents

Amazon Redshift 事件通知

概览

Amazon Redshift 使用 Amazon Simple Notification Service (Amazon SNS) 传输 Amazon Redshift 事件的通知。创建 Amazon Redshift 事件订阅即可启用通知。在 Amazon Redshift 订阅中，您需要为 Amazon Redshift 事件和 Amazon SNS 主题指定一组筛选条件。每当发生与筛选条件匹配的事件时，Amazon Redshift 就会向 Amazon SNS 主题发布通知消息。然后，Amazon SNS 会将消息传输给任何拥有 Amazon SNS 主题订阅的 Amazon SNS 使用者。发送给 Amazon SNS 使用者的消息可以采用 Amazon 区域的 Amazon SNS 支持的任何形式，如电子邮件、文本消息或对 HTTP 端点的调用。例如，所有区域都支持电子邮件通知，但 SMS 通知只能在美国东部（弗吉尼亚北部）区域中进行创建。

创建事件通知订阅时，您需要指定一个或多个事件筛选条件。每当发生与所有筛选条件匹配的事件时，Amazon Redshift 就会通过该订阅发送通知。筛选条件包含源类型（例如集群或快照）、源 ID（例如集群或快照的名称）、事件类别（例如监控或安全）和事件严重性（例如 INFO 或 ERROR）。

您可以将 Amazon Web Services Management Console中的 Enabled（已启用）单选按钮设置为 `No`，或者使用 Amazon Redshift CLI 或 API 将 `Enabled` 参数设置为 `false`，从而轻松地关闭通知而无需删除订阅。

Amazon Redshift 事件通知的账单是通过 Amazon Simple Notification Service（Amazon SNS）发出的。Amazon SNS 费用在使用事件通知时适用；有关 Amazon SNS 账单的更多信息，请转至 Amazon Simple Notification Service 定价。

您还可以使用管理控制台查看已发生的 Amazon Redshift 事件。有关更多信息，请参阅Amazon Redshift 事件 (p. 501)。

主题

- 订阅 Amazon Redshift 事件通知 (p. 504)

订阅 Amazon Redshift 事件通知

您可以创建 Amazon Redshift 事件通知订阅，这样便能在特定集群、快照、安全组或参数组发生事件时收到通知。创建订阅最简单的方式是使用 Amazon SNS 控制台。有关创建和订阅 Amazon SNS 主题的信息，请参阅 Amazon SNS 入门。

您可以创建 Amazon Redshift 事件通知订阅，这样便能在特定集群、快照、安全组或参数组发生事件时收到通知。创建订阅最简单的方式是使用 Amazon Web Services Management Console。如果您选择使用 CLI 或 API 创建事件通知，则必须创建 Amazon Simple Notification Service 主题并订阅有关 Amazon SNS 控制台或 Amazon SNS API 的主题。您还必须保留该主题的 Amazon Resource Name (ARN)，因为在提交 CLI 命令或者 API 操作时会用到。有关创建和订阅 Amazon SNS 主题的信息，请参阅 Amazon SNS 入门。

Amazon Redshift 事件订阅可指定以下事件条件：

- 源类型，值是集群、快照、参数组和安全组。
- 资源的源 ID，例如 `my-cluster-1` 或 `my-snapshot-20130823`。该 ID 所属的资源必须位于与事件订阅相同的 Amazon 区域中。
- “事件”类别的值为“配置”、“管理”、“监控”和“安全性”和“待处理”
- 事件严重性，值是 INFO 或 ERROR。

事件条件可以单独进行指定，只不过您必须先指定源类型，然后才能在控制台中指定源 ID。例如，您可以指定事件类别，而无需指定源类型、源 ID 或严重性。对于不属于在源类型中指定的类型的资源，您可以为其指定源 ID，但系统不会针对来自这些资源的事件发送任何通知。例如，如果您指定了集群源类型和某个安全组的 ID，则该安全组触发的所有事件与相应源类型筛选条件均不匹配，因此系统不会针对这些事件发送任何通知。

Amazon Redshift 会针对任何与在订阅中指定的所有条件匹配的事件发送通知。返回的一系列事件的部分示例：

- 订阅指定的是集群源类型、my-cluster-1 的源 ID、监控类别和 ERROR 严重性。该订阅将仅针对来自 my-cluster-1、严重性为 ERROR 的监控事件发送通知。
- 订阅指定的是集群源类型、配置类别和 INFO 严重性。该订阅将针对来自 Amazon 账户中的任何 Amazon Redshift 集群、严重性为 INFO 的配置事件发送通知。
- 订阅指定的是配置类别和 INFO 严重性。该订阅将针对来自 Amazon 账户中的任何 Amazon Redshift 资源、严重性为 INFO 的配置事件发送通知。
- 订阅指定的是 ERROR 严重性。该订阅将针对来自 Amazon 账户中的任何 Amazon Redshift 资源、严重性为 ERROR 的所有事件发送通知。

如果您在某个现有订阅中删除或重命名其名称被引用为源 ID 的对象，那么该订阅将保持有效，但不会转发来自该对象的任何事件。如果您日后使用该订阅源 ID 中引用的同一名称创建新对象，那么该订阅将会开始针对来自新对象的事件发送通知。

Amazon Redshift 会向 Amazon SNS 主题发布事件通知，该主题由其 Amazon Resource Name (ARN) 标识。当您使用 Amazon Redshift 控制台创建事件订阅时，您可以指定现有 Amazon SNS 主题，也可以请求控制台在创建订阅时创建主题。发送到 Amazon SNS 主题的所有 Amazon Redshift 事件通知均会转发给订阅了该主题的所有 Amazon SNS 使用者。您可以使用 Amazon SNS 控制台对 Amazon SNS 主题进行更改，例如向主题添加使用者订阅或删除主题的使用者订阅。有关创建和订阅 Amazon SNS 主题的更多信息，请转至开始使用 Amazon Simple Notification Service。

下列章节列出了您可以收取通知的所有类型和事件。此外，它还提供有关订阅和使用 Amazon Redshift 事件订阅的详细信息。

Amazon Redshift 事件类别和事件消息

本部分介绍每种 Amazon Redshift 源类型的事件 ID 和类别。

下表显示了集群为源类型时的事件类别和事件列表。

Amazon Redshift 类别	事件 ID	事件严重性	描述
配置	REDSHIFT-EVENT-1000	INFO	参数组 [参数组名称] 已于 [时间] 更新。如果只更改了动态参数，则现在正在修改关联的集群。如果您更改了静态参数，则在重新启动关联集群时将应用所有更新（包括动态参数）。
配置	REDSHIFT-EVENT-1001	INFO	您的 Amazon Redshift 集群 [集群名称] 已于 [时间] 修改为使用参数组 [参数组名称]。
配置	REDSHIFT-EVENT-1500	ERROR (错误)	Amazon VPC [VPC 名称] 不存在。未应用您对集群 [集群名称] 进行的配置更改。请访问 Amazon Web Services Management Console，以解决该问题。
配置	REDSHIFT-EVENT-1501	ERROR (错误)	您为 Amazon VPC [VPC 名称] 指定的客户子网 [子网名称] 不存在或无效。未应用您对集群 [集群名称] 进行的配置更改。请访问 Amazon Web Services Management Console，以解决该问题。
配置	REDSHIFT-EVENT-1502	ERROR (错误)	集群子网组 [子网组名称] 中的子网没有可用的 IP 地址。无法创建集群 [集群名称]。
配置	REDSHIFT-EVENT-1503	ERROR (错误)	Amazon VPC [VPC 名称] 未连接任何互联网网关。未应用您对集群 [集群名称] 进行的配置更改。请访问 Amazon Web Services Management Console，以解决该问题。
配置	REDSHIFT-EVENT-1504	ERROR (错误)	无法访问集群 [集群名称] 的 HSM。
配置	REDSHIFT-EVENT-1505	ERROR (错误)	无法注册集群 [集群名称] 的 HSM。尝试采用其他配置。
配置	REDSHIFT-EVENT-1506	ERROR (错误)	Amazon Redshift 超出了您的账户的弹性网络接口限制。请最多删除 [最大弹性网络接口数] 个弹性网络接口，或请求使用 EC2 增加每个 Amazon 区域的网络接口数限制。
配置	REDSHIFT-EVENT-1509	ERROR (错误)	无法创建 Amazon Redshift 集群 [集群名称]，因为已达到您账户的 VPC 端点限制。删除未使用的 VPC 端点或请求增加 VPC 端点的限制。 有关更多信息，请参阅 Amazon VPC 用户指南中的 VPC 端点。
配置	REDSHIFT-EVENT-1510	ERROR (错误)	我们检测到在 Amazon Redshift 集群 [集群名称] 上加载示例数据的尝试未成功。要加载示例数据，请首先将 VPC 配置为有权访问 Simple Storage Service（Amazon S3）桶，然后创建新集群并加载示例数据。

Amazon Redshift 类别	事件 ID	事件严重性	描述
			有关更多信息，请参阅《Amazon Redshift 集群管理指南》中的启用增强型 VPC 路由。
配置	REDSHIFT-EVENT-1511	ERROR (错误)	无法创建 Amazon Redshift 集群 [集群名称]，因为您已超出您账户中的弹性 IP 地址限制。请删除未使用的弹性 IP 地址，或者使用 Amazon EC2 请求提高限制。
管理	REDSHIFT-EVENT-2000	INFO	您的 Amazon Redshift 集群 [集群名称] 已创建，随时可用。
管理	REDSHIFT-EVENT-2001	INFO	您的 Amazon Redshift 集群 [集群名称] 已于 [时间] 被删除。最终快照 [已/未] 保存。
管理	REDSHIFT-EVENT-2002	INFO	您的 VPC 安全组 [安全组名称] 已于 [时间] 更新。
管理	REDSHIFT-EVENT-2003	INFO	于 [时间] 在 Amazon Redshift 集群 [集群名称] 上开始的维护。该集群在维护期间不可用。
管理	REDSHIFT-EVENT-2004	INFO	于 [时间] 在 Amazon Redshift 集群 [集群名称] 上完成的维护。
管理	REDSHIFT-EVENT-2006	INFO	已于 [时间] 开始调整您的 Amazon Redshift 集群 [集群名称] 的大小。在执行调整大小操作期间，您的集群将处于只读模式。
管理	REDSHIFT-EVENT-2007	INFO	正在调整您的 Amazon Redshift 集群 [集群名称] 的大小。您的集群处于只读模式。
管理	REDSHIFT-EVENT-2008	INFO	已于 [时间] 开始执行还原操作来创建新的 Amazon Redshift 集群 [集群名称] 快照 [快照名称]。要监控还原进度，请访问 Amazon Web Services Management Console。
管理	REDSHIFT-EVENT-2013	INFO	您的 Amazon Redshift 集群 [集群名称] 已于 [时间] 被重命名。
管理	REDSHIFT-EVENT-2014	INFO	收到 Amazon Redshift 集群 [集群名称] 表还原请求。
管理	REDSHIFT-EVENT-2015	INFO	Amazon Redshift 集群 [集群名称] 表还原已于 [时间] 取消。
管理	REDSHIFT-EVENT-2016	INFO	已于 [时间] 开始替换您的 Amazon Redshift 集群 [集群名称]。
管理	REDSHIFT-EVENT-2017	INFO	客户启动了于 [时间] 在 Amazon Redshift 集群 [集群名称] 上开始的维护。该集群在维护期间不可用。
管理	REDSHIFT-EVENT-2018	INFO	客户启动了于 [时间] 在 Amazon Redshift 集群 [集群名称] 上完成的维护。
管理	REDSHIFT-EVENT-2019	ERROR (错误)	客户启动了于 [时间] 在 Amazon Redshift 集群 [集群名称] 上失败的维护。将集群返回到其原始状态。

Amazon Redshift 类别	事件 ID	事件严重性	描述
管理	REDSHIFT-EVENT-2020	INFO	您的 Amazon Redshift 集群 [集群名称] 的跟踪已从 [起点跟踪] 修改为 [目的地跟踪]。
管理	REDSHIFT-EVENT-2021	ERROR (错误)	从我们的容量池获取容量时，Amazon Redshift 集群 [集群名称] 的 [操作] 未成功。我们正在努力获取容量，但目前我们已取消了您的请求。删除此集群并在稍后重试。
管理	REDSHIFT-EVENT-2022	ERROR (错误)	从我们的容量池获取容量时，Amazon Redshift 集群 [集群名称] 的 [操作] 未成功。我们正在努力获取容量，但目前我们已取消了您的请求。容量是在 [备用可用区] 中提供的。请删除该集群，然后在备用可用区中重试。
管理	REDSHIFT-EVENT-2023	ERROR (错误)	我们在您的单节点 Amazon Redshift 集群 [集群名称] 上检测到硬件故障，这可能会导致查询失败或集群间歇性可用。从我们的容量池中获取容量时，更换集群不成功。您需要从快照还原新集群。删除此集群，选择最新的可用快照，然后从该快照还原新集群。这将自动为您预配置正常工作的硬件。
管理	REDSHIFT-EVENT-2024	ERROR (错误)	我们在您的单节点 Amazon Redshift 集群 [集群名称] 上检测到硬件故障，这可能会导致查询失败或集群间歇性可用。从我们的容量池中获取容量时，更换集群不成功。容量是在可用区中提供的：[备用可用区]。删除此集群，选择最新的可用快照，然后从该快照还原新集群。这将自动为您预配置正常工作的硬件。
管理	REDSHIFT-EVENT-3011	INFO	已于 [时间] 开始 Amazon Redshift 集群“[集群名称]”的弹性调整大小操作。在调整大小期间，我们将保持数据库连接。一些查询和连接可能在此操作期间终止或超时。
管理	REDSHIFT-EVENT-3012	INFO	我们已收到于 [时间] 开始的集群“[集群名称]”的弹性调整大小请求。在调整大小操作开始时，我们将提供事件通知。
Pending (待处理)	REDSHIFT-EVENT-2025	INFO	集群 <集群名称> 的数据库将在 <开始时间> 和 <结束时间> 之间更新。您的集群将不可访问。相应地做好计划。
Pending (待处理)	REDSHIFT-EVENT-2026	INFO	集群 <集群名称> 将在 <开始时间> 和 <结束时间> 之间更新。您的集群将不可访问。相应地做好计划。
监控	REDSHIFT-EVENT-2050	INFO	Amazon Redshift 集群 [集群名称] 中检测到硬件问题。已于 [时间] 发起替换请求。
监控	REDSHIFT-EVENT-3000	INFO	您的 Amazon Redshift 集群 [集群名称] 已于 [时间] 重启。
监控	REDSHIFT-EVENT-3001	INFO	已于 [时间] 自动替换您的 Amazon Redshift 集群 [集群名称] 上的一个节点，您的集群运行正常。

Amazon Redshift 类别	事件 ID	事件严重性	描述
监控	REDSHIFT-EVENT-3002	INFO	您的 Amazon Redshift 集群 [集群名称] 已完成调整，可供读取和写入。[时间] 开始调整，[小时数] 小时后完成调整。
监控	REDSHIFT-EVENT-3003	INFO	已从快照 [快照名称] 成功创建 Amazon Redshift 集群 [集群名称]，可供使用。
监控	REDSHIFT-EVENT-3007	INFO	已于 [时间] 成功将您的 Amazon Redshift 快照 [快照名称] 从 [源 Amazon 区域] 复制到 [目标 Amazon 区域]。
监控	REDSHIFT-EVENT-3008	INFO	Amazon Redshift 集群 [集群名称] 表还原已于 [时间] 启动。
监控	REDSHIFT-EVENT-3009	INFO	Amazon Redshift 集群 [集群名称] 表还原已于 [时间] 成功完成。
监控	REDSHIFT-EVENT-3010	ERROR (错误)	Amazon Redshift 集群 [集群名称] 表还原于 [时间] 失败。
监控	REDSHIFT-EVENT-3013	ERROR (错误)	为 Amazon Redshift 集群 [集群名称] 请求的弹性调整大小操作在 [事件] 失败，原因是 [原因]。
监控	REDSHIFT-EVENT-3014	INFO	Amazon Redshift 已于 [时间] 重启集群 [集群名称]。
监控	REDSHIFT-EVENT-3500	ERROR (错误)	您的 Amazon Redshift 集群 [集群名称] 的大小调整失败。将在几分钟内自动重新尝试调整大小操作。
监控	REDSHIFT-EVENT-3501	ERROR (错误)	[时间] 执行还原操作来从快照 [快照名称] 创建 Amazon Redshift 集群 [集群名称] 失败。请重新尝试操作。
监控	REDSHIFT-EVENT-3504	ERROR (错误)	Simple Storage Service（Amazon S3）桶 [桶名称] 无效，无法对集群 [集群名称] 进行日志记录。
监控	REDSHIFT-EVENT-3505	ERROR (错误)	Simple Storage Service（Amazon S3）桶 [桶名称] 没有适用于集群 [集群名称] 的 IAM policy。
监控	REDSHIFT-EVENT-3506	ERROR (错误)	Simple Storage Service（Amazon S3）桶 [桶名称] 不存在。无法继续集群 [集群名称] 的日志记录。
监控	REDSHIFT-EVENT-3507	ERROR (错误)	无法使用 EIP [IP 地址] 创建 Amazon Redshift 集群 [集群名称]。此 EIP 已在使用中。
监控	REDSHIFT-EVENT-3508	ERROR (错误)	无法使用 EIP [IP 地址] 创建 Amazon Redshift 集群 [集群名称]。找不到 EIP。
监控	REDSHIFT-EVENT-3509	ERROR (错误)	没有为集群 [集群名称] 启用跨区域快照复制。
监控	REDSHIFT-EVENT-3510	ERROR (错误)	Amazon Redshift 集群 [集群名称] 表还原于 [时间] 启动失败。原因：[原因]。
监控	REDSHIFT-EVENT-3511	ERROR (错误)	Amazon Redshift 集群 [集群名称] 表还原于 [时间] 失败。

Amazon Redshift 类别	事件 ID	事件严重性	描述
监控	REDSHIFT-EVENT-3512	ERROR (错误)	Amazon Redshift 集群 [集群名称] 因硬件问题失败。集群正在从 [时间] 创建的最新快照 [快照名称] 中自动恢复。
监控	REDSHIFT-EVENT-3513	ERROR (错误)	Amazon Redshift 集群 [集群名称] 因硬件问题失败。集群正在从 [时间] 创建的最新快照 [快照名称] 中自动恢复。在此时间之后所做的任何数据库更改都需要重新提交。
监控	REDSHIFT-EVENT-3514	ERROR (错误)	Amazon Redshift 集群 [集群名称] 因硬件问题失败。集群正处于硬件故障状态。请删除集群并从 [时间] 创建的最新快照 [快照名称] 中恢复集群。
监控	REDSHIFT-EVENT-3515	ERROR (错误)	Amazon Redshift 集群 [集群名称] 因硬件问题失败。集群正处于硬件故障状态。请删除集群并从 [时间] 创建的最新快照 [快照名称] 中恢复集群。在此时间之后所做的任何数据库更改都需要重新提交。
监控	REDSHIFT-EVENT-3516	ERROR (错误)	Amazon Redshift 集群 [集群名称] 因硬件问题失败，且该集群没有备份。集群正处于硬件故障状态并且可以删除。
监控	REDSHIFT-EVENT-3519	INFO	集群 [集群名称] 已于 [时间] 开始重新启动。
监控	REDSHIFT-EVENT-3520	INFO	集群 [集群名称] 已于 [时间] 完成重启操作。
监控	REDSHIFT-EVENT-3521	INFO	我们检测到集群“[[集群名称]”的连接问题。已在 [时间] 启动自动诊断检查。
监控	REDSHIFT-EVENT-3522	INFO	集群“[集群名称]”的恢复操作于 [时间] 失败。Amazon Redshift 团队在寻求解决方案。
监控	REDSHIFT-EVENT-3533	ERROR (错误)	“[集群名称]”的集群调整大小操作已于 [时间] 取消。由于 [原因]，操作被取消。[需要采取的操作]。
监控	REDSHIFT-EVENT-3534	INFO	已于 [时间] 完成 Amazon Redshift 集群“[集群名称]”的弹性调整大小操作。在我们传输数据时，现在可以对集群执行读取和写入操作。在完成数据传输之前，某些查询可能需要更长的时间才能完成。
监控	REDSHIFT-EVENT-3537	INFO	集群“[集群名称]”数据传输已于 [时间，以 UTC 表示] 完成。
监控	REDSHIFT-EVENT-3600	INFO	Amazon Redshift 集群“[集群名称]”所请求的调整大小操作已于过去取消。回滚已于 [时间] 完成。
Pending (待处理)	REDSHIFT-EVENT-3601	INFO	集群 <集群名称> 上的节点将在 <开始时间> 和 <结束时间> 之间替换。您无法推迟该维护。相应地做好计划。
Pending (待处理)	REDSHIFT-EVENT-3602	INFO	集群 <集群名称> 上的节点计划在 <开始时间> 和 <结束时间> 之间替换。您的集群将不可访问。相应地做好计划。

Amazon Redshift 类别	事件 ID	事件严重性	描述
管理	REDSHIFT-EVENT-3603	INFO	执行还原操作来从快照 [快照名称] 创建集群 [集群名称] 因内部错误而失败。集群正处于不兼容的还原状态并且可以删除。尝试将快照恢复到具有不同配置的集群。
管理	REDSHIFT-EVENT-3614	INFO	计划操作 [计划操作名称] 已在 [时间，以 UTC 表示] 创建。第一次调用计划在 [时间，以 UTC 表示] 进行。
管理	REDSHIFT-EVENT-3615	INFO	计划操作 [计划操作名称] 已在 [时间，以 UTC 表示] 计划。
监控	REDSHIFT-EVENT-3616	INFO	[时间，以 UTC 表示] 计划的操作 [计划操作名称] 已完成，状态为“SUCCEEDED”。
监控	REDSHIFT-EVENT-3617	ERROR (错误)	计划操作 [计划操作名称] 在 [时间，以 UTC 表示] 因延迟而被跳过。
监控	REDSHIFT-EVENT-3618	INFO	集群 [集群名称] 暂停操作已于 [时间，以 UTC 表示] 开始。暂停已开始
监控	REDSHIFT-EVENT-3619	INFO	Amazon Redshift 集群 [集群名称] 已于 [UTC 时间] 被成功暂停。
管理	REDSHIFT-EVENT-3626	INFO	计划操作 [计划操作名称] 已在 [时间，以 UTC 表示] 修改。第一次调用计划在 [时间，以 UTC 表示] 进行。
管理	REDSHIFT-EVENT-3627	INFO	计划操作 [计划操作名称] 已在 [时间，以 UTC 表示] 删除。
监控	REDSHIFT-EVENT-3628	ERROR (错误)	[时间，以 UTC 表示] 计划的操作 [计划操作名称] 已完成，状态为“FAILED”。
管理	REDSHIFT-EVENT-3629	INFO	Amazon Redshift [集群名称] 已收到您的重新定位请求。当可用区重新定位完成时，Amazon Redshift 会发送一个事件通知。
管理	REDSHIFT-EVENT-3630	INFO	Amazon Redshift 集群 [集群名称] 已成功地从 [可用区] 重新定位到 [可用区]。您现在可以使用集群。
管理	REDSHIFT-EVENT-3631	INFO	Amazon Redshift 已成功将 Amazon Redshift 集群 [集群名称] 从 [可用区] 重新定位到 [可用区]，以便恢复。
管理	REDSHIFT-EVENT-3632	INFO	Amazon Redshift 因配置更改已暂时禁用 Amazon Redshift 集群 [集群名称] 的集群重定位。请稍后重新尝试集群重新定位。
管理	REDSHIFT-EVENT-3652	INFO	在 Redshift 集群 [集群名称] 上，AQUA 配置状态更改为 [AQUA 配置状态]。此更改将于下次集群重新启动后生效。
监控	REDSHIFT-EVENT-3658	ERROR (错误)	针对 Redshift 集群 [集群 ID]，EC2-Classic 到 EC2-VPC 的迁移失败。

Amazon Redshift 类别	事件 ID	事件严重性	描述
监控	REDSHIFT-EVENT-3659	INFO	针对 Redshift 集群 [集群 ID]，EC2-Classic 到 EC2-VPC 的迁移成功。
监控	REDSHIFT-EVENT-3660	INFO	集群正处于硬件故障状态。请删除 EC2-Classic 集群并从在 [UTC 时间] 创建的最新快照 [快照名称] 还原到 EC2-VPC 集群。
安全性	REDSHIFT-EVENT-4000	INFO	您的 Amazon Redshift 集群 [集群名称] 的管理员凭证已于 [时间] 更新。
安全性	REDSHIFT-EVENT-4001	INFO	已于 [时间] 修改安全组 [安全组名称]。这些更改将自动针对所有关联的集群进行。
安全性	REDSHIFT-EVENT-4500	ERROR (错误)	您提供的安全组 [安全组名称] 无效。未应用您对集群 [集群名称] 进行的配置更改。请访问 Amazon Web Services Management Console，以解决该问题。
安全性	REDSHIFT-EVENT-4501	ERROR (错误)	找不到在集群安全组 [集群安全组名称] 中指定的安全组 [安全组名称]。无法完成授权。
安全性	REDSHIFT-EVENT-4502	ERROR (错误)	Amazon Redshift 集群 [集群名称] 的管理员凭证在 [时间] 因并发活动更新失败。允许当前工作负载完成或减少活动工作量，然后重试该操作。

下表显示的是参数组为源类型时的事件类型和事件列表。

参数组源类型的类别和事件

Amazon Redshift 类别	事件 ID	事件严重性	描述
配置	REDSHIFT-EVENT-1002	INFO	参数 [参数名称] 已于 [时间] 从 [值] 更新为 [值]。
配置	REDSHIFT-EVENT-1003	INFO	已创建集群参数组 [组名称]。
配置	REDSHIFT-EVENT-1004	INFO	已删除集群参数组 [组名称]。
配置	REDSHIFT-EVENT-1005	INFO	已于 [时间] 更新集群参数组 [名称]。如果只更改了动态参数，则现在正在修改关联的集群。如果您更改了静态参数，则在重新启动关联集群时将应用所有更新（包括动态参数）。

下表显示了安全组为源类型时的事件类别和事件列表。

安全组源类型的类别和事件

Amazon Redshift 类别	事件 ID	事件严重性	描述
安全性	REDSHIFT-EVENT-4002	INFO	已创建集群安全组 [组名称]。
安全性	REDSHIFT-EVENT-4003	INFO	已创建集群安全组 [组名称]。
安全性	REDSHIFT-EVENT-4004	INFO	集群安全组 [组名称] 已于 [时间] 更改。更改将自动应用于所有关联的集群。

下表显示了快照为源类型时的事件类别和事件列表。

快照源类型的类别和事件

Amazon Redshift 类别	事件 ID	事件严重性	描述
管理	REDSHIFT-EVENT-2009	INFO	Amazon Redshift 集群 [集群名称] 的用户快照 [快照名称] 已于 [时间] 开始拍摄。要监控快照制作进度，请访问 Amazon Web Services Management Console。
管理	REDSHIFT-EVENT-2010	INFO	您的 Amazon Redshift 集群 [集群名称] 的用户快照 [快照名称] 已于 [时间] 取消拍摄。
管理	REDSHIFT-EVENT-2011	INFO	您的 Amazon Redshift 集群 [集群名称] 的用户快照 [快照名称] 已于 [时间] 被删除。
管理	REDSHIFT-EVENT-2012	INFO	Amazon Redshift 集群 [集群名称] 的最终快照 [快照名称] 已于 [时间] 开始拍摄。
监控	REDSHIFT-EVENT-3004	INFO	您的 Amazon Redshift 集群 [集群名称] 的用户快照 [快照名称] 已于 [时间] 成功完成拍摄。
监控	REDSHIFT-EVENT-3005	INFO	Amazon Redshift 集群 [名称] 的最终快照 [名称] 已于 [时间] 成功完成拍摄。
监控	REDSHIFT-EVENT-3006	INFO	Amazon Redshift 集群 [集群名称] 的最终快照 [快照名称] 已于 [时间] 取消拍摄。
监控	REDSHIFT-EVENT-3502	ERROR (错误)	Amazon Redshift 集群 [集群名称] 的最终快照 [快照名称] 于 [时间] 拍摄失败。团队正在调查此问题。请访问 Amazon Web Services Management Console，以重试该操作。
监控	REDSHIFT-EVENT-3503	ERROR (错误)	您的 Amazon Redshift 集群 [集群名称] 的用户快照 [快照名称] 于 [时间] 拍摄失败。团队正在调查此问题。请访问 Amazon Web Services Management Console，以重试该操作。

使用 Amazon Redshift 控制台管理事件通知

主题

- 创建事件通知订阅 (p. 513)

您可以创建 Amazon Simple Notification Service (Amazon SNS) 事件通知订阅，以便在特定 Amazon Redshift 集群、快照、安全组或参数组发生事件时发送通知。这些通知被发送到 SNS 主题，然后 SNS 主题将消息传输给订阅该主题的任何 SNS 使用者。发送给使用者的 SNS 消息可以采用 Amazon 区域的 Amazon SNS 支持的任何通知形式，如电子邮件、文本消息或对 HTTP 端点的调用。例如，所有区域都支持电子邮件通知，但 SMS 通知只能在美国东部（弗吉尼亚北部）区域中进行创建。有关更多信息，请参阅Amazon Redshift 事件通知 (p. 503)。

本部分介绍如何通过 Amazon Web Services Management Console 管理 Amazon Redshift 事件通知订阅。

创建事件通知订阅

要创建事件订阅

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Redshift 控制台：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Events（事件）。
3. 选择 Event subscription (事件订阅) 选项卡，然后选择 Create event subscriptions (创建事件订阅)。
4. 输入事件订阅的属性，例如名称、源类型、类别和严重性。您还可以启用 Amazon SNS 主题以获取事件通知。
5. 选择 Create event subscriptions（创建事件订阅）以创建订阅。

使用 Amazon CLI 和 Amazon Redshift API 管理事件通知

您可以使用以下 Amazon Redshift CLI 操作来管理事件通知。

- create-event-subscription
- delete-event-subscription
- describe-event-categories
- describe-event-subscriptions
- describe-events
- modify-event-subscription

您可以使用以下 Amazon Redshift API 操作来管理事件通知。

- CreateEventSubscription
- DeleteEventSubscription
- DescribeEventCategories
- DescribeEventSubscriptions
- DescribeEvents
- ModifyEventSubscription

有关 Amazon Redshift 事件通知的更多信息，请参阅Amazon Redshift 事件通知 (p. 503)。

Amazon Redshift 资源中的配额和限制

Amazon Redshift 具有的配额限制了每个 Amazon 区域 Amazon 账户中的多种资源的使用。每个配额都有一个默认值，并且部分配额可以调整。对于可调整的配额，您可以通过提交 Amazon Redshift 限制提高表来请求提高 Amazon 区域中 Amazon 账户的配额。

Amazon Redshift 对象的配额

Amazon Redshift 具有的配额限制了多种对象类型的使用。每个配额都有一个原定设置值。

配额名称	Amazon 默认值	可调整	描述
您可以向其授予为每个快照还原快照的权限的 Amazon 账户	20	否	您可以向其授予为每个快照还原快照的权限的 Amazon 账户的最大数量。
您可以向其授予为每个 Amazon KMS key 密钥还原快照的权限的 Amazon 账户	100	否	您可以向其授予为每个 KMS 密钥还原快照的权限的 Amazon 账户的最大数量。例如，如果您有 10 个快照，它们使用了一个 KMS 密钥加密，那么您可以授权 10 个 Amazon 账户来还原每个快照，或者是其他组合：总共 100 账户以及每个快照不超过 20 个账户。
适用于 Amazon Redshift 的集群 IAM 角色，可用于访问其他 Amazon 服务	50[1]	否	IAM 角色的最大数量，可将这些 IAM 角色与集群关联以授权 Amazon Redshift 访问拥有集群和 IAM 角色的用户的其他 Amazon 服务。 [1]下列区域的配额为 10Amazon Web Services 区域：ap-northeast-3、af-south-1、eu-south-1、ap-southeast-3、us-gov-east-1、us-gov-west-1、us-iso-east-1、us-isob-east-1。
所有用户定义的手动 WLM 队列的并发级别（查询槽）	50	否	由手动工作负载管理定义的所有用户定义的队列的最大查询槽数。
并发扩展集群	10	是	并发扩展集群的最大数量。
集群中的 DC2 节点	128	是	可以分配给集群的 DC2 节点的最大数量。有关每个节点类型的节点限制的更多信息，请参阅Amazon Redshift 中的集群和节点 (p. 50)。

配额名称	Amazon 默认值	可调整	描述
集群中的 DS2 节点	128	是	可以分配给集群的 DS2 节点的最大数量。有关每个节点类型的节点限制的更多信息，请参阅Amazon Redshift 中的集群和节点 (p. 50)。
事件订阅	20	是	此账户在当前 Amazon 区域中的事件订阅的最大数量。
节点	200	是	此账户在当前 Amazon 区域所有数据库实例中的节点的最大数量。
参数组	20	否	此账户在当前 Amazon 区域中的参数组的最大数量。
集群中的 RA3 节点	128	是	可以分配给集群的 RA3 节点的最大数量。有关每个节点类型的节点限制的更多信息，请参阅Amazon Redshift 中的集群和节点 (p. 50)。
连接到集群的 Redshift 托管 VPC 端点	30	是	可以连接到集群的 Redshift 托管 VPC 端点的最大数量。有关 Redshift 托管 VPC 端点的更多信息，请参阅在 Amazon Redshift 中使用 Redshift 托管的 VPC 终端节点 (p. 81)。
通过 RedShift 托管的 VPC 端点访问集群的被授权者	5	是	集群拥有者可以授权为集群创建 RedShift 托管 VPC 端点的最大被授权者数量。有关 Redshift 托管 VPC 端点的更多信息，请参阅在 Amazon Redshift 中使用 Redshift 托管的 VPC 终端节点 (p. 81)。
每个授权的 Redshift 托管 VPC 端点	5	是	可为每个授权创建的 Redshift 托管 VPC 端点的最大数量。有关 Redshift 托管 VPC 端点的更多信息，请参阅在 Amazon Redshift 中使用 Redshift 托管的 VPC 终端节点 (p. 81)。
预留节点	200	是	此账户在当前 Amazon 区域中的预留节点的最大数量。
每个集群的每个数据库中的架构	9900	否	可以在每个集群的每个数据库中创建的 schema 的最大数量。但是，`pg_temp_*` schema 不计入此配额。
安全组	20	是	此账户在当前 Amazon 区域中的安全组的最大数量。
通过 COPY 加载时的单一行大小	4	否	使用 COPY 命令加载时的单一行的最大大小（以 MB 为单位）。
快照	20	是	此账户在当前 Amazon 区域中的用户快照的最大数量。
子网组	20	是	此账户在当前 Amazon 区域中的子网组的最大数量。
子网组中的子网	20	是	子网组的最大子网数。
`large` 集群节点类型的表	9900	否	大型集群节点类型的表的最大数量。此限制包括永久表、临时表、数据共享表和具体化视图。外部表被计为临时表。临时表包括用户定义的临时表以及查询处理或系统维护期间由 Amazon Redshift 创建的临时表。此限制中并不包括视图和系统表。

配额名称	Amazon 默认值	可调整	描述
xlarge 集群节点类型的表	9900	否	xlarge 集群节点类型的表的最大数量。此限制包括永久表、临时表、数据共享表和具体化视图。外部表被计为临时表。临时表包括用户定义的临时表以及查询处理或系统维护期间由 Amazon Redshift 创建的临时表。此限制中并不包括视图和系统表。
具有单节点集群的 xlplus 集群节点类型的表。	9900	否	具有单节点集群的 xlplus 集群节点类型的最大表数量。此限制包括永久表、临时表、数据共享表和具体化视图。外部表被计为临时表。临时表包括用户定义的临时表以及查询处理或系统维护期间由 Amazon Redshift 创建的临时表。此限制中并不包括视图和系统表。
具有多节点集群的 xlplus 集群节点类型的表。	20000	否	具有多节点集群的 xlplus 集群节点类型的最大表数量。此限制包括永久表、临时表、数据共享表和具体化视图。外部表被计为临时表。临时表包括用户定义的临时表以及查询处理或系统维护期间由 Amazon Redshift 创建的临时表。此限制中并不包括视图和系统表。
4xlarge 集群节点类型的表	100000	否	4xlarge 集群节点类型的表的最大数量。此限制包括永久表、临时表、数据共享表和具体化视图。外部表被计为临时表。临时表包括用户定义的临时表以及查询处理或系统维护期间由 Amazon Redshift 创建的临时表。此限制中并不包括视图和系统表。
8xlarge 集群节点类型的表	100000	否	8xlarge 集群节点类型的表的最大数量。此限制包括永久表、临时表、数据共享表和具体化视图。外部表被计为临时表。临时表包括用户定义的临时表以及查询处理或系统维护期间由 Amazon Redshift 创建的临时表。此限制中并不包括视图和系统表。
16xlarge 集群节点类型的表	100000	否	16xlarge 集群节点类型的表的最大数量。此限制包括永久表、临时表、数据共享表和具体化视图。外部表被计为临时表。临时表包括用户定义的临时表以及查询处理或系统维护期间由 Amazon Redshift 创建的临时表。此限制中并不包括视图和系统表。
集群中用户定义的数据库	60	否	可以为每个集群创建的用户定义的数据库的最大数量。
空闲或非活动会话超时	4 小时	否	此设置适用于集群。有关为用户设置空闲会话超时值的信息，请参阅 Amazon Redshift 数据库开发人员指南中的更改用户。用户设置优先于集群设置。
空闲事务的超时	6 小时	否	在 Amazon Redshift 结束与事务关联的会话之前，未结事务的最长不活动时间。此设置优先于任何用户定义的空闲超时设置。它适用于集群。
数据库中存储的程序	10000	否	存储程序的最大数量。请参阅存储程序支持的限制和区别了解更多限制。

Amazon Redshift Serverless 对象的配额

Amazon Redshift 具有的配额限制了 Amazon Redshift Serverless 实例中的多种对象类型的使用。每个配额都有一个原定设置值。

配额名称	Amazon 默认值	可调整	描述
数据库数	100	否	Amazon Redshift Serverless 实例中允许的最大数据库计数。
架构数	9900	否	Amazon Redshift Serverless 实例中允许的最大架构计数。
表的数量	100000	否	Amazon Redshift Serverless 实例中允许的最大表计数。
空闲或非活动会话超时	4 小时	否	有关为用户设置空闲会话超时值的信息，请参阅 Amazon Redshift 数据库开发人员指南中的更改用户。用户设置优先。
空闲事务的超时	6 小时	否	在 Amazon Redshift Serverless 结束与事务关联的会话之前，未结事务的最长不活动时间。此设置优先于任何用户定义的空闲超时设置。
最大连接数	2000	否	允许连接到工作组的连接的最大数目。

有关 Amazon Redshift Serverless 账单如何受超时配置影响的更多信息，请参阅Amazon Redshift Serverless 的计费 (p. 18)。

查询编辑器 v2 对象的配额

Amazon Redshift 具有的配额限制了 Amazon Redshift 查询编辑器 v2 中多种对象类型的使用。每个配额都有一个原定设置值。

配额名称	Amazon 默认值	可调整	描述
连接	500	是	您可以在当前区域的此账户中使用查询编辑器 v2 创建的最大连接数。
保存的查询	2500	是	您可以在当前区域的此账户中使用查询编辑器 v2 创建的最大已保存查询数。
查询版本	20	是	您可以在当前区域的此账户中使用查询编辑器 v2 创建的每个查询的最大版本数。
已保存图表	500	是	您可以在当前区域的此账户中使用查询编辑器 v2 创建的最大已保存图表数。
每个查询获取的行	100000	是	当前区域中此账户中查询编辑器 v2 每次查询获取的最大行数。
每个查询获取的数据大小	5	是	当前区域中此账户中查询编辑器 v2 每次查询获取的数据的最大大小（以兆字节为单位）。

配额名称	Amazon 默认值	可调整	描述
每个主体的同时套接字连接数	10	是	单个主体可以在当前区域中建立的与查询编辑器 v2 的最大同时套接字连接数。如果您收到套接字连接超过限制的错误，请评估是否增加此配额。
每个账户的同时套接字连接数	250	是	账户中的所有主体可以在当前区域中建立的与查询编辑器 v2 的最大同时套接字连接数。如果您收到套接字连接超过限制的错误，请评估是否增加此配额。

Amazon Redshift Spectrum 对象的配额和限制

Amazon Redshift Spectrum 具有以下配额和限制：

- 使用 Amazon Glue Data Catalog 时每个Amazon账户的最大数据库数。有关更多信息，请参阅 Amazon Web Services 一般参考中的 Amazon Glue 服务配额。
- 使用 Amazon Glue Data Catalog 时每个数据库的最大表数。有关更多信息，请参阅亚马逊云科技一般参考 中的 Amazon Glue 服务配额。
- 使用 Amazon Glue Data Catalog 时每个表的最大分区数。有关更多信息，请参阅亚马逊云科技一般参考中的 Amazon Glue 服务配额。
- 使用 Amazon Glue Data Catalog 时每个Amazon账户的最大分区数。有关更多信息，请参阅亚马逊云科技一般参考 中的 Amazon Glue 服务配额。
- 使用 Amazon Glue Data Catalog 时外部表的最大列数（启用伪列时为 1,597，未启用伪列时为 1600）。
- 使用 Amazon Glue Data Catalog 时 ION 或 JSON 文件中字符串值的最大大小为 16 KB。
- 您可以使用单个 ALTER TABLE 语句添加最多 100 个分区。
- 所有 S3 数据必须与 Amazon Redshift 集群位于同一 Amazon 区域。
- ION 和 JSON 中的时间戳必须使用 ISO8601 格式。
- 不支持外部压缩 ORC 文件。
- Text、OpenCSV 和 Regex SERDEs 不支持大于 '\177' 的八进制分隔符。
- 您必须在分区列上指定谓词以避免从所有分区读取。

  例如，以下谓词在列 `ship_dtm` 上进行筛选，但不会将筛选条件应用于分区列 `ship_yyyymm`：

  ```
  WHERE ship_dtm > '2018-04-01'.
  ```

  要跳过不需要的分区，您需要添加谓词 `WHERE ship_yyyymm = '201804'`。此谓词仅允许对分区 `\ship_yyyymm=201804\` 进行读操作。

这些限制不适用于 Apache Hive 元存储。

命名约束

下表介绍 Amazon Redshift 中的命名约束。

集群标识符	• 集群标识符必须仅包含小写字符。 • 它必须包含 1–63 个字母数字字符或连字符。 • 它的第一个字符必须是字母。 • 它不能以连字符结束或包含两个连续连字符。

	• 一个 Amazon 账户内的所有集群必须拥有唯一的标识符。
数据库名称	• 数据库名称必须包含 1-64 个字母数字字符。 • 必须仅由小写字母组成。 • 不能使用保留字。要查看保留关键字的列表，请参阅 Amazon Redshift 数据库开发人员指南中的保留关键字。
Redshift 托管的 VPC 端点的端点名称	• 端点名必须包含 1—30 个字符。 • 有效字符为 A-Z、a-z、0-9 和连字符 (-)。 • 第一个字符必须是字母。 • 名称不能包含两个连续的连字符，也不能以连字符结束。
管理员用户名称	• 管理员用户名必须仅包含小写字符。 • 必须包含 1–128 个字母数字字符。 • 它的第一个字符必须是字母。 • 不能使用保留字。要查看保留关键字的列表，请参阅 Amazon Redshift 数据库开发人员指南中的保留关键字。
管理员密码	• 管理员密码必须包含 8–64 个字符。 • 至少必须包含一个大写字母。 • 至少必须包含一个小写字母。 • 它必须包含一个数字。 • 它可以使用带有 ASCII 代码 33–126 的任何 ASCII 字符，但 ' (单引号) 、" (双引号) 、\、/ 或 @ 除外。
参数组名称	• 参数组名称必须包含 1–255 个字母数字字符或连字符。 • 它必须只由小写字母组成。 • 它的第一个字符必须是字母。 • 它不能以连字符结尾，也不能包含两个连续连字符。
集群安全组名称	• 集群安全组名称必须包含不超过 255 个字母数字字符或连字符。 • 它必须只由小写字母组成。 • 它不得是 **`Default`**。 • 它在您的 Amazon 账户创建的所有安全组中必须具有唯一性。
子网组名称	• 子网组名称必须包含不超过 255 个字母数字字符或连字符。 • 它必须只由小写字母组成。 • 它不得是 **`Default`**。 • 它在您的 Amazon 账户创建的所有子网组中必须具有唯一性。
集群快照标识符	• 集群快照标识符必须包含不超过 255 个字母数字字符或连字符。 • 它必须只由小写字母组成。 • 它不得是 **`Default`**。 • 它在您的 Amazon 账户创建的所有快照标识符中必须具有唯一性。

在 Amazon Redshift 中为资源添加标签

主题

- 标记概述 (p. 520)
- 使用控制台管理资源标签 (p. 521)
- 使用 Amazon Redshift API 管理标签 (p. 521)

标记概述

在 Amazon 中，标签是用户定义的标记，由键-值对组成。Amazon Redshift 支持通过添加标签来提供资源的元数据概述，以及根据成本分配对您的账单报告进行分类。要将标签用于成本分配，您必须先在 Amazon Billing and Cost Management 服务中激活这些标签。有关设置标签并将其用于计费的更多信息，请参阅在自定义账单报告中使用成本分配标签和设置月度成本分配报告。

虽然标签对于 Amazon Redshift 中的资源来说并非必不可少，但它们却有助于提供背景信息。您可能想使用与成本中心、项目名称及该资源的其他相关信息有关的元数据来为资源添加标签。例如，假设您要跟踪属于测试环境和生产环境的资源。您可以创建名为 `environment` 的键并提供值 `test` 或 `production`，以确定在各环境中使用的资源。如果您在其他 Amazon 服务中使用了标签或者具有针对您业务的标准类别，那么，我们建议您为 Amazon Redshift 中的资源创建相同的键值对以保持一致性。

在您调整集群以及将集群快照还原到同一区域后，资源的标签将得以保留。但是，如果您将快照复制到其他区域，则不会保留标签，因此您必须在新的区域重新创建标签。如果删除资源，则会删除所有关联的标签。

每个资源都有一个标签集，它是分配给该资源的一个或多个标签的集合。每个资源的每个标签集内最多有 50 个标签。您可以在创建资源时以及资源创建完成后添加标签。您可以向 Amazon Redshift 中的以下资源类型添加标签：

- CIDR/IP
- Cluster
- 集群安全组
- 集群安全组传入规则
- Amazon EC2 安全组
- 硬件安全模块 (HSM) 连接
- HSM 客户端证书
- 参数组
- 快照
- 子网组

要使用 Amazon Redshift 控制台中的标记，您的 IAM 用户可以附加亚马逊云科技托管策略 `AmazonRedshiftFullAccess`。有关具有可附加到 Amazon Redshift 控制台用户的有限标记权限的示例 IAM 策略，请参阅示例 7：允许用户使用 Amazon Redshift 控制台标记资源 (p. 385)。有关标记的更多信息，请参阅什么是 Amazon Resource Groups？。

标记要求

标签具有以下要求：

- 键不得以 aws: 作为前缀。
- 每个标签集中的各个键必须是独一无二的。
- 键的长度必须介于 1 到 128 个允许的字符之间。
- 值的长度必须介于 0 到 256 个允许的字符之间。
- 每个标签集中的值不需要是唯一的。
- 可以用作键和值的字符包括 Unicode 字符、数字、空格及以下符号：_ . : / = + - @。
- 键和值区分大小写。

使用控制台管理资源标签

要管理您的 Amazon Redshift 资源上的标签

1. 登录到 Amazon Web Services Management Console并打开 Amazon Redshift 控制台，网址：https://console.aws.amazon.com/redshift/。
2. 在导航菜单上，选择 Configurations（配置），然后选择 Manage tags（管理标签）。
3. 输入您的资源选择，并选择要添加、修改或删除哪些标签。然后选择 Manage tags of the resources that you chose（管理您选择的资源的标签）。

   您可以标记的资源包括集群、参数组、子网组、HSM 客户端证书、HSM 连接和快照。
4. 在 Manage tags（管理标签）导航页面中，选择 Review and apply tag changes（查看并应用标签更改），然后选择 Apply（应用）以保存您的更改。

使用 Amazon Redshift API 管理标签

您可以使用以下 Amazon CLI 操作来管理 Amazon Redshift 中的标签。

- create-tags
- delete-tags
- describe-tags

您可以使用以下 Amazon Redshift API 操作来管理标签。

- CreateTags
- DeleteTags
- DescribeTags
- 标签
- TaggedResource

此外，您还可以使用以下 Amazon Redshift API 操作来管理和查看特定资源的标签：

- CreateCluster
- CreateClusterParameterGroup
- CreateClusterSecurityGroup
- CreateClusterSnapshot
- CreateClusterSubnetGroup
- CreateHsmClientCertificate
- CreateHsmConfiguration

- DescribeClusters
- DescribeClusterParameterGroups
- DescribeClusterSecurityGroups
- DescribeClusterSnapshots
- DescribeClusterSubnetGroups
- DescribeHsmClientCertificates
- DescribeHsmConfigurations

Amazon Redshift 的集群版本

Amazon Redshift 定期发布集群版本。您的 Amazon Redshift 集群将在系统维护时段进行修补。补丁的时间取决于 Amazon Web Services 区域和维护时段设置。您可以从 Amazon Redshift 控制台中查看或更改维护时段设置。有关维护的更多信息，请参阅集群维护 (p. 60)。

您可以在 Amazon Redshift 控制台上集群详细信息的 Maintenance（维护）选项卡中查看集群的集群版本。或者，您可以在 SQL 命令的输出中看到集群版本：

```
SELECT version();
```

主题

- Amazon Redshift 补丁 170 (p. 523)
- Amazon Redshift 补丁 169 (p. 523)
- Amazon Redshift 补丁 168 (p. 524)

Amazon Redshift 补丁 170

此修补程序中的集群版本：

- 1.0.40325 – 于 2022 年 7 月 27 日发布

此补丁中的新功能和改进功能

- ST_GeomfromGeoJSON：从采用 GeoJSON 表示形式的 VARCHAR 构造 Amazon Redshift 空间几何体对象。

Amazon Redshift 补丁 169

此修补程序中的集群版本：

- 1.0.40083：于 2022 年 7 月 16 日发布
- 1.0.39734：于 2022 年 7 月 7 日发布
- 1.0.39380：于 2022 年 6 月 23 日发布
- 1.0.39251：于 2022 年 6 月 15 日发布
- 1.0.39009：于 2022 年 6 月 8 日发布

此补丁中的新功能和改进功能

- 添加角色作为 Alter Default Privileges 命令的参数，以支持基于角色的访问控制。
- 添加 ACCEPTINVCHARS 参数，以支持在从 Parquet 和 ORC 文件复制时替换无效的 UTF-8 字符。
- 添加 OBJECT(k,v) 函数，以从键和值对构建 SUPER 对象。

Amazon Redshift 补丁 168

此修补程序中的集群版本：

- 1.0.38698 – 于 2022 年 5 月 25 日发布
- 1.0.38551 – 于 2022 年 5 月 20 日发布
- 1.0.38463 – 于 2022 年 5 月 18 日发布
- 1.0.38361 – 于 2022 年 5 月 13 日发布
- 1.0.38199：于 2022 年 5 月 9 日发布
- 1.0.38112 — 于 2022 年 5 月 6 日发布
- 1.0.37684 — 于 2022 年 4 月 20 日发布

此补丁中的新功能和改进功能

- 在 Amazon Redshift ML 中添加对线性学习器模型类型的支持。
- 为 SQL 事务隔离级别添加了 SNAPSHOT 选项。
- 添加 `farmhashFingerprint64` 作为 `VARBYTE` 和 `VARCHAR` 数据的新哈希算法。
- 在实例化视图的增量刷新中支持 AVG 函数。
- 支持 Redshift Spectrum 中对外部表的相关子查询。
- 为了提高开箱即用的查询性能，Amazon Redshift 会自动为特定表选择单列主键作为分发键。

文档历史记录

下表介绍了 2018 年 6 月之后的每个 Amazon Redshift 集群管理指南发布版本中的重要更改。如需对此文档更新的通知，您可以订阅 RSS 源。

API 版本：2012-12-01

有关对 Amazon Redshift 数据库开发人员指南的更改的列表，请参阅 Amazon Redshift 数据库开发人员指南文档历史记录。

有关新功能的更多信息（包括每个版本的修复和关联的集群版本号的列表），请参阅集群版本历史记录。

update-history-change	update-history-description	update-history-date
Amazon Redshift 补丁 170 已发布。 (p. 523)	正在部署一个新的 Amazon Redshift 补丁。新版本需要几周时间才能在所有支持 Amazon Redshift 的 Amazon Web Services 区域中发布。有关此版本的更多信息，请参阅 Amazon Redshift 补丁 170。	2022 年 7 月 20 日
Amazon Redshift 补丁 169 已发布。 (p. 523)	正在部署一个新的 Amazon Redshift 补丁。新版本需要几周时间才能在所有支持 Amazon Redshift 的 Amazon Web Services 区域中发布。有关此版本的更多信息，请参阅 Amazon Redshift 补丁 169。	2022 年 6 月 8 日
Amazon Redshift 补丁 168 已发布。 (p. 524)	正在部署一个新的 Amazon Redshift 补丁。新版本需要几周时间才能在所有支持 Amazon Redshift 的 Amazon Web Services 区域中发布。有关此版本的更多信息，请参阅 Amazon Redshift 补丁 168。	2022 年 4 月 19 日
支持使用 Amazon Redshift 驱动程序的身份验证配置文件	您现在可以使用身份验证配置文件连接到 Amazon Redshift。	2021 年 8 月 2 日
支持 AQUA	AQUA（高级查询加速器）是一款面向 Amazon Redshift 的分析查询加速器，它使用自定义设计的硬件来加快扫描大型数据集的查询速度。	2021 年 4 月 14 日
支持由 Amazon PrivateLink 提供支持的 Amazon Redshift 的跨 VPC 端点	您现在可以将 Redshift 托管的 VPC 端点与 Amazon Redshift 结合使用。	2021 年 4 月 1 日
支持 Amazon Redshift 查询编辑器增强功能	您现在可以使用具有增强型 VPC 路由、更长查询运行时间和更多集群节点类型的查询编辑器。	2021 年 2 月 17 日
支持与合作伙伴的控制台集成	您可以使用 Amazon Redshift 控制台与合作伙伴集成。	2020 年 12 月 9 日

支持在可用区之间移动集群的能力	现在，您可以在可用区之间移动 RA3 集群。	2020 年 12 月 9 日
支持 ra3.xlplus 节点类型	您现在可以创建 ra3.xlplus 节点类型。	2020 年 12 月 9 日
支持 JDBC 驱动程序版本 2.0	您现在可以配置 JDBC 驱动程序版本 2.0。	2020 年 11 月 5 日
支持 Lambda UDF 和令牌化	您现在可以编写 Lambda UDF 来启用数据的外部令牌化。	2020 年 10 月 26 日
支持安排 SQL 语句的运行	您现在可以在 Amazon Redshift 控制台上安排查询。	2020 年 10 月 22 日
支持用于 Amazon Redshift 的数据 API	Amazon Redshift 现在可以使用内置数据 API 访问。文档更新包含 Amazon Redshift 数据 API 参考。	2020 年 9 月 10 日
支持 Amazon Redshift 控制台查询监控	更新了指南以描述新的查询监控图表。	2020 年 5 月 7 日
对使用限制的支持	更新了指南以描述使用限制。	2020 年 4 月 23 日
多重身份验证	更新了指南以描述多重验证支持。	2020 年 4 月 20 日
弹性调整大小现在支持节点类型更改	更新了弹性调整大小说明。	2020 年 4 月 6 日
支持具有托管存储的 ra3.4xlarge 节点类型	更新了指南以包含 ra3.4xlarge 节点类型。	2020 年 4 月 2 日
支持暂停和恢复	更新了指南以描述暂停和恢复集群操作。	2020 年 3 月 11 日
支持 Microsoft Azure AD 作为身份提供者	更新了指南，以描述将 Microsoft Azure AD 用作身份提供者的步骤。	2020 年 2 月 10 日
支持 RA3 节点类型	更新了指南以描述新的 RA3 节点类型。	2019 年 12 月 3 日
对新控制台的支持	更新了指南以描述新的 Amazon Redshift 控制台。	2019 年 11 月 11 日
安全信息更新	对安全信息文档的更新。	2019 年 6 月 24 日
快照增强功能	Amazon Redshift 现在支持多种管理和计划快照的增强功能。	2019 年 4 月 4 日
并发扩展	您可以配置工作负载管理 (WLM) 来启用并发扩展模式。有关更多信息，请参阅配置工作负载管理。	2019 年 3 月 21 日
更新了 JDBC 和 ODBC 驱动程序	Amazon Redshift 现在支持新版本的 JDBC 和 ODBC 驱动程序。有关更多信息，请参阅配置 JDBC 连接和配置 ODBC 连接。	2019 年 2 月 4 日

推迟的维护	如果需要重新计划集群的维护时段，您可以选择将维护最多延迟 14 天。如果我们需要在您推迟期间更新硬件或进行其他强制更新，我们会通知您并进行必要的更改。在这些更新期间，您的集群不可用。有关更多信息，请参阅推迟维护。	2018 年 11 月 20 日
预先通知	Amazon Redshift 为某些事件提前提供通知。这些事件的事件类别是 `pending`。例如，如果集群中的一个节点需要硬件更新，我们会发送预先通知。您可以订阅与其他 Amazon Redshift 事件相同的待处理事件。有关更多信息，请参阅订阅 Amazon Redshift 事件通知。	2018 年 11 月 20 日
弹性调整大小	弹性调整大小是调整集群大小的最快方法。弹性调整大小会在现有集群上添加或删除节点，然后自动将数据重新分配到新节点。因为它不会创建新集群，所以弹性调整大小操作通常会在几分钟内快速完成。有关更多信息，请参阅调整集群大小。	2018 年 11 月 15 日
新的 ODBC 驱动程序	Amazon Redshift ODBC 驱动程序已更新至版本 1.4.3.1000。有关更多信息，请参阅配置 ODBC 连接。	2018 年 11 月 8 日
取消调整大小操作	您现在可以在调整大小操作正在进行时取消它。有关更多信息，请参阅调整大小操作概述。	2018 年 11 月 2 日
修改集群以更改加密	您可以使用 Amazon 托管式密钥或客户托管式密钥修改未加密的集群以使用 Amazon Key Management Service（Amazon KMS）加密。当您修改集群以启用 KMS 加密时，Amazon Redshift 会自动将您的数据迁移到新加密的集群。您还可以通过修改集群将未加密的集群迁移到加密的集群。	2018 年 10 月 16 日
Amazon Redshift Spectrum 支持增强型 VPC 路由	现在，您可以在集群中使用启用了增强型 VPC 路由的 Redshift Spectrum。您可能需要执行其他配置步骤。有关更多信息，请参阅将 Amazon Redshift Spectrum 与增强型 VPC 路由结合使用。	2018 年 10 月 10 日
查询编辑器	您现在可以从 Amazon Redshift 管理控制台运行 SQL 查询。	2018 年 10 月 4 日

工作负载执行细分图表	您现在可以通过查看控制台中的工作负载执行细分图表，详细查看工作负载的性能。有关更多信息，请参阅分析工作负载性能。	2018 年 7 月 30 日
维护跟踪	您现在可以通过选择维护跟踪来确定集群是否始终会更新到最新版的 Amazon Redshift 或先前版本。有关更多信息，请参阅选择集群维护跟踪。	2018 年 7 月 26 日

下表介绍了 2018 年 7 月前对 Amazon Redshift 集群管理指南的一些重要更改。

更改	描述	发行日期
新的 CloudWatch 指标	针对监控查询性能添加了新 CloudWatch 指标。有关更多信息，请参阅使用 CloudWatch 指标监控 Amazon Redshift (p. 472)。	2018 年 5 月 17 日
HSM 加密	Amazon Redshift 仅支持适用于硬件安全模块 (HSM) 密钥管理的 Amazon CloudHSM。有关更多信息，请参阅Amazon Redshift 数据库加密 (p. 347)。	2018 年 3 月 6 日
IAM 角色创建	如果附加到集群的 IAM 角色无法访问必要的资源，则您可以串联另一个角色（可能属于其他账户）。然后，您的集群临时代入串联的角色来访问数据。您还可以通过串联角色来授予跨账户访问权限。链中的每个角色都会代入链中的下一个角色，直到集群承担位于链尾的角色。您可以串联最多 10 个角色。有关更多信息，请参阅在 Amazon Redshift 中串联 IAM 角色 (p. 428)。	2018 年 2 月 23 日
新的 DC2 节点类型	新一代密集计算 (DC) 节点类型以与 DC1 相同的价格提供更好的性能。为了利用性能改进，您可以将 DC1 集群迁移到较新的 DC2 节点类型。有关更多信息，请参阅Amazon Redshift 中的集群和节点 (p. 50)。	2017 年 10 月 17 日
ACM 证书	Amazon Redshift 正将您的集群中的 SSL 证书替换为 Amazon Certificate Manager (ACM) 颁发的证书。ACM 是一个可信的公有证书颁发机构 (CA)，受当前大多数系统信任。您可能需要更新当前的信任根 CA 证书，才能继续使用 SSL 连接集群。有关更多信息，请参阅将 SSL 连接过渡到 ACM 证书 (p. 220)。	2017 年 9 月 18 日
服务相关角色	服务相关角色是一种独特类型的 IAM 角色，它与 Amazon Redshift 直接相关。服务相关角色由 Amazon Redshift 预定义，具有服务代表您的 Amazon Redshift 集群调用 Amazon 服务所需的所有权限。有关更多信息，请参阅对 Amazon Redshift 使用服务相关角色 (p. 389)。	2017 年 9 月 18 日
IAM 数据库用户身份验证	您可以将系统配置为允许用户创建用户凭证，并基于其 IAM 凭证登录数据库。也可以通过符合 SAML 2.0 标准的身份提供者配置系统，让用户使用联合单点登录进行登录。有关更多信息，请参阅使用 IAM 身份验证生成数据库用户凭证 (p. 393)。	2017 年 8 月 11 日
表级还原支持增强型 VPC 路由	使用增强型 VPC 路由 (p. 293)的集群现在支持表级还原。有关更多信息，请参阅从快照中还原表 (p. 324)。	2017 年 7 月 19 日

更改	描述	发行日期
查询监控规则	使用 WLM 查询监控规则，您可以为 WLM 查询定义基于指标的性能边界，并指定查询超出这些边界时需要采取的操作—log、hop 或 abort。您将在工作负载管理 (WLM) 配置中定义查询监控规则。有关更多信息，请参阅配置工作负载管理 (p. 301)。	2017 年 4 月 21 日
增强型 VPC 路由	在使用 Amazon Redshift 增强型 VPC 路由时，Amazon Redshift 会强制通过 Amazon VPC 路由集群和数据存储库之间的所有 COPY 和 UNLOAD 流量。有关更多信息，请参阅Amazon Redshift 中的增强型 VPC 路由 (p. 293)。	2016 年 9 月 15 日
新的连接日志字段	连接日志 (p. 444) 审计日志有两个用于跟踪 SSL 连接的新字段。如果您定期向 Amazon Redshift 表加载审计日志，则需要向目标表添加以下新列：sslcompression 和 sslexpansion。	2016 年 5 月 5 日
新的 ODBC 驱动程序	Amazon Redshift ODBC 驱动程序已更新至版本 1.2.7.1007。有关更多信息，请参阅配置 ODBC 连接 (p. 207)。	2016 年 30 月 3 日
用于 COPY 和 UNLOAD 的 IAM 角色	您现在可指定您的集群可用于对其他 Amazon 服务的访问的身份验证的一个或多个 Amazon Identity and Access Management (IAM) 角色。IAM 角色提供了为 COPY、UNLOAD 或 CREATE LIBRARY 命令提供身份验证的更安全的替代方法。有关更多信息，请参阅授权 Amazon Redshift 代表您访问其他 Amazon 服务 (p. 425)和使用 IAM 角色授权 COPY、UNLOAD、CREATE EXTERNAL FUNCTION 和 CREATE EXTERNAL SCHEMA 操作 (p. 430)。	2016 年 3 月 29 日
从表中还原	您可以将集群快照中的表还原为活动集群中的新表。有关更多信息，请参阅从快照中还原表 (p. 324)。	2016 年 3 月 10 日
在策略中使用 IAM 条件	您可使用 IAM policy 中的 Condition 元素进一步限制对资源的访问。有关更多信息，请参阅使用 IAM policy 条件进行精细访问控制 (p. 361)。	2015 年 12 月 10 日
修改公开访问性	可以修改 VPC 中的现有集群以更改它是否可公开访问。有关更多信息，请参阅修改集群 (p. 86)。	2015 年 11 月 20 日
文档修复	发布了各种文档修复。	2015 年 8 月 28 日
文档更新	更新了与配置网络设置有关的故障排除指南，以确保具有不同的最大传输单位 (MTU) 大小的主机能决定连接的包大小。有关更多信息，请参阅查询似乎挂起，有时无法连接到集群 (p. 266)。	2015 年 8 月 25 日
文档更新	修订了有关参数组的整个部分，以使其变得更清楚且更有条理。有关更多信息，请参阅Amazon Redshift 参数组 (p. 299)。	2015 年 8 月 17 日
WLM 动态属性	WLM 配置参数现在支持动态应用一些属性。其他属性保持静态更改，并需要重启关联的集群以便能应用配置更改。有关更多信息，请参阅WLM 动态和静态属性 (p. 301)和Amazon Redshift 参数组 (p. 299)。	2015 年 8 月 3 日

更改	描述	发行日期
将 KMS 加密的集群复制到另一个 Amazon 区域	添加了有关配置快照复制授权以支持将 Amazon KMS 加密的集群复制到另一个 Amazon 区域的内容。有关更多信息，请参阅将 Amazon KMS 加密的快照复制到另一个 Amazon 区域 (p. 348)。	2015 年 7 月 28 日
文档更新	更新了数据库加密部分，以更好地说明 Amazon Redshift 如何使用 Amazon KMS 或 HSM 来管理密钥，以及加密过程如何使用所有这些选项。有关更多信息，请参阅Amazon Redshift 数据库加密 (p. 347)。	2015 年 7 月 28 日
新的节点类型	Amazon Redshift 现在提供了一种新的节点类型 DS2。更新了现有节点类型的文档参考，以使用本版本中引入的新的名称。此外，还修订了该部分以便更好地说明节点类型组合和阐述默认配额限制。有关更多信息，请参阅Amazon Redshift 中的集群和节点 (p. 50)。	2015 年 6 月 9 日
预留节点产品	添加了有关新的预留节点产品的内容。此外，修订了该部分以便更好地说明和比较可用的产品，并提供了演示按需和保留节点定价如何影响计费的示例。有关更多信息，请参阅概览 (p. 337)。	2015 年 6 月 9 日
新的 ODBC 驱动程序	Amazon Redshift ODBC 驱动程序已更新。添加了有关这些驱动程序之前版本的部分，以及指向驱动程序发布说明的链接。有关更多信息，请参阅配置 ODBC 连接 (p. 207)。	2015 年 6 月 5 日
文档修复	发布了各种文档修复。	2015 年 4 月 30 日
新功能	此版本的 Amazon Redshift 引入了新的 ODBC 和 JDBC 驱动程序，这些驱动程序已经过优化以便用于 Amazon Redshift。有关更多信息，请参阅使用 SQL 客户端工具连接到 Amazon Redshift 集群 (p. 135)。	2015 年 2 月 26 日
新功能	此版本的 Amazon Redshift 引入了集群性能指标，使您能够查看和分析查询执行详细信息。有关更多信息，请参阅查看查询和加载 (p. 494)。	2015 年 2 月 26 日
文档更新	添加了新的示例策略，该策略说明如何授予针对常见 Amazon 服务操作和 Amazon Redshift 依赖的资源的权限。有关更多信息，请参阅客户托管式策略示例 (p. 381)。	2015 年 1 月 16 日
文档更新	更新了有关设置最大传输单位 (MTU) 以禁用 TCP/IP 极大帧的指南。有关更多信息，请参阅在创建集群时使用 EC2-VPC (p. 54)和查询似乎挂起，有时无法连接到集群 (p. 266)。	2015 年 1 月 16 日
文档更新	修订了有关 `wlm_json_configuration` 参数的内容，提供了示例语法以便在 Linux、Mac OS X 和 Microsoft Windows 操作系统上使用 Amazon CLI 来配置此参数。有关更多信息，请参阅配置工作负载管理 (p. 301)。	2015 年 1 月 13 日
文档更新	添加了缺少的事件通知和说明。有关更多信息，请参阅Amazon Redshift 事件类别和事件消息 (p. 505)。	2015 年 1 月 8 日
文档更新	更新了有关针对 Amazon Redshift 操作和资源的 IAM policy 的指南。修订了该部分以使其变得更清楚且更有条理。有关更多信息，请参阅Amazon Redshift 中的安全性 (p. 345)。	2014 年 11 月 21 日

更改	描述	发行日期
新功能	此版本的 Amazon Redshift 引入了用于通过来自 Amazon Key Management Service (Amazon KMS) 的加密密钥对集群进行加密的功能。Amazon KMS 将安全、高度可用的硬件和软件结合起来，提供可扩展到云的密钥管理系统。有关 Amazon KMS 的更多信息和 Amazon Redshift 的加密选项，请参阅Amazon Redshift 数据库加密 (p. 347)和使用控制台管理集群 (p. 83)。	2014 年 11 月 12 日
新功能	此版本的 Amazon Redshift 引入了用于为资源（例如，集群和快照）添加标签的功能。利用标签，您可以提供用户定义的元数据来根据成本分配对账单报告进行分类，并帮助您更好地标识资源。有关更多信息，请参阅在 Amazon Redshift 中为资源添加标签 (p. 520)。	2014 年 11 月 4 日
新功能	将 dw1.8xlarge 和 dw2.8xlarge 节点大小的最大节点限制增至 128 个节点。有关更多信息，请参阅Amazon Redshift 中的集群和节点 (p. 50)。	2014 年 10 月 30 日
文档更新	添加了指向 Amazon Redshift 使用 PostgreSQL ODBC 驱动程序时需要的 Microsoft Visual C++ 2010 Redistributable Package 的链接。有关更多信息，请参阅在 Microsoft Windows 上安装和配置 Amazon Redshift ODBC 驱动程序 (p. 208)。	2014 年 10 月 30 日
新功能	添加了用于终止来自 Amazon Redshift 控制台的查询和加载的功能。有关更多信息，请参阅查看查询和加载 (p. 494)和在加载操作期间查看集群指标 (p. 498)。	2014 年 10 月 28 日
文档修复	发布了各种文档修复。	2014 年 10 月 17 日
新增内容	添加了有关关闭集群和删除集群的内容。有关更多信息，请参阅关闭和删除集群 (p. 74)和删除集群 (p. 86)。	2014 年 8 月 14 日
文档更新	阐明了集群的 Allow Version Upgrade 设置的行为。有关更多信息，请参阅Amazon Redshift 集群概览 (p. 50)。	2014 年 8 月 14 日
文档更新	修订了有关在 Amazon Redshift 控制台中使用集群的主题的过程、快照和组织。有关更多信息，请参阅使用控制台管理集群 (p. 83)。	2014 年 7 月 11 日
新增内容	添加了有关调整 Amazon Redshift 集群大小的新教程，包括如何在调整集群大小的同时最大程度地减少集群处于只读模式的时间量。有关更多信息，请参阅在 Amazon Redshift 中调整集群大小 (p. 65)。	2014 年 6 月 27 日
新功能	添加了用于重命名集群的功能。有关更多信息，请参阅重命名集群 (p. 74)和修改集群 (p. 86)。	2014 年 6 月 2 日
文档更新	更新了 .NET 代码示例，以便在通过 .NET 以编程方式连接到集群时使用 ODBC 数据提供商。有关更多信息，请参阅使用 .NET 连接到集群 (p. 260)。	2014 年 5 月 15 日
新功能	添加了用于在从快照还原集群时选择其他参数组和安全组的选项。有关更多信息，请参阅从快照还原集群 (p. 328)。	2014 年 5 月 12 日

更改	描述	发行日期
新功能	添加了新的部分以说明如何配置默认 Amazon CloudWatch 告警以监控 Amazon Redshift 集群中使用的磁盘空间百分比。此警报是集群创建过程中的新选项。有关更多信息，请参阅默认磁盘空间警报 (p. 64)。	2014 年 4 月 28 日
文档更新	阐明了有关 Amazon Redshift 中的 Elliptic curve Diffie—Hellman Exchange (ECDHE) 支持的信息。有关更多信息，请参阅使用 SSL 进行连接 (p. 217)。	2014 年 4 月 22 日
新功能	添加了有关 Amazon Redshift 支持 Elliptic curve Diffie—Hellman (ECDH) 密钥协商协议的陈述。有关更多信息，请参阅使用 SSL 进行连接 (p. 217)。	2014 年 4 月 18 日
文档更新	修订并重新整理了使用 SQL 客户端工具连接到 Amazon Redshift 集群 (p. 135)部分中的主题。添加了有关 JDBC 和 ODBC 连接的更多信息和一个关于连接问题的新的疑难解答部分。	2014 年 4 月 15 日
文档更新	添加了整个指南中的 IAM policy 示例中的版本。	2014 年 4 月 3 日
文档更新	添加了有关定价在调整集群大小时的工作方式的信息。有关更多信息，请参阅购买 Amazon Redshift 预留节点 (p. 337)。	2014 年 4 月 2 日
新功能	添加了有关新参数 `max_cursor_result_set_size` 的部分，此部分设置可为单个光标存储的最大结果集大小（以兆字节为单位）。此参数值还影响集群的并行活动光标数。有关更多信息，请参阅Amazon Redshift 参数组 (p. 299)。	2014 年 3 月 28 日
新功能	添加了有关 Cluster Version 字段的说明，现在包含集群引擎版本和数据库修订号。有关更多信息，请参阅Amazon Redshift 集群 (p. 50)。	2014 年 3 月 21 日
新功能	更新了大小调整过程以在集群的 Status 选项卡上显示新的大小调整进度信息。有关更多信息，请参阅调整集群大小 (p. 87)。	2014 年 3 月 21 日
文档更新	重新整理和更新了什么是 Amazon Redshift？ (p. 1)，并修订了 Amazon Redshift 管理概览 (p. 1)。发布了各种文档修复。	2014 年 2 月 21 日
新功能	添加了 Amazon Redshift 集群的新节点类型和大小，并且根据反馈重新编写了相关的集群概览主题，以使其变得更清楚且更有条理。有关更多信息，请参阅Amazon Redshift 集群 (p. 50)。	2014 年 1 月 23 日
新功能	添加了有关使用虚拟私有云中可公开访问的 Amazon Redshift 集群的弹性 IP (EIP) 地址的信息。有关 Amazon Redshift 中的 EIP 的更多信息，请参阅在 VPC 中管理集群 (p. 92) 和在 VPC 中创建集群 (p. 93)。	2013 年 12 月 20 日
新功能	添加了有关 Amazon Redshift 的 Amazon CloudTrail 日志的信息。有关 Amazon Redshift 支持 CloudTrail 的更多信息，请参阅使用 Cloudtrail 进行日志记录 (p. 450)。	2013 年 12 月 13 日

更改	描述	发行日期
新功能	添加了有关 Amazon Redshift 中的数据库审计日志记录功能的新用户活动日志和 `enable_user_activity_logging` 数据库参数的信息。有关数据库审计日志记录的更多信息，请参阅数据库审计日志记录 (p. 443)。有关数据库参数的更多信息，请参阅 Amazon Redshift 参数组 (p. 299)。	2013 年 12 月 6 日
新功能	已更新以描述如何配置 Amazon Redshift 以自动将自动化快照和手动快照复制到辅助 Amazon 区域。有关配置跨区域快照复制的更多信息，请参阅将快照复制到另一个 Amazon 区域 (p. 321)。	2013 年 11 月 14 日
新功能	添加了一个部分来描述连接和用户活动的 Amazon Redshift 审计日志记录，以及如何将这些日志存储在 Amazon S3 中。有关数据库审计日志记录的更多信息，请参阅数据库审计日志记录 (p. 443)。	2013 年 11 月 11 日
新功能	添加了一个部分来描述 Amazon Redshift 加密与用于管理硬件安全模块 (HSM) 中的加密密钥并轮换加密密钥的新功能。有关加密、HSM 和密钥轮换的更多信息，请参阅 Amazon Redshift 数据库加密 (p. 347)、使用硬件安全模块的 Amazon Redshift 加密 (p. 349)和Amazon Redshift 中的加密密钥轮换 (p. 350)。	2013 年 11 月 11 日
新功能	已更新以描述如何使用 Amazon SNS 发布 Amazon Redshift 事件通知。有关 Amazon Redshift 事件通知的更多信息，请参阅Amazon Redshift 事件通知 (p. 503)。	2013 年 11 月 11 日
新功能	已更新以描述 IAM 资源级权限。有关 Amazon Redshift IAM 权限的信息，请参阅Amazon Redshift 中的安全性 (p. 345)。	2013 年 8 月 9 日
新功能	已更新以描述如何还原进度指标。有关更多信息，请参阅从快照还原集群 (p. 322)。	2013 年 8 月 9 日
新功能	已更新以描述集群快照共享和创建快照进度指标。有关更多信息，请参阅共享快照 (p. 325)。	2013 年 7 月 17 日
文档修复	发布了各种文档修复。	2013 年 7 月 8 日
新控制台屏幕	更新了 Amazon Redshift 集群管理指南以匹配 Amazon Redshift 控制台中的更改。	2013 年 4 月 22 日
新指南	这是 Amazon Redshift 管理指南 的第一个版本。	2013 年 2 月 14 日