Redshift Authentication

Overview

The Alchemer Amazon Redshift integration uses AWS credentials to authenticate and securely connect to your Redshift cluster or Redshift Serverless workgroup.

Amazon Redshift API Credentials

What You Need

- AWS Access Key ID
- AWS Secret Access Key

How to Get Your Amazon Redshift API Credentials

1. Create or Identify AWS Credentials
Contact your AWS administrator and request that they create a new IAM user or use an existing one with programmatic access enabled. Make sure they provide you with the **Access Key ID** and **Secret Access Key, as these credentials are required** .

2. Assign Required Permissions
Ensure the IAM user or role has permissions to access Redshift and execute calls like 'Execute', 'Get', and 'Describe'. Please check the AWS documentation if needed.

3. Gather Redshift Connection Details
From the Amazon Redshift console, note your cluster identifier or Serverless workgroup name, database name, and database user.

Additional Setup for the Redshift Workflow Initiator

The Redshift Workflow Initiator needs the permissions below in addition to the credentials above.

- **Note:** The initiator supports Redshift Serverless workgroups only. Provisioned Redshift clusters are not supported for the initiator.

1. Attach IAM permissions
Choose **one** of the options below and attach it to the IAM user.

Option A: Easiest setup

- Attach the AWS managed policy **AmazonRedshiftDataFullAccess**.
- Add this inline policy to the same user:

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

Option B: Most secure (limited to one workgroup)

- Attach this policy instead. Replace `<REGION>`, `<ACCOUNT_ID>`, and `<WORKGROUP_ID>` with your values.
  - The workgroup ID is shown on the workgroup's **General information** page. It is not the workgroup name.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "redshift-serverless:ListWorkgroups",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "redshift-serverless:GetCredentials",
    "redshift-data:ExecuteStatement"
   ],
   "Resource": "arn:aws:redshift-serverless:<REGION>:<ACCOUNT_ID>:workgroup/<WORKGROUP_ID>"
  },
  {
   "Effect": "Allow",
   "Action": [
    "redshift-data:DescribeStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:CancelStatement"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": { "redshift-data:statement-owner-iam-userid": "${aws:userid}" }
   }
  }
 ]
}
```

2. Grant database access

Required for both options. The initiator connects to Redshift as the database user `IAM:<iam-user-name>`. As an admin, run the following in **Redshift Query Editor v2**:

```
GRANT USAGE ON SCHEMA <schema_name> TO "IAM:<iam-user-name>";
GRANT SELECT ON ALL TABLES IN SCHEMA <schema_name> TO "IAM:<iam-user-name>";
```

- **Note:** The `IAM:` database user is created the first time the IAM user connects. If the GRANT fails with "user does not exist," start the initiator setup once (through the database dropdown), then run the GRANT again.

Common setup issues

- **Workgroup dropdown is empty:** `ListWorkgroups` is missing, or the wrong AWS region was entered.
- **Databases don't load:** `GetCredentials` or `ExecuteStatement` is missing, or the workgroup ID in the policy doesn't match.
- **Tables or columns fail with "permission denied":** The database GRANT above is missing.

Need more help? Click here for Amazon Redshift's API help documents.

Authenticate Amazon Redshift in Alchemer

After obtaining your Amazon Redshift credentials, add them to the Alchemer Amazon Redshift integration. Credentials are securely stored in Alchemer and can be reused across workflows.

How to Authenticate

Your browser does not support HTML5 video.

Authentication Walkthrough

1. Start a New Authentication

- Inside any Amazon Redshift integration action, select **New Authentication**.

2. Enter Your Amazon Redshift Credentials

Provide the following:

- AWS Access Key ID
- AWS Secret Access Key

3. Save Your Authentication

- Select **Create**.
- Once created:
  - The authentication is saved and reused for all Amazon Redshift actions
  - You only need to update it if your AWS or Redshift credentials change

Related Articles