Amazon Redshift simplifies the use of other AWS services by introducing the default IAM role

Posted On: Nov 18, 2021

Amazon Redshift now simplifies the use of other services such as Amazon S3, Amazon SageMaker, AWS Lambda, Amazon Aurora, and AWS Glue by allowing customers to create an IAM role from the Redshift console and assigning it as the default IAM role while creating an Amazon Redshift cluster. The default IAM role helps simplify SQL operations such as COPY, UNLOAD, CREATE, EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL, or CREATE LIBRARY that accesses other AWS services by eliminating the need to specify the Amazon Resource Name (ARN) for the IAM role .

Amazon Redshift now provides a new managed IAM policy AmazonRedshiftAllCommandsFullAccess policy that has required privileges to use other related services such as S3, SageMaker, Lambda, Aurora, and Glue. This policy is used for creating the default IAM role with Amazon Redshift console. The end users can use the default IAM role with COPY, UNLOAD, CREATE, EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL, or CREATE LIBRARY commands by specifying IAM\_ROLE with DEFAULT keyword without having to specify ARN for the IAM role.

This feature is now available in all AWS commercial regions except eu-south-1, af-south-1, and ap-northeast-3. You can find more information about the IAM role from the Redshift cluster management [guide](https://docs.aws.amazon.com/redshift/latest/mgmt/default-iam-role.html).

Name, review, and create

**Role details**

Role name

Enter a meaningful name to identify this role.

Maximum 128 characters. Use alphanumeric and '+=,.@-\_' characters.

Description

Add a short explanation for this policy.

Maximum 1000 characters. Use alphanumeric and '+=,.@-\_' characters.

Step 1: Select trusted entities

**Edit**

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"sts:AssumeRole"

],

"Principal": {

"Service": [

"redshift.amazonaws.com"

]

}

}

]

}

Step 2: Add permissions

**Edit**

Permissions policy summary

|  |  |  |
| --- | --- | --- |
| **Policy name** | **Type** | **Attached as** |
| [AmazonS3ReadOnlyAccess](https://us-east-1.console.aws.amazon.com/iam/home#/policies/arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess) | AWS managed | Permissions policy |

Tags

**Add tags (Optional)**

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.









